# Zabezpečenie webových služieb s PKI

**Marcel Zanechal**

**Príspevok sa zaoberá možnosťami implementácie bezpečnostných mechanizmov využívajúcich infraštruktúru verejných kľúčov do systémov pracujúcich na báze webových služieb. S nárastom používania webových služieb v praxi sa táto problematika stáva mimoriadne zaujímavou a jej úspešné zvládnutie bude jedným z rozhodujúcich faktorov z pohľadu používania webových služieb v praxi.**

## O čo ide?

Môžeme to prezradiť vopred, hoci určite všetci poznáme správnu odpoveď už teraz... Samozrejme, ako vždy ide o peniaze! Každá komerčná firma alebo organizácia prirodzene vzniká s cieľom produkcie zisku a zarábania peňazí. Aby tento cieľ bola firma schopná dosiahnuť, musia v nej fungovať obchodné procesy. Týchto obchodných procesov je veľké množstvo. Mimoriadne dôležitá je však ich vzájomná integrácia. Uveďme si ilustratívny príklad.

Predstavme si fiktívnu firmu, v rámci ktorej pracujú (okrem iných) dve oddelenia, a to oddelenie vývoja a oddelenie predaja. V rámci obidvoch oddelení fungujú prepracované, sofistikované a pre náš príklad môžeme predpokladať, že dokonca ideálne obchodné procesy. Oddelenie vývoja je schopné v rekordnom čase a v mimoriadnej kvalite vyvinúť nový produkt presne v súlade s požiadavkami zákazníka. Oddelenie predaja je schopné v rekordnom čase dopraviť každý produkt k zákazníkovi presne podľa jeho želaní. Všetko vyzerá ideálne, ale predsa len jedno ohnivko v tejto reťazi chýba. Ak totiž nie sú obidva uvedené procesy vzájomne integrované, tak sa oddelenie predaja nedozvie včas, že nový produkt je hotový. Tým dochádza k časových stratám, ktoré môžu mať vážne dôsledky, ako napr. finančné straty, nepotrebné viazanie zdrojov, znižovanie dôvery zákazníkov. Naopak, rýchla integrácia obchodných procesov prebiehajúcich tak vo vnútri firmy alebo organizácie, ako aj pri spolupráci s obchodnými partnermi a zákazníkmi, znamená rýchlejšie poskytovanie kvalitných služieb zákazníkom, a tým vyššie zisky, viac voľných zdrojov, vyššiu produkciu a v konečnom dôsledku aj lepšiu kvalitu.

Poukázali sme na význam integrácie obchodných procesov. Táto skutočnosť však nie je novým objavom. Mení sa len prístup k tejto integrácii a spôsob jej zabezpečenia. Kým v minulosti sa tento cieľ dosahoval centralizáciou a automatizáciou spracovania v rámci mainframových systémov, neskôr presunom rozhodovania a spracovania k jednotlivcovi v rámci aplikácií typu klient/server, tak teraz sme sa cez internet, aplikácie e-business a webové portály dostali až k súčasnej integrácii informácií, aplikácií a celých obchodných procesov do sieťového webového prostredia prostredníctvom tzv. webových služieb.

## 1. Webové služby

Webové služby ako služby poskytované v internetovom prostredí vytvárajú potrebný rámec na zabezpečenie interoperability. Sú technologickým základom na integráciu kľúčových obchodných procesov v rámci vnútornej siete firmy alebo organizácie a cez internet (prípadne inú externú sieť) aj s dodávateľmi a klientmi. Používanie webových služieb v praxi umožnila všeobecná akceptovateľnosť dvoch štandardov, a to TCP/IP (Transmission Control Protocol/Internet Protokol) a XML (eXtensible Markup Language). Štandard TCP/IP predstavuje súbor protokolov, ktoré (zjednodušene povedané) slúžia na transfer dát medzi vzdialených počítačmi.

Samotným jadrom webových služieb je jazyk XML, ktorý vlastne definuje syntax na reprezentáciu dát. Táto syntax je ľahko generovateľná a zároveň ľahko čitateľná. Preto predstavuje flexibilný spôsob, ako vytvoriť spoločný formát na zdieľanie informácií a údajov a zároveň flexibilný spôsob zdieľania tohto formátu spolu s príslušnými informáciami a dátami prostredníctvom webu. XML preto v konečnom dôsledku umožňuje zdieľanie informácií konzistentnou cestou cez aplikácie, čím štandardizuje výmenu dát.

