AUTENTIZACE VE WEBOVÝCH APLIKACÍCH

Milada Hrabalová
Hutnická zaměstnanecká pojišťovna (HZP), Jeremenkova 11, 703 00 Ostrava-Vítkovice,
milada.hrabalova@hzp.cz

ABSTRAKT
Příspěvek pojednává obecně o autentizaci, uvádí základní terminologii a předkládá různé způsoby autentizace a jejich plusy a mínusy. Blíže se zabývá autentizací ve webových aplikacích a popisuje legislativní problémy s použitím kvalifikovaných certifikátů.
V posledních dvou kapitolách se zabývá praktickými zkušenostmi Hutnické zaměstnanecké pojišťovny s autentizací pomocí certifikátů a se zaváděním autentizace pomocí jednorázových hesel zasílaných klientovi ve formě SMS kódů.

This paper generally describes authentication problems, defines basic terminology, submits various forms of authentication methods and specifies their positives and negatives. It also deals more closely with the authentication methods in web applications and describes legislative problems with the usage of qualified certificates.
In the last two chapters, the paper presents practical experience of Hutnická zaměstnanecká pojišťovna (HZP - health insurance company) with authentication. It presents the application Elektronická přepážka (Electronic counter) and describes authentication using certificates and implementation of the authentication method via one-time passwords sent to client by SMS messages.

KLÍČOVÁ SLOVA
Autentizace, webová aplikace, certifikát.

1. ÚVOD

Základní terminologie

- **Identifikace** je proces určení identity uživatele. Uživatel identitu zadá např. přihlašovacím jménem
- **Autentizace** (někdy též autentikace nebo autentifikace), je proces ověřování identity uživatele. Následuje za identifikací a systém dle dalších údajů ověřuje, zda uživatel je opravdu tím, za koho se vydává.
- **Autorizace** je proces ověřování, co uživatel může a co nemůže. U některých aplikací může být vyžadována pro každou kritickou funkci.

2. ZPŮSOBY AUTENTIZACE A JEJICH (NE)BEZPEČNOST

Existují tři základní metody autentizace, a to podle toho, zda je autentizace založena na tom:

a) co uživatel zná (heslo, PIN)
b) co uživatel má (předmět)
c) čím uživatel je (biometrická informace – otisk palce, oční duhovka aj.)

Blíže k jednotlivým metodám:

a) Autentizace na základě toho, **co uživatel zná**, je nejjednodušší a nejlevnější způsob autentizace pro zavedení, použití i údržbu, ale je také nejméně bezpečný, pokud není kombinován s jinými způsoby.
Problémy s hesly jsou obecně známé, heslo lze odpozorovat nebo odposlechnout keyloggerem. Uživatelé se nechovají bezpečně, při přemíře hesel si pomáhají lístečky, které ukládají na dostupná místa. Používají se programy pro zapamatování hesel, které heslo předvyplní každému, kdo u počítače právě pracuje. Lidé si neuvědomují hodnotu svého hesla a jsou ochotni jej sdělit; dle BBC [4] jsou jej ochotni prozradit i za kousek čokolády nebo dokonce zadarmo.
Dalším aspektem je zvyšující se rychlost počítačů; nyní stačí k prolomení hesla hrubou silou několik hodin. Bezpečnostním problémem může být i samotné uložení hesel v aplikaci.
Přes všechny tyto bezpečnostní problémy lze tímto způsobem u některých bank ještě přistupovat ke svému účtu přes internet a provádět tam transakce.

b) Autentizace na základě toho, **co uživatel má** (předmět) je již složitější; předmět musí být vytvořen a musí existovat příslušné čtecí zařízení. Klasickým autentizačním předmětem je čipová karta. Pokud tato metoda není kombinovaná s jinou, není také příliš bezpečná. Předmět uživatel může ztratit nebo se předmět může porouchat aniž by to na něm bylo vidět.

c) Autentizace na základě toho, **čím uživatel je** (biometrika) není příliš rozšířená. Je tomu tak proto, že tato metoda není zcela přesná a je ze všech nejnákladnější. Je nutná čtečka konkrétního biometrického údaje. Při autentizaci dochází jak k nesprávným odmítnutím oprávněných uživatelů, tak k nesprávnému přijetí neoprávněných uživatelů. Příčinou je to, že se při autentizaci málokdy podaří získat shodný vzorek jako ten, který je uložen v informačním systému. Proto nelze nastavit systém na absolutní shodu jako např. u hesel, nebyl by přijat žádný uživatel. Biometrický údaj nelze udržet v tajnosti - otisky prstů zanechává uživatel na všem, čeho se dotkne. Důležité jsou i právní otázky, protože informační systém zpracovává citlivé biometrické informace. Autentizovat takto uživatele pro přístup do PC se (zatím) nevyplatí. Používá se pro přístup do aplikací s přísně utajovanými daty.

