# BEZPEČNOSTNÍ PROSTŘEDKY PRO ELEKTRONICKÝ PODPIS

**Miloslav Špunda**


## Anotace

Příspěvek se zabývá technickými prostředky pro podporu užití elektronického podpisu v prostředí nemocničního informačního systému (NIS). Je diskutováno uložení šifrovacích klíčů a certifikátů s respektováním principů PKI (Public Key Infrastructure) včetně hardwarového řešení tohoto problému a problému autentizace uživatele (bezpečnostní prostředky).



## Klíčová slova

*Elektronická zdravotnická dokumentace, nemocniční informační systém, elektronický podpis, certifikovaný bezpečnostní předmět*


## Úvod

Tento příspěvek je určen kvalifikovaným koncovým uživatelům v prostředí, kde se užívá elektronický podpis. Toto prostředí má specifické znaky v nemocničních informačních systémech, kdy po přechodu na elektronické vedení zdravotnické dokumentace je nutné při respektování platného právního rámce splnit zásady informační bezpečnosti. Současně však přichází požadavek na co nejmenší zátěž uživatele (lékaře, zdravotnického personálu) souvisící s užíváním elektronického podpisu.

Při užití elektronického podpisu má zásadní význam autentizace uživatele, která musí zajišťovat ochranu před zneužitím a zaručovat tak pravost elektronického podpisu na elektronickém dokumentu (např. lékařské zprávě). Autentizaci uživatele i užití technik pro přidání elektronického podpisu k dokumentu podporují bezpečnostní prostředky, které budou dále popsány.

Smyslem příspěvku je zároveň popsat rizika spojená s užitím elektronického podpisu. Koncový uživatel v NIS má rizika plynoucí u užití elektronického podpisu znát včetně uživatelské znalosti příslušných bezpečnostních prostředků. Jsou naznačeny i možnosti použít přidělené technické prostředky pro elektronický podpis i mimo prostor NIS k podepisování libovolných dokumentů.

Problematika bezpečnostních prostředků souvisících s elektronickým podpisem se tedy rozpadá na dvě části:

- prostředky pro autentizaci uživatele (který bude elektronický podpis užívat)
- prostředky pro uložení šifrovacích klíčů a certifikátů (čipová karta nebo USB token) společně nazývané **bezpečnostní předměty**

*Poznámka: V dalším budeme pro bezpečnostní předměty užívat společné označení* **token**.

### Metody autentizace

Uživatel elektronického podpisu má svou vlastní identitu (která se ověřuje autentizací před použitím tokenu) a tzv. digitální ID (privátní a veřejný klíč s certifikáty), které se užívá při podepisování dokumentu. Digitální ID uživatele je uloženo na tokenu, požadavky na jeho bezpečnost se budeme zabývat v dalším. Smyslem užití tokenu je zvýšit bezpečnost uložením zejména privátního šifrovacího klíče mimo HDD počítače nebo ještě lépe úplně zamezit jeho přeneseni mimo token během podepisování dokumentu.

Ověření identity uživatele před použitím tokenu pro elektronický podpis spadá do obecnější oblasti ochrany dat. S podobným problémem se např. setkáváme při ověření oprávnění spustit operační systém počítače.

Klasickým způsobem je autentizace uživatele pomocí jména a hesla. Jedinou ne příliš velkou překážkou při pokusu narušit bezpečnost je zde heslo. Heslo lze však uhádnout (se snadno dostupnou SW podporou), odpozorovat (web kamery, digitální fotoaparáty, aj.), odchytit na úrovni klávesnice (rezidentní program zaznamenávající všechny stisknuté znaky), přitom existují i další možnosti jak heslo neoprávněně získat.

Odolnost hesla lze zvýšit více způsoby, např. předpisem pro tvorbu hesla (délka, typ znaků) nebo nepoužíváním statických hesel. Možná je i kombinace užití hesla zároveň s tokenem (dvoufaktorová autentizace). Tento způsob je řádově bezpečnější. Možná jsou i další řešení pomocí bezpečnostních předmětů jako snímačů otisků prstů, analyzátorů DNA a dalších, které využívají biometrických údajů o uživateli. Dalšími možnostmi jsou autentizační kalkulátory generující jednorázová přístupová hesla či užití jednorázových kódů ve formě SMS zprávy.