Z technologického pohľadu sa XML skladá z dvoch častí. Je to tzv. XML Base a tzv. XML Protocol. Bez toho, aby sme zachádzali do technologických detailov uveďme len, že XML Base definuje samotný dokument XML (alebo správu). Na druhej strane protokol XML špecifikuje samotnú výmenu XML dokumentov.

## 2. Bezpečnosť webových služieb

Uviedli sme, v čom spočíva sila XML z pohľadu rozširovania prístupu k informáciám a obchodným procesom. Toto rozširovanie však zároveň znamená širší prístup k citlivým informáciám. Prostredníctvom správ na báze XML sú napríklad zdieľané objednávky, faktúry a čísla kreditných kariet. Preto sa, prirodzene, zároveň zvyšuje riziko vážnej straty vyplývajúce z možnej kompromitácie alebo vyzradenia týchto informácií.

Z uvedeného je zrejmé, že webové služby nemôžu v každodennej praxi uspieť bez implementácie príslušných bezpečnostných mechanizmov. Je potrebné zabezpečiť utajenie, integritu a dostupnosť príslušných správ XML a zároveň dostatočne zabezpečiť proces autentizácie a autorizácie. Objasnime si uvedené pojmy na príklade.

Predstavme si, že prostredníctvom webových služieb, teda formou správy XML, je zasielaná faktúra na finančné oddelenie. Počas samotného prenosu je potrebné túto správu ochrániť pred vyzradením jej obsahu (pričom nezáleží, či by išlo o náhodné alebo úmyselné odchytenie faktúry), a teda je potrebné zabezpečiť jej utajenie. Počas transferu správy XML môže dôjsť k jej úmyselnej alebo neúmyselnej modifikácii. Je preto dôležité, aby bolo možné v ľubovoľnom čase overiť, či k tomu došlo alebo nie. Tento proces nazývame overením integrity správy. Po príchode faktúry na finančné oddelenie je ďalej potrebné overiť, či príslušný pracovník finančného oddelenia je oprávnený danú faktúru spracovať. Na to je potrebné najprv overiť jeho identitu (tzv. proces autentizácie) a vzápätí treba overiť aj to, či má samotné oprávnenie na spracovanie (tzv. proces autorizácie).

Zabezpečiť dostupnosť v súvislosti s webovými službami je rovnako dôležité. Možno ju však zabezpečiť iba štandardnými technolo-

gickými opatreniami (ako napr. redundancie, zrkadlenia a pod.) a z tohto pohľadu je uvedená problematika mimo zamerania nášho článku.

Je potrebné pripomenúť, že sme uviedli iba základné bezpečnostné požiadavky a že existuje mnoho ďalších, ako napr. požiadavka na zabezpečenie neodopretia pôvodu (v súvislosti s naším príkladom faktúry by to znamenalo, že je možné dokázať, že faktúru skutočne odoslal ten, kto ju odoslal, pričom dotyčná osoba nemôže tento fakt nijako poprieť).

Bohužiaľ z pohľadu bezpečnosti musíme konštatovať, že webové služby nemajú štandardne implementované bezpečnostné mechanizmy, ktoré by zabezpečili spomínané bezpečnostné požiadavky. Ako sme však už uviedli, ich implementácia je mimoriadne dôležitá v záujme obchodného úspechu každého podnikajúceho subjektu. Je preto nevyhnutné tieto mechanizmy do webových služieb dodatočne implementovať.

### 3. XML Security

Prirodzenou odpoveďou na špecifikované bezpečnostné požiadavky bolo rozšírenie samotného XML o ďalšiu časť, ktorá dopĺňa existujúce XML Base a XML Protocol. Touto časťou je XML Security, ktoré samotné sa skladá z 5 častí, a to:

- XML Signature (XS),
- XML Encryption (XE),
- XML Key Management Specification (XKMS),
- Security Assertion Markup Language (SAML),
- XML Access Control Markup Langugage (XACML).

XS špecifikuje schému XML pre kryptograficky autentizované dáta. Autentizovať je pritom možné celý dokument XML, samostatné časti dokumentu, alebo dokonca externé dátové objekty, na ktoré dokument XML iba odkazuje.

XE špecifikuje schému pre šifrovanie dát. Opäť je možné šifrovať celý XML dokument, samostatné časti dokumentu, alebo dokonca externé dátové objekty, na ktoré dokument XML iba odkazuje.

