Biometrický podpis – mýty a fakta

V médiích i na odborných konferencích se poslední dobou stále častěji setkáváme s propagací dynamického biometrického podpisu, který v sobě kloubí přirozenost a jednoduchost podpisu vlastnoručního při zachování vysoké míry bezpečnosti a důvěryhodnosti podpisu elektronického.

Dynamický biometrický podpis (dále též DBP) se nepokrytě zaměřuje na odvětví, kde panuje dlouhodobá averze vůči používání elektronického podpisu na bázi certifikátů, a na oblasti, kde je vyžadována dlouhodobá platnost a ověřitelnost digitálních dokumentů (orgány veřejné moci, zdravotnictví, bankovnictví apod.), tedy na odvětví, kde se zpravidla ze zákona vyžaduje užití zaručeného, nebo dokonce uznávaného elektronického podpisu.

Skutečnost, že DBP splňuje požadavky platné legislativy na zaručený elektronický podpis, je uváděna jako nezvratný fakt, který však nebývá podložen žádnými objektivními technickými nebo právními argumenty a zakládá se většinou pouze na subjektivním názoru. Pojďme se ale na výhody i nevýhody této nesporně zajímavé technologie podívat střízlivým okem platné legislativy a zhodnotit důsledky jejího možného praktického využití.

Dynamický biometrický podpis vs. zákon o elektronickém podpisu

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů [1], který je transpozicí směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy [2] (dále jen „Směrnice"), definuje v § 2 písm. a) elektronický podpis jako „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě". Zaručeným elektronickým podpisem se pak podle zákona č. 227/2000 Sb. rozumí „elektronický podpis, který splňuje následující požadavky:

1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat".

Na rozdíl od „obyčejného" elektronického podpisu, kde postačuje připojení či logické spojení s jinými elektronickými daty, a elektronický podpis tak slouží jako metoda ověření pravosti, u zaručeného elektronického podpisu musí být mimo jiné splněno, že podpis je jednoznačně spojen s podepisující osobou a umožňuje zjistit její totožnost. Z těchto definic vyplývá, že pro zaručený elektronický podpis je nezbytné použití takové technologie, která zaručuje existenci jednoznačného spojení mezi zaručeným elektronickým podpisem a podepisující osobou.

Posouzení shody či neshody dynamického biometrického podpisu s výše uvedenými požadavky na zaručený elektronický podpis je samozřejmě přímo závislé na definici DBP, resp. na požadavcích na něj kladených. Pokud jej budeme definovat v souladu s dostupnými materiály o DBP jako „elektronický záznam ručně psaného podpisu zahrnující grafickou podobu podpisu a stanovené biometrické charakteristiky specifické pro autora podpisu", pak

v této podobě požadavky zákona zjevně nenaplňuje. Biometrické charakteristické znaky jsou sice popisovány jako „biometrická stopa, která je unikátní pro každého jednotlivce a nemůže být padělatelem reprodukována", verifikace DBP však spočívá v „porovnání biometrického vzorku v databázi podpisů daného uživatele s provedeným podpisem na shodu ve stanovených tolerancích".

Právě nastavení tolerancí (parametrů FAR – FalseAcceptanceRate/četnost chybného přijetí a FRR – FalseRejectionRate/četnost nesprávného odmítnutí), které pro faktickou reálnou použitelnost dané technologie nemohou být ani blízké nule (rozptyl měřených hodnot je poměrně velký i u normálních, zdravých jedinců, technologie navíc musí počítat i s lidmi nemocnými, nervózními nebo motoricky indisponovanými), prakticky vylučuje jednoznačné spojení mezi podpisem a podepisující osobou a jeho stoprocentní ověřitelnost.

