

Zpráva o stavu e-podpisu

Vojtěch Kment, 26. listopadu 2002 – vyšlo 6.12.2002

Promotorem zavádění standardizovaného elektronického podpisu jsou všude na světě především orgány státní a veřejné správy. Komerční sféra se ke společným normám přidává průběžně. Před rokem vláda nařídila zřizovat elektronické podatelny, uběhlo půl roku od akreditace první certifikační autority, v létě bylo zahájeno přijímání elektronicky podepsaných formulářů na MPSV, většinou však v současnosti probíhá práce na projektech v pozadí. Je vhodná příležitost seznámit se situací a nezaspat.

Elektronický podpis provází smíšené komentáře. Jeho funkce i účel jsou dobře chápány v abstraktní rovině, v konkrétním provedení však jeho bezpečná implementace naráží na houšť právních předpisů a mezinárodních technických norem, jejichž zvládnutí leckoho odrazuje či přinejmenším způsobuje značné zdržení při osvojování. **Bez elektronického podpisu ale jednoduše další pokrok automatizace informačních systémů není možný.**

Snahou Vlády ČR je zřídit základní infrastrukturu elektronických podatelen na úřadech, z níž by se mohly odvíjet snahy o podporu dalších aplikací. Z proběhlých interview ministra Mlynáře plyne, že prvními aplikacemi by především měly být ty, jež jsou používány nejčastěji při jejich pravidelném opakování. Náměstek Úřadu pro veřejné informační systémy (ÚVIS) Michal Frankl říká, že za takové byly zjištěny zejména: přiznání k DPH, hlášení zdravotním pojišťovnám a správám sociálního zabezpečení (u malých firem), výpisy z obchodního rejstříku, výpisy z rejstříku trestů, potvrzení o bezdlužnosti, pozemkové výpisy z katastrálních úřadů, zadávání veřejných zakázek a podávání nabídek na ně. Komunikace běžného občana bývá více fragmentovaná, méně pravidelná, a kvůli jednorázovosti se zatím z pohledu samotného občana spíše nevyplácí.

První větší projekt přesto vznikl přímo pro občany. Stal se jím letos v létě zahájený provoz „Formulářů pro dávky státní sociální podpory“, jímž lze vyplnit, podepsat a podat cca. 14 formulářů (obr. 1). Projekt nechalo vypracovat Ministerstvo práce a sociálních věcí (MPSV) v rámci programu IS státní soc. podpory. Projekt sklídl rozporuplné ohlasy, protože sociálně slabší občané nemívají prostředky na provoz počítače a kvalifikovaného certifikátu. Přílohy k žádostem je též zatím nutné poslat běžným způsobem.

Formuláře lze ale použít i v dalších dvou režimech, totiž jen vytisknout, nebo vyplnit a vytisknout. Problém listinných příloh je obecný a dokud nebudou elektronizovány veškeré agendy ve veřejné správě, ale i jiných třetích stran (např. u firem - zaměstnavatelů), vždy k němu může dojít. Konečně, na některé dávky, jako jsou např. přídavky na dítě, popř. porodné, mají nárok i ti občané, u nichž vlastnictví a užívání počítačů připadá do úvahy.

Projekt může sloužit i jako příklad, že aplikace s e-podpisem lze vytvořit.

Zatím bohužel nelze poskytnout praktické zkušenosti z provozu. Systém vyžaduje přítomnost zvláštního identifikátoru MPSV v certifikátu (probíráno ve zvláštním článku), bez něhož příjem formuláře odmítne. Tento identifikátor si nechalo vložit do certifikátu zatím asi 110 osob, zatím však nikdo z nich o žádnou dávku nepožádal.

obr. 1 Formuláře dávek státní sociální podpory jsou první „strukturovanou“ aplikací, při níž lze veřejné správě podat elektronicky podepsanou žádost

