Jednoznačná identifikace se zachováním soukromí

Vojtěch Kment – vyšlo 31.1.2003

Uvádění identifikátorů v certifikátech veřejného klíče u elektronicky podepsaných zpráv je technicky lákavé a zároveň právně a bezpečnostně nežádoucí i uživatelsky nepraktické. Dvě 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.

Tuzemský 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".

CA sice uchovává další informace o certifikovaném, údaje neuvedené v certifikátu třetím stranám poskytuje ale pouze na žádost soudu. Certifikovaný si řídí své soukromí tím, které informace o sobě do certifikátu nechá vložit. V případě komunikace zaměstnanců firem jejich protějškům identifikaci usnadňuje povinné uvedení rejstříkového názvu organizace v políčku O (Organizace), popř. i OU (organizační jednotka), Title (funkce) a zejména adresa elektronické pošty. Při styku B2C může být dostatečné zajištění platby. **Problém identifikace však přetrvává u skutečně masové automatizované komunikace, jaké čelí veřejná správa či velké e-businessy.**

Nevhodné je použití rodného čísla v certifikátu. Kóduje chráněné osobní údaje, existují jeho duplicity, u zaměstnance je nerelevantní a jako společný identifikátor usnadňuje spojování databází.

Identifikátor MPSV

Ministerstvo práce a sociálních věcí ČR (MPSV) nalezlo řešení v dohodě s CA, jež do vydávaných certifikátů volitelně uvádí identifikátor MPSV (viz obr. 1), jednoznačně identifikující osobu v rámci IS MPSV. Bez identifikátoru se komunikace s osobou odmítne.

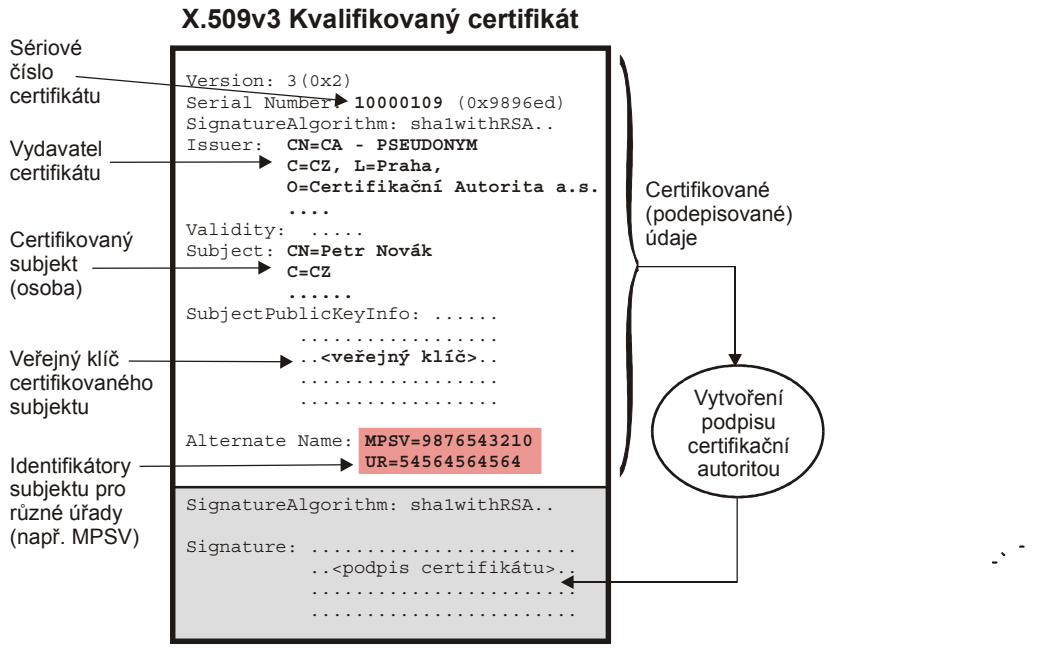
Metoda nicméně skrývá nevýhody, jež se ozřejmí představou, že by stejně postupovalo více úřadů:

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 jejích 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 usnadní spojování databází.



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

Identifikaci se snaží řešit i do loňská novela 226/2002Sb. ZoEP 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.*

Paradoxně, „takové údaje“ jsou obsaženy 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 aj. situaci z technického ani zákonného hlediska nezlepší, vzniká nadbytečná identifikace. MPSV si sice se svým identifikátorem poradí snadněji, certifikovaní ale budou zakoušet uvedené nevýhody.