Pokud je autentizace založena pouze na jedné metodě, pak se nazývá jednofaktorovou autentizací, podobně dvoufaktorová nebo třífaktorová autentizace. Nejobvyklejší je v současné době dvoufaktorová autentizace, založená na prvních dvou metodách autentizace, tj. uživatel vlastní nějaký autentizační předmět a k tomuto předmětu musí znát přístupové heslo.

K vyšší bezpečnosti autentizace bývají využívány certifikáty (digitální podpis) a to obvykle tak, že uživatel má svůj certifikát uložen na předmětu (token, karta), ke kterému je nutno znát heslo. Předměty, na kterých jsou uloženy certifikáty, jsou konstruovány tak, že soukromý klíč nemůže tento předmět opustit. Jedná se o dvoufaktorovou autentizaci.
Certifikát může být uložen i na pevném disku počítače, ale v tom případě klesá bezpečnost. Pokud případný útočník převezme počítač, je pro něj mnohem jednodušší certifikát zneužít. Použití cetifikátů je poměrně náročné na znalosti uživatelů, dle našich zkušeností má s nimi velké procento uživatelů problémy. Z neznalostí mohou vzniknout i bezpečnostní incidenty - uživatelé nechápou, že by soukromý klíč měli udržet v tajnosti.

Již při analýze nového informačního systému je důležité vybrat vhodnou metodu autentizace v souladu s bezpečnostní politikou organizace. Je nutné uvážit jaká data v aplikaci jsou, zda je možný vzdálený přístup a další okolnosti. V rámci školení zaměstnanců o informační bezpečnosti je potřebné stále opakovat zásady ochrany autentizačních údajů, ostatní uživatele alespoň poučit. Doporučuji ve smlouvě formulovat zodpovědnost za dodržování bezpečnostní politiky a výslovně za utajení uživatelských autentizačních údajů.

3. AUTENTIZACE VE WEBOVÝCH APLIKACÍCH

Webová aplikace nebo aplikace s webovým rozhraním je aplikace poskytovaná uživatelům prostřednictvím webových stránek a přistupuje se k ní pomocí webového prohlížeče. V dalším textu se zaměřím především na aplikace, které jsou určeny pro širší okruh uživatelů a ne jen zaměstnance jedné organizace. Jsou to služby jako např. freemail, různé státní registry, služby zdravotních pojišťoven nebo internetbanking.
Z širokého záběru webových služeb vyplývají také různé požadavky na bezpečnost autentizace. Pro služby **freemailu** bude jistě stačit heslo, u dalších aplikací je nutno posoudit citlivost informací, ke kterým se uživatel dostane a pro citlivější již kromě bezpečnější autentizace bude určitě nutná i šifrovaná komunikace.

Internetbanking

Nejčastější autentizace je bohužel stále ještě i pro citlivější údaje pomocí jména a hesla, ať už se přihlašovacímu jménu říká přístupové nebo identifikační číslo a heslu PIN. V případě bank lze většinou volitelně zvýšit bezpečnost autentizace certifikátem nebo alespoň zavést autorizaci některých peněžních transakcí např. zasíláním jednorázových kódů SMS. Požadavek na zvýšení bezpečnosti je věcí klienta a mnoho klientů může z pohodlnosti nechat zabezpečení na nejnižší úrovni. V tomto případě ale doporučuji zvolit bezpečnost vyšší, úměrnou výši rizika.

Registry vedené státem

Czech POINT je projekt, který občanům umožní získat ověřené výstupy z informačních systémů státní správy. O tyto výstupy je možno požádat na mnoha místech, např. na poště, na krajských a obecních úřadech nebo u notáře. Na uvedených místech musí být osoba, která má přístup do těchto informačních systémů. V poslední době probíhala diskuse ohledně bezpečnosti Czech POINTu, protože autentizace byla v době psaní tohoto příspěvku prováděna pouze pomocí hesla. Prohlášení MV ČR k tomuto problému viz [7]. Jak budou přibývat agendy, které budou pomocí tohoto systému přístupné, plánuje MVČR zabezpečit přístup pomocí certifikátů.

