MOŽNOSTI ELEKTRONICKÉHO PODPISU VE ZDRAVOTNICKÉ DOKUMENTACI

Miloslav Špunda

Anotace

Příspěvek se zabývá problematikou užití elektronického podpisu ve zdravotnické dokumentaci v prostředí informačního systému zdravotnického zařízení, zejména nemocničního informačního systému (NIS). Příspěvek popisuje princip zaručeného elektronického podpisu, technické předpoklady jeho užití a možnosti implementace v prostředí NIS.

Klíčová slova

elektronická zdravotnická dokumentace, nemocniční informační systém, elektronický podpis, časové razítko

Úvod

V současné době se setkáváme se stále širším užitím pouze elektronické formy dokumentů v informačních systémech. Informační systémy přecházejí na tuto formu obvykle postupně, dokumenty jsou paralelně uchovávány i v písemné formě. Jejich předávání a manipulace s nimi však přechází na formu pouze elektronickou, dřívější pouze písemné dokumenty jsou často skenovány a poté též uloženy také v elektronické formě.

S těmito trendy se setkáváme také v oblasti vedení elektronické zdravotnické dokumentace, která je stále častěji uchovávána pouze na paměťových mediích. Tento vývoj odpovídá i legislativním trendům v rámci EU, odpovídá mu i naše národní legislativa v této oblasti (Zákon č. 227/2000 Sb. o elektronickém podpisu).

Plné zavedení zdravotnické dokumentace v čistě elektronické formě musí vycházet z platného právního rámce a zároveň musí být technicky řešeno tak, aby byla respektována informační bezpečnost. Prakticky to znamená, že v informačním systému musí být užit zaručený elektronický podpis a časové razítko, bezpečnostní kopie podepsaných dokumentů, zajištěna archivace dokumentů a jejich celková správa včetně workflow dokumentů ve zdravotnickém zařízení.

Základní pojmy

Metody použití elektronického podpisu (přesněji digitálního podpisu) vycházejí z kryptografických šifrovacích algoritmů. Pojem elektronický podpis zahrnuje širší oblast prokázání totožnosti v elektronické formě (např. snímání otisku prstu, struktury oční duhovky a dalších biometrických atributů uživatele). **Digitální podpis** však zajišťuje několik nezbytných prvků zároveň. Při doplnění **časovým razítkem** zaručuje i prokazatelnost doby podepsání dokumentu.

Prvky zajištěné užitím digitálního podpisu:

- identifikace (jednoznačné určení podepsaného subjektu),
- integrita (lze prokázat, že po podepsání nedošlo k žádné změně (soubor není úmyslně či neúmyslně změněn)),
- autenticita (lze ověřit identitu subjektu, kterému digitální podpis patří),
- nepopiratelnost (nelze popřít autorství elektronického dokumentu).

Při použití pro podepisování zdravotnické dokumentace je vyžadován tzv. zaručený elektronický podpis, s předepsaným užitím kvalifikované certifikace, tedy založený na kvalifikovaném certifikátu a spojený s užitím časového razítka. Časové razítko jednoznačně dokládá existenci označených dat před uvedeným časovým okamžikem.

Při užití kryptografie je nutno řešit problém převedení zašifrovaného textu zpět do otevřené (čitelné) podoby. K tomu je třeba znát šifrovací klíč, největší problém je jeho bezpečné předání adresátovi. Z tohoto pohledu lze kryptografické metody rozdělit podle způsobu manipulace se šifrovacím klíčem. Podle toho můžeme rozlišit dva druhy šifrovacích algoritmů, se symetrickým a asymetrickým šifrováním.

Symetrické šifrování užívá jediného šifrovacího klíče pro zašifrování i dešifrování předávaných dat. Nevýhodou je, že při vyzrazení tohoto klíče jsou prozrazeny všechny zašifrované informace. Slabým článkem je tedy bezpečné předání šifrovacího klíče adresátovi i jeho následné udržení v tajnosti. Z technického hlediska je výhodou vysoká rychlost šifrovacích algoritmů.

Pro účely digitálního podpisu se užívá **asymetrické kryptografie** (kryptografie s veřejným klíčem). Tato metoda užívá dvojice šifrovacích klíčů, veřejného a soukromého. Veřejný klíč je volně dostupný všem subjektům, které se účastní šifrované komunikace. Soukromý klíč je naopak pouze v držení vlastníka a přísně chráněn, pokud možno i HW prostředky. Princip užití dovoluje text zašifrovaný soukromým klíčem dešifrovat pouze příslušným klíčem veřejným a naopak. Matematické funkce použité v šifrovacích algoritmech asymetrických šifer prakticky neumožňují reverzní výpočet, tedy prolomení šifry a zneužití šifrovaného textu. V praxi je nejčastěji užíván algoritmus RSA (Rivest – Shamir – Aleman) nebo též algoritmy na bázi eliptických křivek (ECC), autorů N. Koblize a V.S. Millera (1985). Nevýhodou asymetrických šifrovacích algoritmů je, že ve srovnání se symetrickými algoritmy jsou výrazně pomalejší. V případě užití pro digitální podepisování, kdy délka šifrovaného a dešifrovaného textu je malá, není tato nevýhoda tak významná.

