

## Možnosti rozšíření identifikačních údajů majitele certifikátu se zachováním jeho soukromí

Vojtěch Kment (Vojtěch KMENT CONSULTING, <http://www.vkc.cz>)

*Při používání certifikátů veřejného klíče pro elektronický podpis často vzniká potřeba přesné identifikace protějšku, zejména v široce otevřených systémech bez předchozího styku komunikujících stran. Úřad MPSV ČR proto v současnosti nechává vkládat jím vydané identifikátory do certifikátu veřejného klíče osoby. Toto řešení je sice technicky lákavé, zároveň je však právně a bezpečnostně nežádoucí i uživatelsky nepraktické. Dvě v článku popisovaná řešení používají unikátní identifikátory vydávané různými organizacemi nezávisle na sobě, bez uvádění do kvalifikovaných certifikátů. Metody zajišťují plnou automatizaci zpracování elektronicky podepsaných dokumentů i právní jistotu spoléhající strany při omezení rizik narušení soukromí podepisujících, hladší pracovní procesy a malé náklady.*

Český kvalifikovaný certifikát veřejného klíče (dále podpisový certifikát) vydaný akreditovaným poskytovatelem certifikačních služeb (certifikační autoritou, dále CA), určený pro ověřování elektronických podpisů, může ze zákona o elektronickém podpisu (dále ZoEP) obsahovat až tak málo identifikace jako je jen jméno a příjmení osoby, či jen pseudonym (vhodné pro podatelny úřadů). Občanů jména např. Petr Novák jsou v ČR stovky, mnohonásobné mohou být i certifikáty vystavené např. na „Ferda Mravenec – Pseudonym“.

Slovenská právní úprava je obdobná, byť přesunutá spíše do úrovně vyhlášky – 538/02 Z.z. Kvalifikovaný certifikát opět musí obsahovat: „meno a priezvisko alebo pseudonym“ rozšířené o „doplňujúci identifikátor zabezpečujúci jednoznačnosť identifikačných údajov držiteľa certifikátu“.

Zlepšení identifikace se snaží řešit i do loňská novela českého ZoEP (226/2002Sb.) přidáním:

*§11 ...Pokud je zaručený elektronický podpis založený na kvalifikovaném certifikátě užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.*

Česká ani slovenská úprava však nestanoví přesně, jaké údaje (identifikátor) se mají použít pro jednoznačnou identifikaci držitele certifikátu. Řešením nabílední je do certifikátu vložit rodné číslo osoby. Jenže rodné číslo kóduje chráněné osobní údaje, existují jeho duplicity, u zaměstnance je nerelevantní a jako společný nadužívaný identifikátor technicky usnadňuje nežádoucí spojování databází.

Pro zlepšení identifikace by se teoreticky mohly použít další osobní údaje držitele certifikátu, jež má CA běžně k dispozici při ověřování. Bohužel ani uvedení přesné adresy a data narození by nemuselo vést k jednoznačné identifikaci, jednoznačné by však bylo např. číslo občanského průkazu. Použití těchto identifikačních údajů je však opět sporné, protože veřejně prozrazuje o dotyčném některé jeho osobní údaje, které lze případně zneužít např. pro krádeže identity i mimo oblast elektronického podpisu vůbec.

Ještě jinou možností je nechat občanům státu vydat nový jednoznačný identifikátor osoby ~ elektronické rodné číslo, jež by neobsahoval významové podúdaje. Jeho jednotným zavedením by se však opět usnadnilo nežádoucí spojování záznamů osob z různých databází a následné hrozby vůči soukromí. Ačkoliv si toho často lidé nejsou vědomi, ochrana soukromí a zábrana před neoprávněným

shromažďováním osobních údajů patří v polistopadové éře mezi nejváženější práva občanů, zaručovaná na úrovni Ústavy ČR v rámci tzv. „Listiny základních práv a svobod“. Praktickou úpravou oblasti tohoto ústavního práva pak v ČR je především zákon o ochraně osobních údajů 101/2000 Sb.