XKMS definuje dôveryhodné webové služby pre manažovanie kryptografických kľúčov, a to vrátane kľúčov verejných. Vo všeobecnosti definuje 3 druhy služieb:

- XML Key Information Service Specification (X-KISS) – podporuje služby súvisiace s používaním kryptografických kľúčov (napr. lokalizácia, overenie platnosti),
- XML Key Registration Service Specification (X-KRSS) – podporuje služby používané držiteľom kryptografických kľúčov (napr. registrácia, rušenie platnosti, obnova kľúča, vydanie nového kľúča),
- Bulk Key Registration (X-Bulk) – ide o rozšírenie X-KRSS umožňujúce hromadnú registráciu.

SAML slúži na špecifikáciu a zdieľanie dát použitých na rozhodnutie o autorizácii (tzv. dôveryhodných tvrdení). Ide napríklad o schválené roly a certifikáty. Ako príklad môžeme uviesť situáciu, keď sa používateľ prihlási a autentizuje do systému. V tom čase vzniká tzv. autentizačné tvrdenie. Toto tvrdenie je potom ďalej v rámci systému zdieľané a je použité pri použití ďalšieho systému bez nutnosti opätovnej autentizácie samotným používateľom.

XACML je ďalším rozšírením SAML, ktoré umožňuje priamo špecifikovať politiku riadenia prístupu.

### 4. Webové služby verZus PKI

Teraz sme v situácii, keď už máme implementované bezpečnostné mechanizmy, ktoré nám dokážu zabezpečiť vyššie špecifikované bezpečnostné požiadavky. S kryptografickými kľúčmi už XML Security dokáže tieto požiadavky zabezpečiť. Stále nám však ostáva jeden problém, a tým je celkový manažment kryptografických kľúčov.

Ako sme už uviedli, XKMS definuje služby pre manažovanie kľúčov. Môžeme preto veľmi jednoducho použiť symetrické šifrovanie, ktoré zjednodušene znamená použitie jedného tajného kľúča na komunikáciu medzi dvojicou PC. To ale znamená, že už pri 10 počítačoch budeme na úplnú komunikáciu potrebovať 45 šifrovacích kľúčov! Hneď je zrejmé, že je naozaj pravda, že oveľa efektívnejšie je použitie asymetrickej kryptografie, ktoré znamená použitie páru kľúčov pre každé PC. Pri 10 počítačoch to znamená použitie iba 10 párov kľúčov na úplnú komunikáciu. Jeden z týchto kľúčov je tajný a označuje sa ako súkromný. Druhý je verejný a všeobecne dostupný v otvorenej forme každému. S využitím známeho verejného kľúča je každý schopný zašifrovať správu pre majiteľa tohto kľúča. „Matematika“ v pozadí nám zaručuje, že dešifrovať túto správu je možné iba prislúchajúcim súkromným kľúčom, a to znamená, že správu je schopný dešifrovať iba majiteľ tohto kľúča.

Bez zachádzania do ďalších detailov si uveďme, že existuje prepracovaná infraštruktúra na manažovanie takýchto súkromných kľúčov. Určite sa už každý stretol s pojmom PKI (z angl. Public Key Infrastructure), ktorým sa táto infraštruktúra označuje. Ide v súčasnosti jednoznačne o najkvalitnejšiu infraštruktúru na manažovanie kryptografických kľúčov.

PKI predstavuje kvalitnú bezpečnostnú infraštruktúru. Cenou za ňu je však jej komplikovaná implementácia. Ďalšou nevýhodou je potreba úpravy aplikácii alebo vývoja nových aplikácii schopných s touto infraštruktúrou spolupracovať.

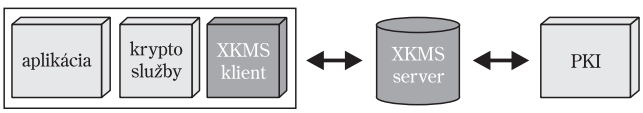
Na druhej strane máme webové služby, ktoré majú nedostatočnú bezpečnosť, ale majú široké možnosti aplikácií. Ako sme už uviedli, webové služby umožňujú sústrediť sa priamo na biznis a obchodné skúsenosti, a nie na vývoj špeciálneho typu aplikácií.