Aby mohl být DBP považován za zaručený elektronický podpis, bylo by nezbytné určit, jakým způsobem budou naplněny všechny požadavky zákona na zaručený elektronický podpis:

- Jednoznačné spojení s podepisující osobou – musí být jisté, že daný podpis mohla vytvořit pouze jedna konkrétní osoba. Sám o sobě tento požadavek DBP nenaplňuje. Porovnání vytvořeného DBP s podpisovým vzorem v předpokládaném úložišti podpisových vzorů (referenční databáze) naráží na skutečnost, že v současné době DBP dosahují dle dostupných zdrojů zhruba 95% spolehlivosti při ověřování shody aktuálního podpisu s podpisovým vzorem. Nelze tedy vyloučit pokus o vědomé napodobení statických a dynamických vlastností podpisu určité osoby ani nechtěnou shodu dvou či více podpisů různých osob.

  V případě DBP není použit žádný prvek, který je zcela jedinečný pro podepisující osobu a který by byl obdobou soukromého klíče při vytváření zaručeného elektronického podpisu.

- Umožnění identifikace podepisující osoby ve vztahu k datové zprávě – tj. zajištění neodmitnutelnosti odpovědnosti – podepisující osoba nemůže popřít, že určitou datovou zprávu podepsala. Musí být tedy zajištěno, aby bylo možné prokázat, že podpis se vztahuje ke konkrétní datové zprávě. Splnění tohoto požadavku nelze v současnosti zajistit jinak než použitím k tomu určených speciálních kryptografických metod – hashovacích funkcí a šifrování. V případě jejich užití ovšem DBP ztrácí proklamovanou neomezenou platnost a nezávislost na přirozeném slábnutí běžně užívaných kryptografických algoritmů.

- Vytvoření a připojení k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou; podepisující osoba je dle zákona povinna zacházet s prostředky jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití. V případě zaručeného elektronického podpisu má data pro vytváření elektronických podpisů (tzv. soukromý klíč) v držení pouze podepisující osoba a odpovídá za jejich náležité používání a ochranu před zneužitím; za prostředek pro vytváření elektronických podpisů se zde považuje technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů (např. čipová karta nebo podepisovací aplikace).

  V případě DBP lze za tento prostředek označit nejspíše tablet, na němž je podpis vytvořen, případně pero (tzv. smartpen), kterým je vytvořen, a příslušný obslužný software. Lze předpokládat, že takovýto prostředek bude častěji v držení příjemce „podpisu" (např. banka, na jejímž tabletu klient vytváří podpis) než pod výhradní kontrolou podepisující osoby (která by v opačném případě musela potřebný prostředek nosit stále u sebe), což vzhledem k reálnému riziku neoprávněného zachycení a okopírování biometrických charakteristických znaků a k jednoduchosti jejich zneužití představuje významné bezpečnostní riziko.

- Připojení podpisu k datové zprávě, ke které se vztahuje, takovým způsobem, že je možno zjistit jakoukoli následnou změnu dat – bez užití kryptografických funkcí zmíněných v předchozích odstavcích není DBP sám o sobě žádným nezpochybnitelným způsobem připojen k datové zprávě, ke které se vztahuje. Případná změna dat nemá na podpis žádný vliv.

O čem se příliš nemluví

Přestože je mezi výhodami DBP prezentována přirozenost úkonu vytvoření biometrického podpisu, ověření tohoto podpisu již tak snadné a přirozené není. K ověření elektronického podpisu postačuje spoléhající se straně veřejný klíč podepisující osoby, který je téměř vždy ve formě certifikátu připojen přímo k vlastnímu podpisu, případně všichni kvalifikovaní poskytovatelé certifikačních služeb provozují veřejné seznamy vydaných kvalifikovaných certifikátů.

