ELEKTRONICKÁ ZDRAVOTNÍ POJIŠŤOVNA HZP

Milada Hrabalová
Otakar Fišer

Hutnická zaměstnanecká pojišťovna, Jeremenkova 11, 703 00 Ostrava-Vítkovice, ČR
milada.hrabalova@hzp.cz, fiser@hzp.cz

Abstrakt
Elektronická zdravotní pojišťovna umožňuje komunikovat s partnery pojišťovny, tj. pojištěnci, zdravotnickými zařízeními a plátci pojistného. Tuto aplikaci provozuje Hutnická zaměstnanecká pojišťovna již déle než rok. V rámci této aplikace byla realizována i elektronická podatelna, která doplňuje služby pojišťovny. Komunikace je zabezpečená šifrováním a je využíván elektronický podpis.
V příspěvku jsou uvedeny naše zkušenosti s návrhem a realizací této aplikace.

1. HZP

Hutnická zaměstnanecká pojišťovna (HZP) je zdravotní pojišťovna, která zajišťuje své služby pro více než 333 tisíc pojištěnců převážně na území severní a jižní Moravy.

Web:	http://www.hzp.cz	E-Podatelna:	posta@hzp.cz
Informace:	infocentrum@hzp.cz	E-Přepážka:	https://vip.hzp.cz
Telefon:	+0042 599 09 09 09		

2. Elektronická zdravotní pojišťovna

Elektronická zdravotní pojišťovna umožňuje klientům elektronicky komunikovat, tj. mimo jiné předávat dokumenty a hlášení, vyřizovat žádosti nebo nahlížet do vlastních osobních dat uložených v informačním systému, bez nutnosti navštívit pojišťovnu. Komunikace probíhá z pohodlí domova či kanceláře 24 hodin denně 7 dní v týdnu.
Zdravotní pojišťovna udržuje ve svém informačním systému citlivé osobní údaje o pojištěncích, proto bylo důležité zabezpečit komunikaci podle příslušného zákona [1]. Komunikace je standardně šifrována a používá elektronický podpis dle platné legislativy [2].
Komunikace pojištěnců, plátců a zdravotnických zařízení s pojišťovnou vychází z požadavků, které jsou dány platnou legislativou; jedná se např. o ohlašovací povinnost, zasílání výkazů atd. Na počátku byly realizovány nejčastěji se vyskytující případy. Aplikace nyní sestává ze dvou částí:

- Elektronická podatelna (E-podatelna)
- Elektronická přepážka (E-přepážka)

3. Elektronická podatelna

Elektronická podatelna je rozšířením a doplněním funkcí stávající podatelny; je oficiálním místem pro příjem a odesílání elektronických dokumentů. Umožňuje obecnou komunikaci klientů s pojišťovnou pomocí e-mailu. Byla uvedena do provozu 1.12.2001. Používá doporučenou adresu posta@hzp.cz. Elektronická podatelna byla vytvořena v souladu se

standardem Úřadu pro veřejné informační systémy (ÚVIS). Dokumenty mohou být elektronicky podepsané a případně šifrované. Pro podpis lze použít standardní certifikát.

Postup:
Klient zašle hlášení, výkaz, žádost, obecně žádost nebo podání, na adresu podatelny a téměř ihned obdrží automatické potvrzení o přijetí v této formě:

> **Od**: odesilatel
> **Komu**: posta@hzp.cz
> **Předmět**: dle odesilatele
> **Byla přijata dne**: datum, hodina a minuta přijetí
> **Pod jednacím číslem**: číslo pro odkazy

Pokud je zpráva elektronicky podepsána, jsou uvedeny některé identifikační údaje z předmětu certifikátu. Pokud je zpráva šifrována, je tato skutečnost uvedena. Na konci potvrzení je uveden odkaz pro sledování stavu zpracování žádosti v pojišťovně, tj. identifikace jeho žádosti a stav zpracování. Pro evidenci se používají:

- kniha přijaté ověřené pošty, pro podepsané podání,
- kniha přijaté neověřené pošty.

Pracovnice podatelny rozešlou žádosti podle obsahu příslušným zaměstnancům; žádost může být přeposlána dál.

4. Elektronická přepážka

Elektronická přepážka umožňuje komunikovat s partnery; v zásadě lze provádět veškeré obvyklé funkce. E-přepážka je na adrese https://vip.hzp.cz a byla uvedena do provozu 2.4.2002.
Demo najdete na stránkách pojišťovny http://www.hzp.cz/. Objasní veškeré funkce E-přepážky; je zde popsán postup přihlášení a registrace, objasnění základních pojmů, jsou uvedeny nejčastější dotazy a seznam uznávaných certifikačních autorit.