Kromě Czech POINTu patří k této kategorii ještě např. zdravotnické registry, které provozuje KSRZIS (Koordinační středisko pro resortní zdravotnické informační systémy) pod MZ ČR. Těchto registrů je asi 30 a jsou to registry od zcela veřejných (RANKMED - Vyhodnocení kvality webových stránek zdravotnických institucí a organizací) po velmi citlivé (RPN - Registr pohlavních nemocí, NOR - Národní onkologický registr). Vstup je řešen do veřejných registrů bez autentizace, ostatní registry jsou zabezpečeny autentizací jménem a heslem nebo certifikátem na čipové kartě.
Uvedené dva případy jsou vybrány pouze jako příklady. Existují další webové aplikace, které umožňují zasílat subjektům různá hlášení na státní orgány, případně si prohlížet svá data.

Služby zdravotních pojišťoven
Většina zdravotních pojišťoven používá pro autentizaci klientů certifikáty, jedna dovoluje pojištěncům k souhrnným údajům přístup prostřednictvím hesla (PINu). HZP dlouho řešila autentizaci certifikátem, ale z důvodů, které budou blíže rozvedeny v dalších dvou kapitolách, jsme začali nabízet autentizaci i SMS kódy.

4. PROBLÉM S KVALIFIKOVANÝMI CERTIFIKÁTY

Zákon o elektronickém podpisu [2] neupravuje používání kvalifikovaných certifikátů pro jiné úkony než pro elektronické podepisování. MI ČR vydalo vyhlášku [3] s účinností od 17. 8. 2007, v které je pro kvalifikované poskytovatele certifikačních služeb uvedena povinnost řídit se při poskytování kvalifikovaných certifikačních služeb normou ČSN ETSI TS 101 456 [5]. Uvedená norma obsahuje požadavek, aby podepisující osoby používaly **kvalifikovaný** certifikát **pouze** pro elektronický podpis a poskytovatele zavazují k tomu, aby podepisující osoby k tomuto smluvně zavázali. Kvalifikovaní poskytovatelé certifikačních služeb tuto povinnost začlenili v souladu s legislativou do svých bezpečnostních politik.
Pokud tedy majitel certifikátu použije kvalifikovaný certifikát k autentizaci nebo šifrování, jedná se o porušení výše uvedené normy a vyhlášky. Pro toto porušení ale nejsou uvedeny žádné sankce.
Jaký důvod vedl ETSI (European Telecommunications Standards Institute) k tomuto kroku? Jejich stanovisko je uveřejněno na stránkách MV ČR [5] a vyplývá z něj, že je někdy nezbytné „odtajnit“ šifrovací klíč, např. při odchodu zaměstnance, a tímto odtajněním už není dodržen základní požadavek na podepisovací klíče, tj. jejich udržení pod výhradní kontrolou podepisující osoby.
Již od začátku vydávání kvalifikovaných certifikátů odborníci na tento fakt upozorňovali, např. Vondruška, a to nejen v [8].

Pro lepší pochopení cituji definici autentizace a podpisu při použití certifikátu dle [5]:

- Podpisem se rozumí úkon podepisující osoby, který má význam vzhledem k podepisovaným datům. Podepisující osoba potvrzuje, že se s daty, která podepsala, seznámila a s jejich obsahem souhlasí.

- Autentizací je míněno vytvoření podpisu k náhodně vygenerovaným datům, přičemž tento úkon slouží pouze k určení identity dané osoby a nemá žádné následky vzhledem k obsahu náhodně vygenerovaných dat.

HZP ve své aplikaci pro klienty, tzv. E-přepážce, využívala dlouhých 6 let dvoufaktorovou autentizaci heslem a certifikátem a nyní tedy vyvstal problém. Uznáváme certifikáty jak komerční, jichž se výše uvedené omezení netýká, tak kvalifikované. Nechceme-li nutit uživatele k porušování normy a vyhlášky, je nutno aplikaci upravit. Vzhledem k nejasnosti jsme si vyžádali stanovisko MV ČR a uvedli navrhovaný způsob přihlašování do aplikace pomocí certifikátu:

„Uživatel vyplní jméno a heslo. Objeví se mu text, který oznamuje přihlášení do aplikace s uvedením datumu a času přihlášení. Tento text uživatel podepíše svým (kvalifikovaným) certifikátem. Následně dojde k výpočtu hashe hesla a zašifrované heslo, jméno v otevřené podobě, podpis a certifikát se pošle na server. Tam se heslo porovná s obsahem databáze, ověří se platnost podpisu, ověří se platnost certifikátu a z certifikátu (pokud je podpis a certifikát platný) si aplikace vezme některé údaje, které porovná s obsahem databáze a tak ověří identitu uživatele. Pokud vše dopadne kladně, uživatel je úspěšně přihlášen."