Naproti tomu ověření biometrického podpisu vyžaduje porovnání připojených biometrických dat s nějakou formou důvěryhodného vzoru. Tento základní princip, na kterém je ověřování založeno, přímo vede k nutnosti vybudování referenční databáze biometrických vzorků, kde by každý uživatel DBP musel být předem zaregistrovaný a kde by byly uloženy základní biometrické charakteristiky jeho podpisu. Pokud by měl být DBP používán v oblasti orgánů veřejné moci, je pravděpodobnější vybudování celostátní referenční databáze než několika menších oddělených databází pro jednotlivé agendy, do kterých by se uživatelé museli registrovat zvlášť. Centralizované shromažďování takovýchto extrémně citlivých a potencionálně zneužitelných dat by však oprávněně mohlo vyvolat nedůvěru veřejnosti.

V této souvislosti je třeba upozornit i na ekonomický aspekt plošného zavedení DBP. Samotné vybudování referenční databáze by se vzhledem k nezbytnosti velmi přísných bezpečnostních opatření neobešlo bez významných investic, které by dále vzrostly o náklady na správu a řízení přístupu k databázi, neboť každé ověření DBP by vyžadovalo přímé spojení do této databáze, z povahy přenášených dat pravděpodobně přes zabezpečený kanál.

Dalším problematickým aspektem je relativně snadné podvodné získání podpisových dat. V případě elektronického podpisu založeného na kvalifikovaném certifikátu má data pro vytváření elektronických podpisů (tzv. soukromý klíč) v držení pouze podepisující osoba a odpovídá za jejich náležité používání a jejich ochranu před zneužitím. Při správném užívání si je podepisující osoba vždy vědoma, že se soukromý klíč používá a že se elektronicky podepisuje. Získat neoprávněně soukromý klíč cizí osoby je tak za běžných okolností takřka nemožné.

Neoprávněné získání charakteristických biometrických dat je oproti tomu jednodušší a lze jej často provést i bez vědomí podepisující se osoby. Je to umožněno právě podobností úkonu biometrického podpisu s podpisem vlastnoručním, který se děje v běžném životě takřka automaticky a bez adekvátní míry opatrnosti. V kombinaci s výše popsanou praktickou neexistencí možnosti výhradní kontroly nad prostředkem pro vytváření podpisu (tabletu, elektronického pera) je nasnadě, že získání podpisu, a tedy i shromažďovaných biometrických charakteristik vytipované osoby bez jejího vědomí (nebo s jejím vědomím, ale pod nepravdivou záminkou) pomocí např. záměrně upraveného tabletu bude v porovnání s podpisy založenými na infrastruktuře veřejných klíčů (PKI) relativně jednoduché.

S předchozím odstavcem úzce souvisí další poměrně závažný bezpečnostní nedostatek – nelze revokovat podpisová data. Pokud dojde ke kompromitaci dat pro vytváření elektronických podpisů (soukromého klíče), lze ho snadno a rychle pomocí standardních a dobře známých nástrojů zneplatnit a v případě potřeby si vygenerovat klíč nový. Pokud dojde k neoprávněnému získání základních biometrických charakteristik libovolné osoby, ať již podvodem pomocí způsobu popsaného výše nebo jejich zcizením z referenční databáze biometrických vzorků, lze jen velmi obtížně zabránit jejich zneužití. Napadený uživatel (pokud se o této skutečnosti vůbec dozví) se může pokusit vědomě změnit svůj podpisový vzor, což však do jisté míry jde proti základní myšlence sběru a porovnávání vůči neovlivnitelných biometrických charakteristik osoby a nepochybně by to obnášelo velmi zdlouhavou a nesnadnou fázi učení a zvykání si na jiný podpis.