Zavádění e-podpisu závisí jednak na každém úřadu a instituci zvlášť, jednak na kvalitě společné koordinace. Úřady se často zdráhají začít využívat e-podpis, neboť si nejsou jisty jeho bezpečností, právní průkazností elektronických dokumentů, popř. poukazují na nejasnou či chybějící legislativu v jejich případě, problémy dlouhodobé archivace, možnost falšování současných podpisů po pokroku technologie apod. ÚVIS a úřady si tak mezi sebou přehazují horký brambor odpovědnosti za to, čím naplní je které vyvstalé problémy řešit. Jediným dalším projektem, o němž je obecně známo, že probíhá, je projekt formulářů na Ministerstvu financí pro podání příznání DPH, daně silniční, daně z nemovitosti, a hlášení o vyplacených nezdaněných částkách, jež navazuje na větší projekt správy daní. Pilotní provoz lze očekávat během první poloviny roku 2003. Projekty dalších daňových podání budou hotovy až po uspokojivém vyřešení některých zmíněných problémů, nejdříve v roce 2004.

Rozvoj e-podpisu ovšem probíhá na více frontách zároveň, jejich stav je probrán ve zbytku článku.

Zákony a předpisy

Český zákon o elektronickém podpisu 227/2000Sb. byl přijat již před dvěma lety. Musel si rok počkat na vytvoření odboru na čerstvě vzniklém Úřadu pro ochranu osobních údajů (ÚOOÚ), jenž k němu po své stabilizaci loni v říjnu vydal prováděcí vyhlášku 366/01Sb. Od ní se odvinul proces akreditace, dovršený úspěšným schválením První certifikační autority, a.s. (ICA) letos v březnu, jež od té doby může a vydává kvalifikované certifikáty použitelné ve státní a veřejné správě.

Před rokem vyšlo nařízení vlády 304/01Sb. pro zavádění elektronických podatel, jež je dále rozvíjeno předpisy ÚVIS, jež je zákonem 365/2000Sb. zmocněn ke stanovování technicko-organizačních standardů ICT pro oblast veřejné správy. Po novém roce 2003 se ÚVIS i výše zmíněný odbor ÚOOÚ stanou i s dosavadními pravomocemi součástmi nového ministerstva informatiky.

Letos v létě proběhla i malá novelizace zákona o elektronickém podpisu 226/2002Sb., především upřesňující podmínky používání e-podpisu v kontextu jiných zákonů a administrativních agend. Dobře vystavěným aplikacím a produktům by průběžná adaptace na změny neměla zásadně vadit.

Zákony a předpisy v SR

V SR byl letos na jaře přijat zákon 212/2002 z.z. "O elektronickom podpise", doprovazený na konci září sérií šesti vyhlášek 537 až 542/2002 z.z.. Stejně jako český je inspirován doporučeními EU, celkově je však jeho vyznění výrazně tužší a méně liberální. To teoreticky přispívá k vyšší bezpečnosti uživatelů, prakticky však může být téměř nemožné předpisům vyhovět. Slovenský zaručený elektronický podpis je v zákoně o tři a ve vyhláškách pak ještě o další dva stupně zaručenější než český. Zejména vyhláškou stanovené zahrnutí tzv. podpisových politik a podpisových údajů nemá dosud oporu v používaných technických standardech. Velmi sporná je vyhláška 539/2002 z.z., jež se má zabývat bezpečností prostředků a produktů pro vytváření elektronických podpisů, místo toho však provádí výčet (navíc často nesmyslných) funkčních vlastností a připomíná prospekt některého produktu. Např. požadavek na zálohování (soukromého) klíče je vysloveně nebezpečný.