Kromě asymetrických šifrovacích algoritmů s veřejným klíčem se při užití digitálního podpisu setkáme ještě s jednocestnými algoritmy (HASH funkce). Jde o matematickou funkci, kterou lze v jednom směru spočítat snadno, zatímco v opačném směru (inverzní zobrazení) jen velmi obtížně. Výsledkem HASH funkce je obvykle 128 nebo 160 bitová sekvence jednoznačně charakterizující vstupní blok dat. Přitom při změně jediného bitu vstupu, je výsledek užití HASH funkce výrazně odlišný. Nejčastěji užívanými algoritmy tohoto typu jsou v současnosti MD5 (Message Digest 5) a SHA1 (Secure Hash Algorithm).

Při užití **digitálního podpisu daného datového souboru** se postupuje způsobem, který dovoluje jednoznačné ověření autenticity, integrity, autorství (nepopiratelnost) a času podpisu dokumentu. V případě zaručeného digitálního podpisu je užito digitálního certifikátu podepsaného akreditovanou kvalifikovanou certifikační autoritou.

Podepisování:

- na soubor je užit HASH algoritmus, vznikne bitový řetězec dané délky jednoznačně reprezentující vstupní data (někdy nazývaný otisk souboru),
- HASH (otisk souboru) je poté zašifrován privátním klíčem podepisujícího, tím vznikne vlastní digitální podpis, který se přidá k podepisovaným datům,
- ke zprávě se přidá ještě digitální certifikát (viz dále) podepisujícího, který slouží adresátovi k ověření podpisu.

Ověření podpisu:

- příjemce vypočte HASH z přijatého (původního) souboru,
- dešifruje podpis pomocí veřejného klíče odesilatele, který získá z digitálního certifikátu odesilatele, vznikne HASH z podpisu,
- porovnáním výsledků (HASH souboru a HASH vzniklý dešifrováním podpisu) se ověří, že odesilatelem je vlastník připojeného certifikátu a držitel privátního klíče.

Digitální certifikát je v asymetrické kryptografii krátký strukturovaný datový blok (formát X.509 definovaný mezinárodní normou) obsahující zejména veřejný šifrovací klíč digitálně podepsaný certifikační autoritou, která certifikát vydala a zaručuje jeho správnost. Certifikát dále obsahuje informace o majiteli veřejného klíče i o vydavateli certifikátu (certifikační autoritě).

Certifikát obsahuje následující položky:

- sériové číslo,
- identifikační údaje majitele certifikátu,
- algoritmus použitý k vytvoření podpisu,
- identifikační údaje vydavatele certifikátu,
- datum počátku platnosti certifikátu,
- datum konce platnosti certifikátu,
- účel veřejného klíče (šifrování, ověřování podpisů nebo obojí),
- veřejný klíč (délka je závislá na způsobu použitého šifrování),
- algoritmus otisku certifikátu,
- vlastní otisk certifikátu, sloužící k ověření neporušenosti certifikátu.

Při ověřování certifikátu se ověřuje důvěryhodnost v něm uvedených údajů. Není nutno ověřovat každý certifikát, užije se principu přenosu důvěry, kdy na základě důvěryhodnosti certifikační autority a platnosti jejího digitálního podpisu pod certifikátem se usoudí na pravdivost údajů v certifikátu. V případě,

že certifikát je vydán akreditovanou kvalifikovanou certifikační autoritou s respektováním Zákona o elektronickém podpisu, mluvíme o **kvalifikovaném certifikátu**, který je uznáván pro komunikaci se státními institucemi. Tento typ certifikátu se užije při podepisování zdravotnické dokumentace.

Certifikační autorita (CA) je subjekt vydávající digitální certifikáty (veřejné šifrovací klíče, které podepisuje svým digitálním podpisem). CA svou autoritou stvrzuje pravdivost údajů, které jsou ve volně dostupném certifikátu uvedeny. Majitel veřejného klíče při formální proceduře certifikační autoritě prokáže správnost údajů, které jsou poté obsahem vydaného certifikátu. Certifikační autorita musí odpovídajícím způsobem pečovat o svou důvěryhodnost (např. zveřejnit způsoby zajištění bezpečnosti dat a všech okolností souvisících s vydáváním certifikátů). Ověřování certifikátů je zjednodušeno hierarchickým modelem využívaným certifikačními autoritami. Stačí pak vlastnit několik kořenových certifikátů CA, kterým důvěřujeme. Zjednoduší se tak automatizované ověření certifikátu.

Mezi majitelem certifikátu a CA existuje smluvní vztah. Majitel certifikátu musí CA oznámit zejména prozrazení (diskreditaci) soukromého klíče. To vede CA k neprodlenému zneplatnění certifikátu zařazením do seznamu zneplatněných certifikátů CRL (Certificate Revocation List). Zde je uvedeno sériové číslo zneplatněného certifikátu, datum zneplatnění a obvykle i důvod. Seznam CRL je zveřejněn na Internetu a pravidelně aktualizován (odpovědnost CA).