4.1 Funkce přepážky

Služby E-přepážky využívají především plátci a zdravotnická zařízení, kteří komunikují s pojišťovnou pravidelně, obvykle jednou měsíčně; tuto komunikaci mohou provádět i zprostředkovatelské firmy. Pro pojištěnce existuje několik funkcí a lze je používat i jako zákonný zástupce např. pro dítě. Elektronická přepážka umožňuje komunikaci pouze registrovaným klientům a vyžaduje certifikát pro elektronický podpis.

Funkce pro jednotlivé partnery
Pojištěnci

- Výdajový účet pojištěnce
  Výdajový účet pojištěnce obsahuje seznam výkonů, léků a zdravotních pomůcek, které byly na pojištěnce vykázány a pojišťovnou zaplaceny. Pojištěnec získá přehled o ceně zdravotní péče, která byla poskytnuta. Tento účet může být využit ke kontrole. Součástí účtu je seznam navštívených zdravotnických zařízení, celkové náklady na péči, předepsané léky s odkazem na příbalový leták; seznamy a výčty lze podle potřeby vhodně seřadit.
- Změna kontaktních údajů

- Hlášení o dlouhodobém pobytu v cizině
- Hlášení o změně plátce

Zdravotnická zařízení

- Vykázání zdravotní péče poskytnuté pojištěncům
- Výpis plateb na účet zdravotnického zařízení
- Ověření příslušnosti pojištěnce k pojišťovně
- Přehled kapitovaných pojištěnců

Plátci zdravotního pojištění

- Hromadné oznámení zaměstnavatele
- Přehled o platbě pojistného
- Požadavek na seznam zaměstnanců

Další funkce jsou určeny pro všechny klienty:

- Doručená a odeslaná pošta
- Nastavení uživatelského prostředí

Administrátor přepážky má řadu funkcí pro správu a administraci klientů:

- Administrace a aktivace klientů
- Administrace certifikátů
- Statistiky o uživatelích a komunikaci

4.2 Podmínky komunikace

Technické podmínky

- Prohlížeč:
  Microsoft Internet Explorer 5.1 nebo vyšší, který umožňuje 128 bitové šifrování.
- ActiveX:
  Komponenta ActiveX objektu SignForm pro podepisování formulářů; je to komponenta do Windows. Lze ji najít a nainstalovat i z internetových stránek pojišťovny.
- Poštovní program:
  MS Outlook nebo MS Outlook Expres.

Certifikát

Klient musí mít předem na PC, na čipové kartě nebo eTokenu nainstalován svůj osobní certifikát. Lze použít certifikát akreditované certifikační autority, v současné době pouze I.CA (http://www.ica.cz/), nebo komerční certifikáty I.CA, GTS (http://www.eidentity.cz/) a dalších; seznam uznávaných autorit je na webu pojišťovny. Certifikát musí být dle normy X509 verze 3, standardu RFC-2459, klíč musí mít délku 1024 bitů [4].

Registrace

Klient vyplní formulář pro registraci umístěný na internetových stránkách E-přepážky. Pokud klient již komunikuje s pojišťovnou jiným způsobem a jeho údaje jsou v informačním systému, stačí vyplnit základní identifikaci, např. rodné číslo nebo IČ, a další údaje se doplní.

Smlouva

Certifikát sám o sobě nestačí pro jednoznačné přiřazení osoby k certifikátu, neobsahuje dostatečné údaje, je to nástroj k podpisu. Přiřazení klienta k certifikátu je provedeno smlouvou, ve které je uvedeno:

- jméno a příjmení klienta, adresa a rodné číslo nebo datum narození,

- údaj z certifikátu, tj. název poskytovatele certifikačních služeb a sériové číslo certifikátu,
- identifikace pojišťovny a certifikát serveru E-přepážky,
- rozsah funkcí podle typu klienta,
- dohoda o šifrování.

Standard pro šifrování není zatím legislativně stanoven, v zákoně o ochraně osobních údajů je pouze obecný požadavek na zabezpečení. Při standardní obměně certifikátu po roce není třeba nové smlouvy. Po podepsání smlouvy aktivuje administrátor přístup do E-přepážky a lze zahájit komunikaci.