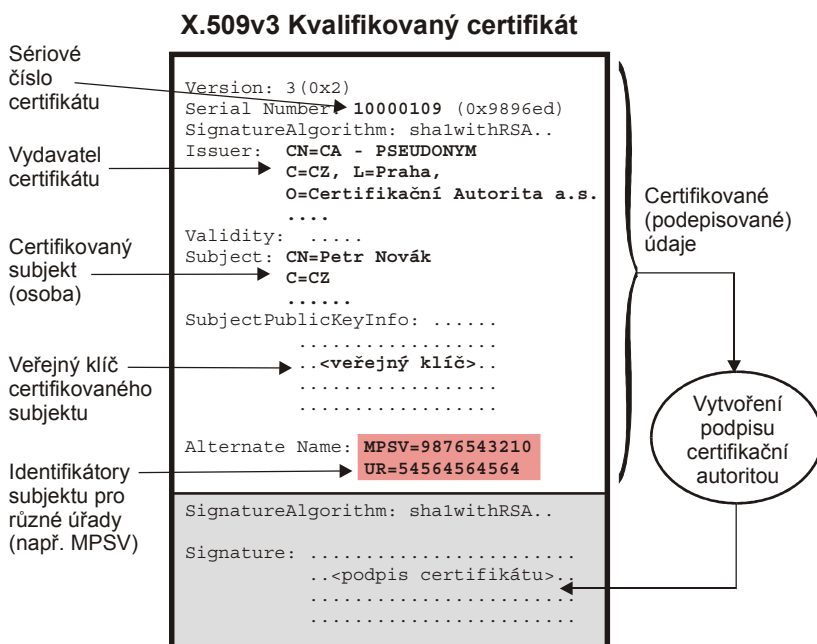
Certifikovaný si běžně řídí své soukromí tím, které informace o sobě do certifikátu nechá vložit. Jakékoliv jiné údaje, jež si certifikovaný do certifikátu uvést nepřeje a které si CA pořizuje při ověřování (např. informace z kopie občanského průkazu), poskytne CA třetím stranám pouze na žádost soudu. Jakékoliv jiné žádosti o sdělení identifikačních údajů osoby uvedené v certifikátu CA běžně ignoruje.

V případě komunikace zaměstnanců firem jejich protějšků může identifikaci usnadnit povinné uvedení rejstříkového názvu organizace v poličku O (Organizace), popř. i OU (organizační jednotka), Title (funkce) a zejména adresa elektronické pošty. Dodržení těchto pravidel je však např. v ČR stanoveno však až na úrovni certifikační politiky zatím jediné akreditované CA a není jisté, zda tuto konvenci budou jiné CA rovněž dodržovat.

Při styku druhu B2C může být namísto pečlivého zjišťování identity dostatečné přesné zajištění platby. **Problém identifikace však přetrvává u skutečně masové automatizované komunikace, jaké čelí veřejná správa či velké e-businessy.**

## Identifikátor MPSV

Ministerstvo práce a sociálních věcí ČR (MPSV) nalezlo řešení uvedeného problému jednoznačné identifikace v dohodě s CA, která na žádost certifikovaného do vydávaného certifikátu uvádí jeho identifikátor MPSV (viz obr. 1), jednoznačně identifikující certifikovanou osobu v rámci informačního systému MPSV. Bez identifikátoru v certifikátu IS MPSV komunikaci s osobou odmítne.



**obr. 1 – Kvalifikovaný certifikát obsahující identifikátor MPSV v alternativním jménu subjektu, nepraktické a bezpečnostně nevhodné řešení**

Metoda nicméně skrývá nevýhody, jež se ozřejmí představou, že by stejně postupovalo více úřadů:

1. Certifikáty se neustále budou doplňovat o další identifikátory. Tzn. vydávání stále nových podpisových certifikátů (po 700,- Kč), dle platné certifikační politiky vždy k novým podpisovým klíčům. Současné certifikáty, platné i zneplatněné, vedou i k nepřehlednosti a nesnadnosti komunikace dané osoby i jejich protějšků.

2. Podpisové certifikáty jsou veřejné, identifikátory se kompromitují.
3. Úzké propojení systémů na jednu CA podvazuje konkurenci certifikátorů.

Zájemce by si teoreticky mohl nechat vytvořit identifikátory pro všechny úřady předem (nejpozději při certifikaci), v praxi je to nerealistické. Druhá potíž je zásadní - identifikátory úřadů by v certifikátu vytvořily „superID“, sice nevýznamové, jeho veřejnost ale útočníkům opět usnadní spojování databází.