Shrnutí a možná využití DBP

Jak vyplývá z výše uvedeného, dynamický biometrický podpis nelze bez dalších dodatečných opatření považovat za zaručený elektronický podpis ve smyslu § 2 písm. b) zákona č. 227/2000 Sb. Obdobný závěr učinilo ve svém stanovisku k této problematice i ministerstvo vnitra jakožto ústřední správní orgán státní správy pro oblast elektronického podpisu a gestor zákona o elektronickém podpisu. Pokud by tato technologie měla být plošně zavedena za účelem náhrady nebo alternativy k zaručenému elektronickému podpisu, bylo by nutné vyřešit řadu jejích problematických aspektů. Jedná se zejména o finanční náklady, které by s sebou toto plošné zavedení dynamického biometrického podpisu neslo (pořízení tabletů a per, vybudování celostátní referenční databáze biometrických vzorů), o snadné neoprávněné získání charakteristických podpisových dat a o faktickou neexistenci jednoduchého postupu revokace kompromitovaných podpisových dat.

Neposlední problém by mohla představovat oblast přeshraničního uznávání elektronických podpisů, neboť ani evropská legislativa s užitím jiné technologie než PKI v praxi nepočítá.

Přestože je tento článek k dynamickému biometrickému podpisu spíše kritický, bezesporu má tato technologie své využití. Jen je potřeba ji správně aplikovat. Protože je v oblasti elektronického podpisu z pochopitelných důvodů kladen maximální důraz na jedinečnost podpisových dat a tím na nezpochybnitelnost propojení podepisující osoby a jejího podpisu, což samotná technologie DBP nesplňuje, jedním z možných využití by mohlo být zkombinování technologie DBP s léty ověřenými a bezpečnými nástroji PKI.

Lze si např. představit použití DBP jakožto náhrady autentizace k přístupu k soukromému klíči podepisující osoby, kdy by zůstalo zachováno vytváření zaručeného elektronického podpisu v souladu s dnešními zvyklostmi, ale místo zadávání PINu před každým použitím soukromého klíče by se podepisující osoba autentizovala pro někoho možná přirozenějším a pohodlnějším způsobem právě pomocí DBP. Vzor podpisu by mohl být v zašifrované podobě uložen přímo na prostředku pro bezpečné vytváření elektronického podpisu, čímž by byla zajištěna jeho trvalá ochrana proti zneužití a odpadla by nutnost vytváření drahé a kontroverzní celostátní databáze podpisových vzorů. Za vhodnější ale považuji využití DBP obecně v rovině autentizačního nástroje, ekvivalentního např. k dnes velmi rozšířeným čtečkám otisků prstů.

Jaroslav Tománek
tomanek@ica.cz

Ing. Jaroslav Tománek

Absolvent Fakulty jaderné a fyzikálně inženýrské ČVUT v Praze (Bc.) a Provozně ekonomické fakulty ČZU v Praze (Ing.). Působil na Ministerstvu vnitra ČR, kde se zabýval legislativními i technickými aspekty elektronického podpisu včetně zastupování ČR v pracovních skupinách při Evropské komisi. Dnes je zaměstnancem společnosti První certifikační autorita, a.s.

POUŽITÉ ZDROJE

[1] Česká republika. *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)* [online]. 24 s. [cit. 2011-12-28]. (PDF). Dostupné na WWW: <http://www.mvcr.cz/soubor/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

[2] Evropská unie. *Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy ze dne 13. prosince 1999* [online]. 15 s. [cit. 2011-12-28]. (PDF). Dostupné na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:CS:PDF>.

[3] KODL, J., SMEJKAL, V. Jednofaktorová autentizace na bázi dynamického biometrického podpisu. In konference *Datové schránky – rok druhý*, Praha, 18. května 2011. [online]. 34 s. [cit. 2011-12-28]. (PDF). Dostupné na WWW: <http://www.dataschranky.cz/2011/download/prezentace/kodl.pdf>.

[4] PETERKA, J. *Elektronický podpis na rozcestí*. [online] [cit. 2011-12-28]. Dostupné na WWW: <http://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti>.

[5] VALÁŠEK, M. Nahradí dynamické biometrické podpisy ty současné elektronické? [online] [cit. 2011-12-28]. Dostupné na WWW: <http://www.lupa.cz/clanky/nahradi-dynamicke-biometricke-podpisy-ty-soucasne-elektronicke>.