Komunikace
Klient se přihlásí jménem a heslem do E-přepážky a po kontrole certifikátu si zvolí požadovanou funkci; součástí komunikace může být předání nebo převzetí dat, požadavek na data z informačního systému se vyřizuje přibližně asi půl hodiny. Klient obdrží výsledky do složky v E-přepážce a upozornění na e-mail nebo mobil, pokud si tak zvolí.

4.3 Technické řešení

Preferovali jsme otevřené řešení, nenáročné a laciné pro uživatele.

Klientská část – PC uživatele
Popis v předcházející části, tj. Windows s MS prohlížečem, komponenta ActiveX, poštovní program a certifikát.

Internet serverová část
- www server Apache s modulem mod_ssl pro podporu šifrování SSL,
- OS Linux,
- databáze MySQL,
- skriptovací jazyk PHP.

Informační systém pojišťovny
Je založen na OS UNIX a databázi Progress; je oddělen firewallem od demilitarizované zóny, ve které jsou jen vyžádané údaje E-přepážky. Informační systém zajišťuje komunikaci pomocí UUCP; nyní v intervalu 30 minut. Většina úloh je zpracovávána automaticky bez nutnosti zásahu obsluhy, nebo je alespoň automaticky zařazena do standardního zpracování.

4.4 Zabezpečení komunikace

- Šifrování komunikace na základě protokolu HTTPS, tj. HTTP over SSL, založeno na Open Source knihovnách OpenSSL.
- Autentizace, tj. totožnost uživatele a serveru, využívá vlastnost HTTPS, kdy se provádí vždy autentizace serveru a volitelně autentizace uživatele. Autentizace se provádí za použití asymetrické kryptografie. Samotné šifrování přenášených dat používá symetrické šifrování. Protokol SSL nelze použít pro autorizaci dat, protože nemá přístup do aplikačních dat. Autentizace uživatele je dále zajištěna přihlašovacím jménem a heslem.
- Autorizace dat, tedy pravost dat a integrita, je zajištěna komponentou ActiveX objektu SignForm, který provádí elektronické podepsání dat odeslaných z HTML formuláře. Řešení je založeno na Microsoft CryptoAPI.

- Platnost použitého certifikátu se kontroluje při každém přihlášení klienta oproti Certificate Revocation List, tj. seznam odvolaných certifikátů (CRL); aktualizuje se dvakrát denně.

4.5 Několik poznámek a vysvětlení k elektronickému podpisu

Elektronický podpis
V komunikaci mezi klientem a pojišťovnou je nutná důvěryhodná třetí strana, tzv. Certifikační autorita (CA). Tato autorita má plnit dvě základní funkce:

- certifikační – zaručuje, že deklarovaný veřejný klíč patří dané osobě,
- validační – potvrzuje platnost certifikátu, vydává seznam odvolaných certifikátů CRL.

Pro komunikaci s institucemi státní správy je nutný kvalifikovaný podpis akreditované CA. Ostatní subjekty mohou uznávat i jiné certifikáty, pokud se tak dohodnou.

Zaručený elektronický podpis
Splňuje následující požadavky dle [2]:

- autentizace - je jednoznačně spojen s podepisující osobou,
- identifikace - umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Kvalifikovaný a komerční certifikát
Ze zákona jsou kvalifikované oba, v praxi se používá termín *kvalifikovaný* pro certifikát akreditované CA, pro jehož získání je třeba doložit dva doklady totožnosti. *Komerční (klientský, osobní)* certifikát se liší menší „přísností“ při jeho získání, stačí jeden doklad totožnosti. Tento typ certifikátů vydávávají certifikační autority neakreditované, ale i akreditovaná I.CA. Lze jej plnohodnotně používat na základě smlouvy mezi subjekty. Tento certifikát je obvykle levnější.

Certifikační autority
Fungování naší aplikace jsme vyzkoušeli se všemi druhy certifikátů od všech certifikačních autorit. Některé autority vyžadují osobní návštěvu kontaktního místa; to může být problém, pokud je toto místo vzdáleno. Ostatní autority vyžadují smlouvu ověřenou notářem. Je to jednodušší, ale déle to trvá; certifikát je vystaven CA po obdržení ověřené smlouvy.

5. Řešitelé

ProIT a.s. (www.proit.cz)
Je řešitelem Elektronické přepážky a podatelny. Softwarová firma, která se zaměřuje na integraci a outsourcing aplikací, bezpečnost a další služby ICT.
Certifikační autorita **eIdentity, s.r.o.** (www.eidentity.cz)
Dříve KPNQwest Czechia, s.r.o., nabízí zatím komerční certifikáty. Intenzivně spolupracujeme v oblasti aplikování certifikátů, spolupráce je pro obě strany výhodná. Získali jsme certifikáty pro testování pro vlastní pracovníky i pro naše klienty.
Napojení na informační systém pojišťovny byl zajištěn vlastními pracovníky.