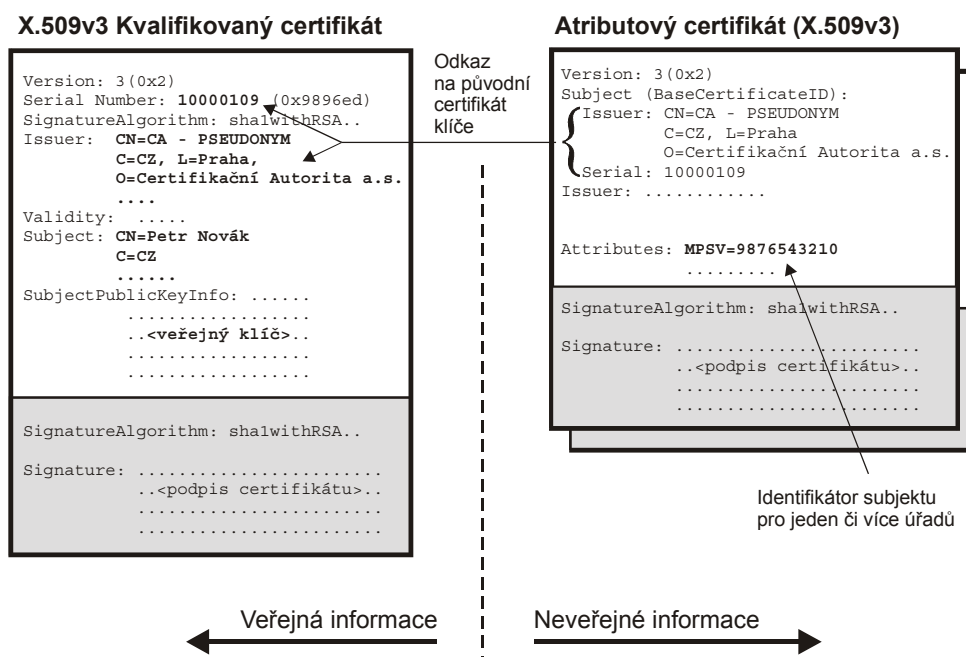
Přitom paradoxně „takové údaje“ (z výše citované novely ZoEP) nebo identifikátor (ze slovenské vyhlášky 538/2002 Z.z.) sloužící pro jednoznačnou identifikaci jsou v běžných certifikátech X.509 obsaženy již od certifikačního pravěku. Dvojice vydavatel a sériové číslo (Issuer+SN) unikátně identifikuje certifikát a potažmo osobu (pravost Issuer se zjistí ověřením podpisu CA). Zahrnutí identifikátoru MPSV apod. identifikátorů situaci z technického ani právního hlediska nezlepší, vzniká nadbytečná identifikace. MPSV popř. jiné úřady si sice se svým identifikátorem poradí snadněji, certifikování ale budou zakoušet výše uvedené nevýhody.

Přitom dostačuje, aby se vytvořilo „spojení“ mezi podpisovým certifikátem a identifikátory. ZoEP vytváření odkazů na podpisový certifikát nijak neomezuje. Následuje popis 2 takových metod.

## Řešení 1: Atributové certifikáty

Atributové certifikáty se liší od známých podpisových certifikátů tím, že neobsahují veřejný klíč certifikované osoby, ale jiné její ověřené údaje (atributy). Atributový certifikát může např. obsahovat dispoziční práva, role, funkce apod., zde identifikátor osoby u určitého úřadu. Postupy CA při ověřování mohou být stejně přísné jako u kvalifikovaných certifikátů, tj. shodně důvěryhodné.

První výhoda je, že atributové certifikáty lze vydávat v čase postupně, před zahájení komunikace s dalším úřadem, původní podpisový a předchozí atributové certifikáty jsou zachovány. Odpadá shánění mračna dokladů při první certifikaci. Druhá výhoda je soukromí – atributový certifikát může být u CA neveřejný (lze se doptat pouze na stav platnosti) a certifikovaný ho poskytuje jen vybraným protějškům dle svého uvážení.



obr. 2 Identifikátor vložený do atributového certifikátu, které mohou být chráněné a neveřejné

Atributový certifikát se odkazuje na podpisový certifikát, je podepsán CA, nejjednodušeji tou, jež vydala podpisový certifikát, obecně i jinou. Při vydání shodnou CA má CA možnost plně ověřit totožnost identity osoby na podpisovém certifikátu a atributovém certifikátu, při vydání jinou osobou je třeba, aby žadatel prvotní žádost podepsal klíčem odpovídajícím odkazovanému podpisovému certifikátu a doložil tak své vlastnictví podpisového certifikátu nepřímo.