Z uvedeného prirodzene vzniká myšlienka prepojenia webových služieb s PKI. Umožnilo by to využiť kvalitnú bezpečnostnú infraštruktúru na zaručenie bezpečnosti a zároveň by to odbúralo potrebu vývoja špeciálnych aplikácií, nakoľko by stačilo priamo využiť webové služby. Je však takéto prepojenie vôbec možné?

Našťastie, odpoveď na túto otázku je kladná. Integráciu PKI do webových služieb totiž hravo rieši XKMS! A navyše takým spôsobom, že táto integrácia je „neviditeľná“ pre implementáciu webových služieb (a teda vývojárov). Webové služby priamo komunikujú iba so serverom XKMS, ktorý potom zabezpečuje spoluprácu s PKI. XKMS teda vlastne poskytuje outsourcing PKI. Celá situácia je znázornená na obr. 1.

S využitím XKMS vieme teda priamo vo webových službách napríklad registrovať používateľa, rušiť platnosť kľúčov, obnovovať kľúče, vydávať nové, lokalizovať ich a overovať platnosť kľúčov. A to všetko bez potreby vývoja špeciálnych aplikácií. Všetko dokážeme zabezpečiť priamo použitím webových služieb.

Uveďme praktický príklad. Predstavme si, že máme vyvinutú obchodnú aplikáciu, ktorá umožňuje elektronicky podpísať objednávku. Ide o webovú aplikáciu. Z pohľadu používateľa je teda všetko jednoduché, celú transakciu dokáže realizovať priamo v internetovom prostredí. Avšak s jednou veľkou výnimkou. Pri prvom použití tejto aplikácie musí používateľ aplikáciu opustiť a priamo požiadať „nejakú“ certifikačnú autoritu (t. j. poskytovateľa certifikačných služieb, a teda služieb súvisiacich s manažovaním kľúčov) o vydanie certifikátu. Štandardne to znamená, že používateľ musí navštíviť webovú stránku certifikačnej autority. Táto situácia sa zásadne mení použitím XKMS. Prostredníctvom XKMS je totiž priamo aplikácia schopná generovať kľúčový pár, registrovať sa u cer-




**Obr.1 Outsourcing PKI s využitím XKMS**

tifikačnej autority a získať certifikát. Celý proces prebieha automaticky a pre samotného používateľa „neviditeľne“.

## 5. HAS – Príklad použitia

Konkrétny príklad použitia webových služieb s využitím PKI v praxi je možné nájsť v [4]. Bezpečné webové služby sú využité pre autentizačné služby v rámci systému zdravotnej starostlivosti (HAS – z angl. Healthcare Authentication Service). Ide o poskytovanie citlivých dát laboratórnym špecialistom na základe ich autentizácie a autorizácie. Pre tento systém existuje webová stránka tvoriaca rozhranie HTML pre webové služby, ktoré bezpečným spôsobom zaisťujú transfer zdravotných záznamov autorizovaným odborníkom. Webové služby využívajú XKMS na overenie platnosti certifikátu príslušného odborníka. Následne je využitý SAML na získanie bezpečnostného profilu tohto odborníka. Po autentizácii je profil skladajúci sa z dôveryhodných tvrdení vrátený webovým službám vo forme správy SAML. Webové služby následne overia prístupové práva a v prípade, že je prístup odborníka k citlivým dátam povolený, sú mu tieto dáta bezpečným spôsobom zaslané. Podrobnejšie informácie je možné nájsť priamo v [4].

## Záver

Ukázali sme, že webové služby s využitím PKI ponúkajú „to najlepšie z dvoch svetov“:

1. komunikačné a integračné atribúty XML,
2. bezpečnostné služby na báze PKI,
3. „neviditeľnosť“ PKI pre implementáciu webových služieb (a teda pre vývojárov).

## Literatúra

[1] BROWN, A.: Create Secure Web Services With PKI.. netMagazine, 2002.

[2] Delivering Web Services Security: The Entrust Secure Transaction Platform. Entrust, Inc., 2002.

[3] Streamlining PKI for Web Services. Baltimore Technologies plc., 2002.

[4] VeriSign Digital Trust Services: Enabling Trusted Web Services. VeriSign, Inc., 2002.

**RNDr. Marcel Zanechal, PhD.**

**Tempest, s. r. o.**
**Landererova 1**
**811 09 Bratislava**
**Tel.: 02/50 26 71 11**
**e-mail: marcel_zanechal@tempest.sk**