### Obecné požadavky na bezpečnostní předměty

Těmito požadavky se jsou obvykle míněny mechanické a ergonomické vlastnosti tokenů, v případě použití v NIS však volbu typu tokenu a jeho vlastností obvykle koncový uživatel nemůže ovlivnit. Je součástí návrhu technického řešení elektronické zdravotní dokumentace. Splněním některých požadavků lze navíc rozšířit oblasti užití (např. karty též vstupy do budov a další služby).

- Z vlastností tokenů podle nichž lze posoudit vhodnost jejich užití uveďme:
- odolnost tokenu vůči vnějším vlivům (mechanická odolnost (náraz), statická elektřina, elektromagnetické pole, vlhkost vzduchu, aj.)
- odolnost konektorů a čtecího zařízení (u čipových karet) (uvádí se např. garantovaný počet zasunutí/vysunutí tokenu)
- mobilita (je dána skutečností, jaký HW a SW je pro daný token potřebný, u karet navíc čtečka)

Z požadavků rozšiřujících možnosti užití tokenu lze v případě čipových karet uvést:

- personalizaci (jméno držitele, fotografie, čárový kód a další)

- magnetický proužek (karta má kromě smart čipu též magnetický proužek pro např. docházkový systém, aj.)

Uvedené výhody obvykle USB token neumožňuje využít.

**Bezpečnostní požadavky na bezpečnostní předměty (tokeny)**

Bezpečnostních požadavků na tokeny je celá řada, zde probereme jen nejdůležitější včetně možných způsobů jejich splnění. Z uživatelského hlediska je důležitý zejména způsob zacházení s heslem tokenu a způsob manipulace s digital ID uživatele(vložení, event. export do/z tokenu).

**Autentizace uživatele vůči tokenu** má několik způsobů řešení. Obecně heslo (sada alfanumerických znaků) má z hlediska bezpečnosti větší váhu než pouhý PIN (jen číslice), což je dáno velkým řádovým rozdílem možných kombinací. Při chybném zadání hesla (překročení povoleného počtu pokusů o zadání) dojde k zablokování tokenu s následujícími možnostmi:

- automatické smazání všech uložených dat
- možnost pouze ručního smazání pomocí utility
- zadání dalšího kódu PUK (Personal Unblocking Key)

Zadání PUK kódu může umožnit buď další sadu pokusů nebo častěji dovolí nové nastavení PIN. Přitom dvojici PIN/PUK může vlastnit pouze jedna osoba nebo PUK může znát administrátor systému (pokud nevadí, že při novém nastavení hesla nejsou data chráněna vůči osobě administrátora).

Setkáváme se též se systémy, kde po překročení povoleného počtu zadání hesla dojde automaticky ke znehodnocení tokenu a je třeba uživateli vydat nový (s celou procedurou pro převzetí tokenu). Obecně platí nepřímá úměrnost mezi bezpečností a pohodlím uživatele (i cenou).

**Způsob ověření hesla** po zadání na klávesnici též spolurozhoduje o bezpečnosti celého systému. Zde záleží na tom zda je užit pouze paměťový token či procesorový token. V prvním případě musí zašifrování hesla a porovnání provést SW počítače, což nelze z hlediska bezpečnosti doporučit.

**Bezpečnostní certifikace** je jedinou možností, jak zaručit fyzickou bezpečnost tokenu. Je vodítkem pro volbu tokenu pro danou aplikaci elektronického podpisu v informačním systému. Setkáme se obvykle se dvěma základními bezpečnostními certifikacemi, americkou normou FIPS (vydána NIST – National Institute of Standards and Technology) a evropskou normou ITSEC (Information Technology Security Evaluation Kriteria). V návrhu elektronického podpisu v NIS ve VFN bylo užito certifikace podle FIPS 140-2 Level 2 (přibližně odpovídá ITSEC E4 High).

Na typu certifikace záleží méně, podstatné je, že bez jejího užití nelze o garanci bezpečnosti tokenu dobře hovořit.