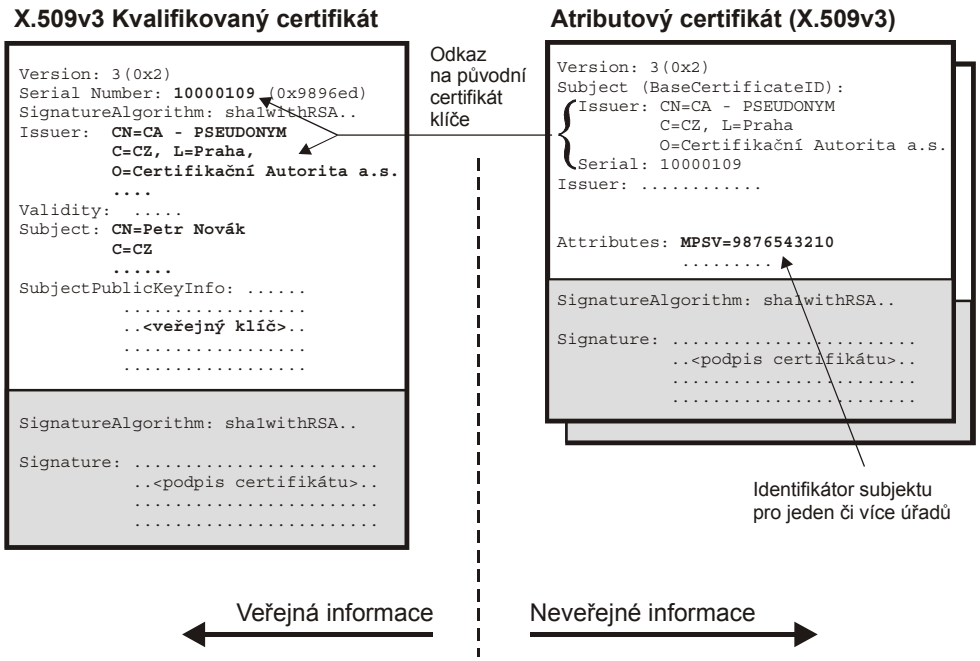
Přitom dostačuje, aby se vytvořilo „spojení“ mezi podpisovým certifikátem a identifikátory. ZoEP vytváření odkazů na podpisový certifikát nijak neomezuje. Následuje popis 2 takových metod.

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 certikaci. 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.

Atributový certifikát se odkazuje na podpisový certifikát, je podepsán CA, nejjednodušeji tou, jež vydala podpisový certifikát, obecně i jinou. Při vhodné certifikační politice vydávání kvalifikovaných certifikátů může být atributový certifikát použit i s pozdějšími podpisovými certifikáty, tj. být vystaven na delší dobu životnosti.

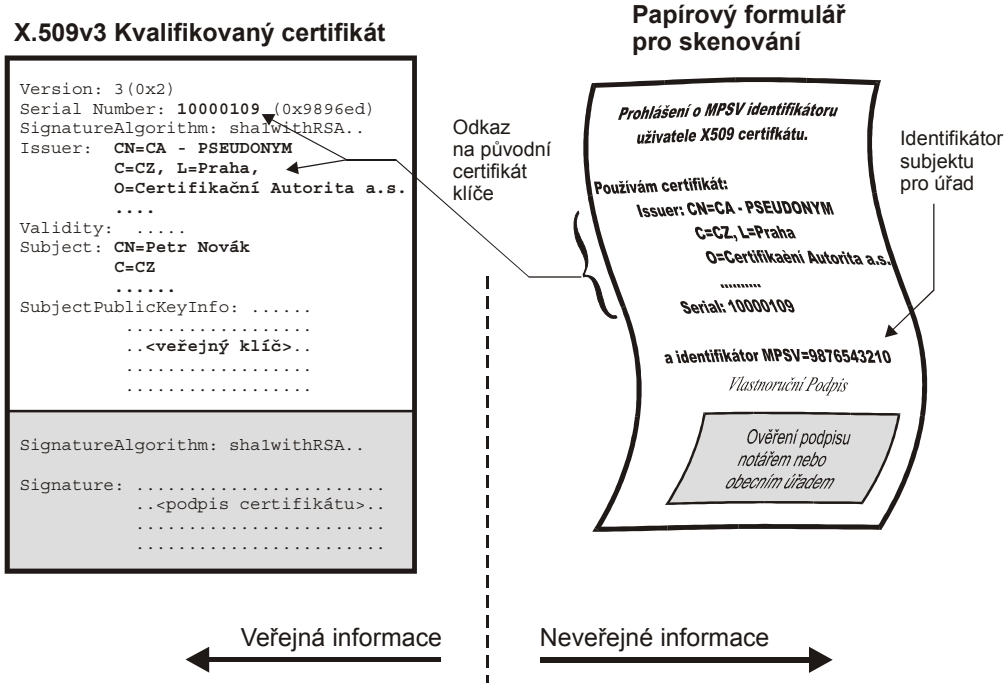
Atributové certifikáty zmiňuje již X.509v3 z roku 1997, do módy se dostávají až nedávno, viz čerstvé dokumenty ETSI 102 044 nebo RFC 3281.



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

Řešení 2 – Certifikace notáři

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, jež má opřeno o notářem ověřený podpis osoby, tj. silnější ověření, než se vyžaduje v 99% případech styku se státní správou. Metoda má 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 českém 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