Naopak kladem slovenských předpisů je třeba stanovení formátů elektronicky podepsovaných dokumentů (vše otevřené standardy), a požadavek na to, aby neobsahovaly aktivní součásti. Slovenský zákon je místy přesnější, než jeho o dva roky mladší česká obdoba, všechny předpisy dohromady však rovněž obsahují značné množství vágností, bohužel prostor článku neumožňuje ani výčet upozornění na ně. Protože vyhláskové tabulky podpisových schemat jsou totožné jako v Česku, čistě technicky budou asi četné e-podpisy kompatibilní, zatímco mohou vzniknout právní problémy s jejich vzájemnou uznatelností.

Elektronické podatelny

Elektronické podatelny jsou vstupní přijímací body organizací veřejné správy pro elektronicky podané a podepsané zprávy a dokumenty, jako potenciálně plnohodnotné náhrady klasického písemného podání.

Povinnost zřizovat podatelny vláda nakázala výše zmíněným nařízením, jež stručně řečeno nakazuje zřídit si schránku(y) elektronické pošty, oznámit veřejně její adresu jako podatelny a starat se o ni. Letos v červnu ÚVIS vyhlášku rozvedl a vydal standard ISVS 016/01.01 pro elektronické podatelny. Oba dokumenty jsou považovány za vágní a jistě prodělají další vývoj.

Elektronická podatelna ala ÚVIS odpovídá v minimální verzi poštovnímu klientu internetu SMTP/POP3 s mírně rozšířenými funkcemi. Poštu lze přijímat on-line i off-line (jen u malých obcí), každou došlou zprávu je třeba zarchivovat, prověřit na výskyt virů, ověřit platnost podpisu i platnost souvisejícího kvalifikovaného certifikátu včetně kontroly zneplatnění, odeslat zpět potvrzení o příjmu zprávy a zprávu předat k dalšímu vyřízení v organizaci podle jejich vnitřních předpisů.

Z technických parametrů podatelna musí přijímat dokumenty ve formátech .txt a .html, podporovat MIME a S/MIME, a podpisová schémata s algoritmy RSA či DSA ve spojení s SHA1, dobrovolně i jiné. Podatelna musí podporovat i příjem na disketách. Standard definuje i organizační zázemí podatelny a atestační podmínky produktů podatelen.

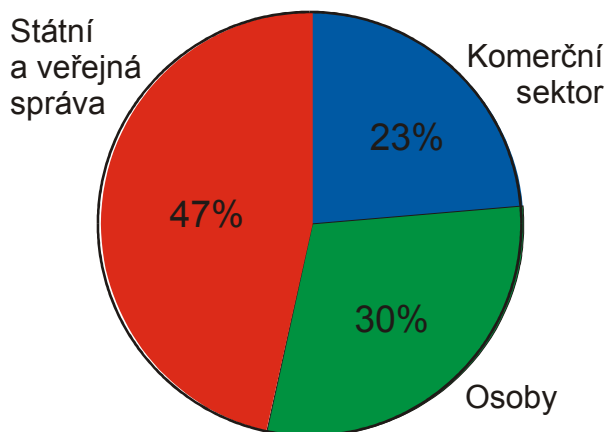
Předpisy ale nestanoví povinnost centrálně hlásit zřízení podatelny, takže nelze vytvořit „Žluté stránky elektronické veřejné správy“. Nelze ani říci, kolik elektronických podatelen v současnosti skutečně existuje, ani prověřit, jak reálně fungují.

Akreditované kvalifikované certifikáty

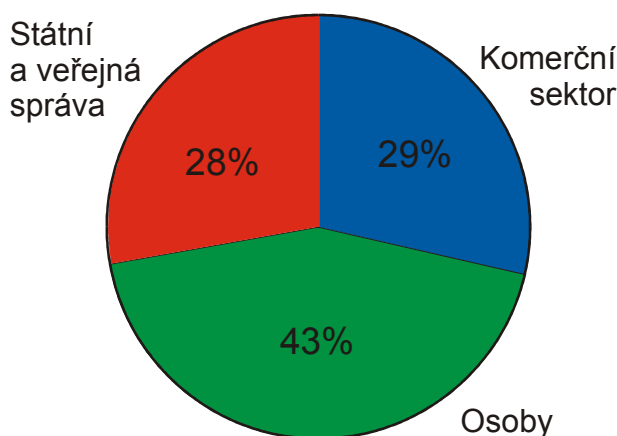
Za půl roku trvání akreditace bylo vydáno skoro 600 kvalifikovaných certifikátů, zjevně především průkopníkům a fandům technologie e-podpisu. V oblasti veřejné správy získalo kvalifikovaný certifikát pro jednoho či více pracovníků cca. 80 organizací. Z toho lze přeci jen soudit na počet existujících