6. Zkušenosti a praxe

Motivy, které nás vedly k tomuto příspěvku, pramení především z našeho pocitu, že aplikace s elektronickým podpisem jsou především pro uživatele složitější; novým prvkem je legislativa kolem e-podpisu, nástroje pro podpis, potřeba udržet nástroje pro podpis pod kontrolou, identifikace občana a bezpečnost aplikace. Chceme jen upozornit na některé aspekty tohoto problému.

Vlastní zkušenosti

Problematika elektronického podpisu je poměrně nová. V době, kdy pojišťovna se svým projektem začínala, neexistovaly aplikace používající elektronický certifikát. Pouze proprietární řešení v bankovním sektoru, ale tyto aplikace používaly a stále používají vlastní certifikát platný pouze ve styku s bankou. V té době byl přijat zákon o elektronickém podpisu a ještě neexistovala akreditovaná certifikační autorita.

Gramotnost populace

Gramotnost je v oblasti elektronického podpisu minimální, podpis je málo rozšířen. Uživatelé předpokládají, že dodavatelé software připraví vhodné produkty. K tomu ještě přispívá složitá právní problematika a poměrně komplikované a nezvyklé nástroje. Úroveň znalostí je nízká, experti v této problematice téměř neexistují.

Našim klientům i vlastním zaměstnancům, kterým jsme se systematicky věnovali, trvalo dlouho než pochopili některé nové skutečnosti při práci s certifikátem. Museli pochopit i technické souvislosti zvláště při manipulaci s certifikáty. Každý sám si musí umět požádat o certifikát, projít a pochopit návody, zadat všechny parametry a hesla, vyřídit formality kolem registrace a nainstalovat certifikát. To je složité.

Znalosti uživatelů o této problematice jsou nedostatečné. Každý „nějak“ ví, co znamená jeho podpis na dokumentu, ale v případě elektronického podpisu je nutno tuto věc formalizovat a exaktně vyložit. Zatím není jasné, jak by celá problematika mohla být použita před soudy; zdá se, že veškerá procesní řízení jsou doposud nastavena na papírové dokumenty.

Česká republika zatím nemá dostatečný počet aplikací, a proto je to nezajímavé pro občany a instituce. Komunikace se státní správou se teprve pomalu rozbíhá.

Problémy s klienty

Přestože jsme chtěli, aby všechna naše řešení nebyla závislá na konkrétním SW. Při používání podpisů jsme nuceni svým klientům doporučovat v poštovních programech vcelku odzkoušené MS Outlook nebo MS Outlook Expres na Windows s MS prohlížečem. I přes to se stává, že někteří klienti nejsou schopni otevřít podepsanou nešifrovanou zprávu. Souvisí to snad s konkrétní instalací Windows a prohlížeče; obvykle se odstraní přeinstalováním. Klienti používající Notes mají problémy s otvíráním zašifrované zprávy, který neumíme zatím řešit; tento problém je údajně znám. Máme zkušenost, že téměř každému našemu klientovi jsme museli se získáním certifikátu nebo s registrací do naší Elektronické přepážky pomáhat, pokud jim nepomáhal např. zdatný potomek.

Pojišťovna

Na Elektronickou přepážku zatím neprovádíme žádnou intenzivní reklamu, jen střízlivé oznámení pro zájemce. Chceme komunikovat jen s těmi, kteří budou ochotni překonat počáteční potíže, proto zatím dáváme certifikáty zdarma. Náš cíl je získávat zkušenosti a prověřit vyzkoušet funkcionalitu E-přepážky. Vzdálenější cíl jsou web services.

Protože pro práci s Elektronickou přepážkou a elektronickým podpisem jsou důležité alespoň základní znalosti problematiky, oslovujeme hlavně větší firmy, tj. plátce a zdravotnická

zařízení, kteří mají vlastní informatiky. Paradoxně nás vyhledávají spíše menší firmy, zprostředkovatelské firmy a samotní pojištěnci, fandové v této oblasti. Očekáváme větší přírůstek klientů, až bude existovat více aplikací, až se bude komunikovat se státní správou a problematika e-podpisu bude známější věc.