**Import/export digitálního ID** při práci s tokenem je možný více způsoby, významně však ovlivňuje bezpečnost elektronického podpisu. Jde zejména o dvojici šifrovacích klíčů (privátní, veřejný), import kvalifikovaného certifikátu

je menším problémem. Z hlediska bezpečnosti by měl token mít následující vlastnosti:

- klíč nelze z tokenu exportovat¨
- klíč je užíván pouze v tokenu, při šifrování/dešifrování jej neopouští
- pár klíčů lze na tokenu vytvořit

Z hlediska způsobu vytvoření a uložení klíčů RSA algoritmu jsou tyto základní možnosti:

- RSA pár je vytvořen přímo na tokenu (nejvyšší bezpečnost), nevýhodou je nemožnost vytvořený pár klíčů exportovat (záloha při ztrátě tokenu)
- RSA pár je vytvořen pomocí SW, který je příslušenstvím tokenu, následně se do tokenu nahraje (s možností vytvoření zálohy), podmínkou je „bezpečné" PC, takže proces proběhne důvěryhodně
- RSA pár je vytvořen nespecifickým SW vůči tokenu a pomocí utility nahrán (nejméně bezpečné)

*Poznámka: Některé bezpečnostní systémy dovolují při dodržení standardů PKCS (Public Key Cryptographic Standards) manipulaci s digitálními identitami, tedy vyměňovat a importovat do tokenu certifikáty, šifrovací klíče event. další data užívaná bezpečnostním systémem.*

### Možnosti technického a administrativního řešení v NIS

Implementace elektronického podpisu do NIS (obvykle již existujícího a v provozu) obvykle nepředpokládá užití bezpečnostních předmětů mimo tento systém. Organizace vydávání kvalifikovaných certifikátů oprávněným uživatelům je vázána přesným administrativním postupem, totéž se týká jejich zneplatnění při ztrátě kontroly nad užíváním bezpečnostního předmětu (tokenu).

Uveďme v závěru přehledně hlavní kroky při manipulaci s tokeny, jak mohou být řešeny v rámci NIS.

Proces vydání tokenu a přidělení kvalifikovaného certifikátu se děje v rámci administrativního procesu, kdy si pracovník v rámci úpravy pracovních povinností založí prostřednictvím webového rozhraní účet u CA (certifikační autority dostupné v rámci intranetu NIS) a vyplní žádost o vydání kvalifikovaného certifikátu. Při generování žádosti je zároveň vytvořen klíčový pár (privátní/veřejný klíč) a nahrán do bezpečnostního předmětu. Žádost odesílaná CA je s užitím této dvojice klíčů digitálně podepsána.

CA vygeneruje na základě žádosti kvalifikovaný certifikát (QC) s příslušnými parametry, který poté oprávněný uživatel importuje do svého bezpečnostního předmětu (bezpečnostní předmět má identifikační číslo, které je zároveň s kvalifikovaným certifikátem uloženo do systému správy elektronických identit).

Důležitý je postup při zneplatnění kvalifikovaného certifikátu (na základě žádosti pověřeného pracovníka-personalisty zaslané CA). Důvodem může být,

jak jsme již uvedli, ztráta kontroly nad užíváním bezpečnostního předmětu (tokenu), zjištění nesprávných údajů o identitě oprávněné osoby, změna skutečností vedoucích k získání statutu oprávněné osoby, aj.

Na základě autentizované žádosti o odvolání platnosti kvalifikovaného certifikátu CA provede příslušnou úpravu ve svém IS a aktualizuje veřejný seznam odvolaných certifikátů. Podle důvodů vedoucích k zneplatnění kvalifikovaného certifikátu personalista aktivuje proces vydání nového QC.

Zálohování podpisových dat (páru klíčů) se neprovádí a v případě ztráty bezpečnostního předmětu (tokenu) je třeba proces vydání QC opakovat od začátku.

## Literatura

*[1.] Špunda, M.: Možnosti elektronického podpisu ve zdravotnické dokumentaci, MEDSOFT'2010, Creative Connections s.r.o., 2010, s. 191-196, ISSN 1803-8115*

**Kontakt:**

**Doc. Ing. Miloslav Špunda, CSc.**
Ústav biofyziky a informatiky UK 1. LF
Kateřinská 32, Praha 2
E-mail: *miloslav.spunda@lf1.cuni.cz*