„aktivních“ podatelen. Existují ovšem i další podatelny, vzniklé ještě podle vládního nařízení, jež si zatím kvalifikovaný certifikát nepořídily a jež by jej nyní již správně míti měly.

Překvapivě mnoho certifikátů si objednaly komerční firmy. Kvalifikovaný certifikát si jich pořídilo stejné množství jako úřadů, ačkoliv jim zákon ani předpisy povinnost zřizovat podatelny a tyto certifikáty nenařizují. Další zhruba 1/3 registrací je soukromými osobami, i když je zjevné, že minimálně polovina z nich opět pochází z firem, jež se zatím nechtěly zatěžovat dokládáním firemních náležitostí, ale pohlát si s technologií. Stav ilustrují obr. 2 a obr. 3.



obr. 2 Rozložení certifikovaných dle počtu osob



obr. 3 Rozložení certifikovaných dle počtu různých právních subjektů

Alarmující je, že přes 20% certifikovaných získává certifikát na dva a více pokusů. To spadá na vrub jak chybějícím znalostem uživatelů, tak i nedostatečné technické podpoře od I.CA. Registrační zmatky pak způsobují i to, že není vždy dodržována certifikační politika I.CA. Např. pole O má obsahovat přesný název organizace dle obchodního rejstříku, existují však např. kvalifikované certifikáty s „O=PVT“ bez uvedení formy společnosti. Též v případě organizací veřejné správy toto pole není vyplněno vždy zcela ideálně.

Komerční sektor

Firmy a podniky technologické obdoby elektronického podpisu již dlouho používají, ale spíše v proprietární podobě. Aplikace sahají od vnitrofiremních poštovních systémů, přes objednávkové systémy až po telebankingy. V nadcházející éře by tyto systémy měly adaptovat nebo doplnit na standardy „veřejného“ e-podpisu, poskytujícího vysokou bezpečnostní úroveň, širokou vzájemnou interoperabilitu subjektů navzájem mezi sebou a zasazení do obecného právního řádu.

Pro úspěch e-podpisu bude důležité i další zlepšení služeb bank. Vždyť jedna z výhod e-transakcí je rychlost, jež dosud v ČR vážně na pomalosti plateb přes clearing ČNB. Nejen e-obchod, ale i řada veřejných agend bude potřebovat přijímat platby (místo kolků). Banky nemusí e-podpisu jen pomáhat, ale i samy ho využít pro podpisy příkazů k platbě, jako úplný, nebo doplňkový prostředek ochrany telebankingu, používající veřejně prověřenou technologii e-podpisu.

Závěr

Akreditovaná certifikační autorita vydává kvalifikované certifikáty, použitelné pro e-podpisy i ve veřejné správě. Úřady jsou ve fázi zavádění elektronických podatelů pro univerzální agendu. První formulářovou aplikací se staly dávky sociální péče. Běží projekty daňových formulářů. Další projekty jsou zřejmě ve fázích úvah či přípravy. O elektronický podpis jeví zájem četné soukromé subjekty. Brzdou rozvoje je především nedostatečně rozšířené a osvojené know-how o e-podpisu, potřebné pro poučené řešení nejasností předpisů, a vyšší důvěru v technologie.

Autor je konzultant elektronického podpisu

<http://www.vkc.cz>