Bezpečnost
U běžných aplikací je bezpečnost řešena pomocí nadřazené bezpečnostní politiky organizace. U E-přepážky se jedná o komunikaci mezi „nebezpečným světem internetu“ a konkrétním systémem, který je uvnitř firmy. Uživatel si musí uvědomit, že si nástroje na podpis musí chránit. Týká se to každé výměny počítače, fyzické opravy atd. Uživatel musí vědět, kde nástroje pro podpis má, jak si je má hlídat, jak se dá podpis zneužít. Již při žádosti o certifikát si musí uživatel uvědomit možné důsledky zneužití certifikátu a zvolit si jeho vhodné vlastnosti.

Legislativa
Dosavadní zákon má řadu nedostatků. Mimo jiné např. nejednoznačná identifikace osoby v popisu certifikátu, časové razítko atp. I s tímto zákonem lze řešit řadu aplikací, je nutné však rozumět možnostem a omezením zákona. Věci neřešené a chybějící v zákoně je nutno vyřešit nebo stanovit v rámci aplikace, smluvním ujednáním, technickým nebo organizačním řešením.

Identifikace občana
Současné certifikáty neobsahují identifikátor, který by jednoznačně určoval danou osobu. Někteří autoři, např. [3] soudí, že takový identifikátor by ani být neměl a preferují tzv. *atributové* certifikáty. Tyto certifikáty neobsahují veřejný klíč certifikované osoby, ale jiné její ověřené údaje. Tento certifikát může být i neveřejný a odkazuje se na podpisový certifikát.
Pro komunikaci s Ministerstvem práce a sociálních věcí je nutno mít v certifikátu tzv. *bezvýznamový identifikátor*, speciální identifikátor ministerstva.
Identifikace občana buď rodným číslem (RČ) nebo bezvýznamovým identifikátorem občana (BIO) je v současné době vymezována a zdá se, že není jasné, jak bude státní správa těchto identifikátorů používat. Proti RČ je Úřad pro ochranu osobních údajů, ale některé resorty např. zdravotnictví si nedovedou zatím představit dokumentaci bez RČ.

Řešitelé a aplikace
Analytici musí znát uvedenou problematiku, nemohou čekat podporu od právníků, manažerů a různých dalších zadavatelů. Nové nástroje a možnosti IT se rychle rozvíjí, problematiku je nutné průběžně sledovat. Cílový produkt je nutno vytvořit flexibilně, protože praxe bude vyžadovat úpravy. Vhodné je obecnější řešení, které lze modifikovat, se sadou různých pomocných nástrojů. Patřičnou pozornost je nutné věnovat návodům a helpům, pro komunikaci s klienty a uživateli.

Nedostatek standardů
Ve zdravotnictví nejsou definovány standardy pro elektronickou komunikaci. Tento nedostatek je znám, příslušné instituce se příliš nesnaží o nápravu. Na standardy čekají firmy vyvíjející aplikace, pokud nebudou standardy nezačne vývoj nových produktů. XML pro standardy se zatím v této oblasti nepoužívá. Týká se to poměrně komplikovaných nemocničních systémů nebo programů pro ambulance. Koneční uživatelé, lékaři a managementy zdravotnických zařízení nechtějí experimentovat s novými nestabilním

aplikacemi. Zájem mají pouze zprostředkovatelské firmy; jsou zaměřeny na vlastní počítačové zpracování a dovedou ocenit výhody.

7. Závěr

Nástroje pro elektronický podpis jsou i přes určité nedostatky vhodné pro určitou třídu úloh; jedná se především o cyklické úlohy, které mají charakter požadavek-odpověď. Jsou to úlohy podobné běžným úkonům s bankou, zdravotní pojišťovnou nebo s úřady. Tyto úlohy předpokládají sice u uživatelů určité znalosti navíc, ale přinášejí podstatné zjednodušení a urychlení operací. V budoucnu povedou k další integraci informačních systémů, usnadnění a zautomatizování komunikace.
Elektronická přepážka a podatelna jistě usnadní komunikaci klientům pojišťovny; uspoří čas, zjednoduší předávání dat, lze komunikovat bez časového omezení. Komunikace je jednodušší a rychlejší. Pro pojištěnce přináší ještě další hodnoty – získává aktuální informace o poskytované péči v detailním členění.

Literatura:

1. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
2. Zákon č. 227/2000 Sb., o elektronickém podpisu a změně některých dalších zákonů
3. Kment, V.:Jednoznačná identifikace se zachováním soukromí. Computerworld 4/2003
4. Dostálek, L.:Velký průvodce protokoly TCP/IP: Bezpečnost. Computerpress, Praha, 2001