Z odpovědi MV ČR vyplývá, že námi navrhovaný způsob přihlašování je v souladu se zákony, vyhláškami i normami, přestože se de facto jedná o autentizaci a pro aplikace typu eGovernment by i takovéto použití kvalifikovaného certifikátu bylo nepřípustné.

5. AUTENTIZACE SMS KÓDY

V HZP jsme předpokládali, že certifikáty se rozšíří a přestože nebude platit co občan, to certifikát, alespoň střední penetrace certifikáty bude. Postupem času ale bylo čím dál jasnější, že kdo nezastupuje organizaci nebo sám nepodniká certifikát nepotřebuje, je pro něj drahý a používání složité. Nenaplnila se velká očekávání v souvislosti s elektronickým podpisem: elektronický podpis je používán jen malou skupinou obyvatel a nestačí jediný certifikát pro všechny aplikace.

Legislativní problémy s kvalifikovaným certifikátem a malé rozšíření certifikátů nás donutilo hledat pro naše klienty jiné způsoby autentizace. Nakonec jsme se rozhodli pro autentizaci SMS kódy. Jedním z důvodů, proč jsme tomuto způsobu dali přednost před ostatními je skutečnost, že dle údajů ČSÚ [9] vlastnilo v roce 2006 více než 80% obyvatel ČR mobilní telefon. Takže s rozšířením ani obsluhou „zařízení" nebude žádný problém.

Naše aplikace využívá pro autentizaci nadále heslo, navíc (místo certifikátu) je využit mobilní telefon uživatele, na který je zaslán jednorázový SMS kód, který musí uživatel zadat při přihlašování. Sám uživatel si může zvolit, zda tento kód bude používat jen pro vstup do E-přepážky nebo zda bude potvrzovat každou transakci novým kódem. Vzhledem k tomu, že u mobilních telefonů chybí údaje uvedené v certifikátu o uživateli, musí klient, který se chce takto autentizovat, navštívit kontaktní místo HZP pro ověření.

Autentizaci SMS kódy zprovoznila HZP dne 1.3.2008 a okamžitě byl vidět zájem ze strany klientů o tento způsob autentizace. Je zřejmé, že klienti chtějí komunikovat, ale certifikát považují za překážku. Nyní si mohou vybrat, zda chtějí používat certifikát nebo SMS kódy. Zasílání SMS kódů je zdarma.

6. ZÁVĚR

Autentizace je branou do aplikace a z tohoto pohledu je nutno zvolit vhodnou metodu. Dvojnásob to platí u webových aplikací, k nimž se může přihlásit téměř kdokoliv. Někdy se jedná jen o požadavek, aby oprávněnou osobou byla tatáž osoba, která si vytvořila účet (freemail), jindy je nutná přesná identifikace přihlašované osoby. Se vzrůstajícím nebezpečím v internetovém prostoru je důležité hledat dokonalejší a bezpečnější způsoby autentizace, které ale nebudou finančně nákladné a nebudou klást na uživatele přehnané nároky na obsluhu.

LITERATURA

[1] Příručka manažera VIII. – Autentizace uživatelů a autorizace elektronických transakcí, TATE International, 2007
[2] Zákon č. 227/2000 Sb., o elektronickém podpisu a změně některých dalších zákonů
[3] Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb
[4] BBC News, Passwords revealed by sweet deal [online], 20.4.2004, dostupné z http://news.bbc.co.uk/2/hi/technology/3639679.stm
[5] MVČR, Informace k používání kvalifikovaných certifikátů pro elektronický podpis a zároveň pro autentizaci a šifrování, [online], 25.5.2006, dostupné z http://www.mvcr.cz/micr/scripts/detail.php_id_3533.html
[6] Norma ČSN ETSI TS 101 456 Elektronické podpisy a infrastruktury - Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty
[7] MVČR, Systém Czech POINT je dostatečně zabezpečen, [online], 4.2.2008, dostupné z http://www.mvcr.cz/rs_atlantic/project/article.php?id=84009
[8] Vondruška, P.: Rozjímání nad PKI, Data Security Management, DSM 5/2004, Praha.
[9] ČSÚ, Mobilní telefonní síť v ČR [online], 26.11.2007, dostupné z http://www.czso.cz/csu/redakce.nsf/i/mobilni_telefonni_sit_v_cr