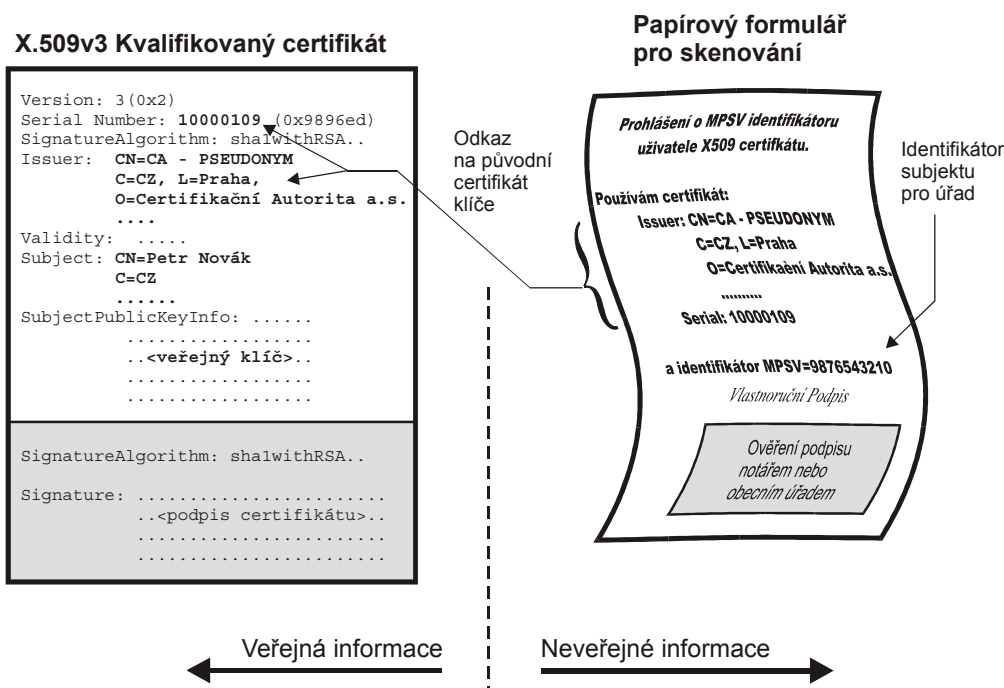
Při vhodné certifikační politice vydávání kvalifikovaných certifikátů může být atributový certifikát použit i s později vydanými podpisovými certifikáty, tj. být vystaven na delší dobu životnosti.

Atributové certifikáty zmiňuje již X.509v3 z roku 1997, do módy se dostávají až nedávno, viz čerstvé dokumenty ETSI 102 044 nebo RFC 3281.

## Řešení 2 – Certifikace notářů

Analogii atributových certifikátů mohou spravovat i samotné úřady. Protože často nedisponují sítí poboček, v nichž by mohly odpovědně samy ověřovat, mohou využít služeb klasických notářství. Stačí, aby zvláštní aplikace vhodným způsobem uživateli vytiskla písmem fonty OCR několik jeho údajů: identifikaci, z podpisového certifikátu zejména Issuer+SN a kýžený identifikátor organizace.

Dokument může být pro vyšší bezpečnost a integritu digitálně podepsán nebo hašován (haš či podpis vytištěn), především však bude klasicky podepsán u notáře (30,- Kč) a zaslán běžnou poštou (viz obr. 3).



obr. 3 Identifikátor zaznamenaný na formuláři s notářsky ověřeným vlastnoručním podpisem, formulář po naskenování archivován

Úřad došlý papírový dokument naskenuje a po provedení funkce OCR získá spojení z čísla certifikátu na svůj identifikátor. Pokud notář neověřuje souvislost osoby s identifikátorem, má takto ověřený vztah kvalitu prohlášeného atributu (claimed attribute). Úřad nicméně zpravidla může provést kontrolu doplňkových identifikačních údajů (adresa bydliště apod.) notářem vždy ověřených, úroveň notářsky ověřovaného podpisu je přitom silnější způsob ověření, než se vyžaduje v 99% případech styku se státní správou.

Metoda skýtá stejné výhody jako první, navíc není třeba čekat na ustálení formátů atributových certifikátů v implementacích a bude kompatibilní s podpisovými certifikáty mnoha CA. Ověřované podpisy rovněž mají v právu své pevné zakotvení, praxi i rozvětvenou síť notářů i jiných ověřovatelů. Úřad může i vydat atributový certifikát jako v prvním řešení a zaslat jej uživateli elektronicky.

---

Autor je konzultant elektronického podpisu

<http://www.vkc.cz>

---

## Vhodná doplňková literatura

- [1] Kment, V.: „E-podpis v praxi s komplikacemi”, ComputerWorld 4/2003, Praha - leden 2003.
- [2] ITU-T Recommendation X.509 (1997 E): „Information Technology - Open Systems Interconnection - The Directory: Authentication Framework“, June 1997.
- [3] ETSI-TC ESI: „Requirements for role and attribute certificates“, ETSI TR 102 044 V1.1.1 (2002-12), Sophia Antipolis Cedex, December 2002.
- [4] Farrell, S., Housley, R.: „An Internet Attribute Certificate Profile for Authorization”, RFC 3281, April 2002.
- [5] Zákon 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), Sbírka zákonů - Částka 32/2000, Praha 2000.
- [6] Zákon 226/2002 Sb. kterým se mění ... zákon 227/2000Sb o elektronickém podpisu, Sbírka zákonů - Částka 87/2000, Praha 2002.
- [7] První certifikační autorita, a.s.: „Certifikační politika pro vydávání osobních kvalifikovaných certifikátů, Verze 1.03“, Praha 2002.
- [8] Zákon 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, Zbierka zákonov – Čiastka 91/2002, Bratislava 2002.
- [9] Vyhláška Národného bezpečnostného úradu 538/2002 Z.z. o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o kvalifikovaných certifikátoch), Zbierka zákonov – Čiastka 211/2002, Bratislava 2002.