Formální kroky při žádostech o certifikát vyřizuje registrační autorita podřízená CA. Ověřuje identitu žadatelů a pravost údajů uvedených v žádosti o certifikát. Žádost při zachování důvěrnosti pak postupuje CA, obvykle zprostředkuje předání certifikátu jeho majiteli.

Vzhledem k omezené časové platnosti certifikátů (doba platnosti obvykle 1 rok) je zejména u dokumentů s delší dobou platnosti nutno užít kromě digitálního podpisu v rámci PKI (Public Key Infrastructure) ještě **časové razítko** TS (time stamp). Kvalifikované časové razítko poskytne na požádání autorita časových značek TSA (Time Stamp Autority). HASH (otisk) dokumentu, který chce klient opatřit časovým razítkem se elektronicky zašle certifikovanému poskytovateli TSA, který otisk opatří TS, elektronicky podepíše a zašle zpět.

Postup vytvoření časového razítka:

- klient zajistí HASH dokumentu a doplní jej dalšími údaji (normalizovaná žádost o vydání časové značky),
- žádost je odeslána TSA,
- TSA k HASHi přidá přesný časový údaj, vznikne časová značka,
- TSA časovou značku digitálně podepíše (vznikne TS) a odešle klientovi,
- platnost TS lze ověřit porovnáním HASHe dokumentu s HASHem dešifrovaným z TS pomocí certifikátu TSA.

TSA garantuje, že časový údaj vložený do kvalifikovaného časového razítka odpovídá hodnotě koordinovaného světového času UTC (Coordinated Universal Time). Po vypršení doby platnosti certifikátu stačí vyhodnotit časové

razítko vymezující dobu vzniku dokumentu. Spadá-li tato doba do doby platnosti certifikátu, potvrzuje to věrohodnost digitálního podpisu.

Technické předpoklady

Bezpečnost autentizace a šifrování je dána také způsobem uložení a manipulace se šifrovacími klíči. Problematické je uložení na pevném disku počítače nebo na externím USB flash disku. Jako bezpečný prostředek pro autentizaci a zároveň bezpečné úložiště pro malá data (několik kB) je vhodné užít čipovou kartu nebo USB token. Zde je možno bezpečně ukládat šifrovací klíče, certifikáty, atd. Pro privátní a veřejný klíč s certifikáty se užívá označení **digitální ID**.

Podstatnou výhodou těchto prostředků pro ukládání digitálních ID je, že privátní šifrovací klíč nemusí toto zařízení při šifrování vůbec opustit, není ani na okamžik vydán mimo čipovou kartu či token do počítače. Šifrování proběhne přímo v kartě nebo USB tokenu.

Používané čipové karty nebo USB tokeny jsou chráněny PIN (Personal Identification Numer) nebo heslem, které jsou užity pro autentizaci uživatele. Heslo (alfanumerický řetězec) je zde bezpečnější než PIN (řetězec číslic). Při opakovaném chybném zadání hesla dojde k zablokování. Přitom může být nastaveno automatické smazání všech uložených informací nebo mohou být smazány ručně pomocí utility. Odblokování může být umožněno zadáním dalšího kódu PUK (Personal Unblocking Key) s možností nastavit nové heslo či PIN. Pro kartu nebo token se užívá společné označení **bezpečnostní předmět**.

Možnosti implementace

Zavedení elektronického podpisu v prostředí NIS znamená respektovat specifické podmínky medicínského prostředí. Zdravotnická dokumentace je stále více uchovávána pouze v elektronické formě a duplikována v tištěné či psané formě jen v nezbytných případech. Implementace digitálního podpisu však znamená významný zásah do uživatelského prostředí. Máme na mysli případ zavedeného běžícího informačního systému a uživatele, kteří rutinně pracují se zavedenými aplikacemi.

V předešlých odstavcích byly popsány základní předpoklady pro užití digitálního podpisu. Způsob splnění těchto předpokladů a zavedení nových věcí v prostředí s plně pracovně zatíženým personálem zdravotnického zařízení vyžaduje citlivý přístup bez zbytečného obtěžování.

Vlastní technické zásahy do jednotlivých aplikací NIS jsou z tohoto hlediska méně významné. Zabudování SW podpory digitálního podpisu a naopak jeho ověření s identifikací autora podpisu je technickým problémem, kde směrem ke koncovým uživatelům je významná jen otázka uživatelského interface. Ten musí být koncipován tak, aby užití digitálního podpisu uživatelské prostředí zbytečně nekomplikovalo. Kromě elektronicky podepisovaných dokumentů bude nadále v NIS existovat skupina dokumentů, kde podle stávajících předpisů není digitální podpis nutný.

Hlavní problém představuje způsob spolupráce s kvalifikovanou certifikační autoritou, která poskytne digitální ID (e-Identitu) jednotlivým pracovníkům

zdravotnického zařízení. Organizace jednotlivých žádostí o digitální ID a jejich vyřizování musí být taková, aby nenarušovala chod zdravotnického zařízení jako celku.

Kontakt:

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