

"PROJEKT vOKO™2004" – XML ROZHRAŇÍ VE SLUŽBÁCH IS APA

(Projekt "vOKO" – IV.)

Dr. Ing. Vladimír Strnad
PDS s.r.o.
Viniční 20, 615 00 Brno
Email: v.strnad@pds.cz

Úvod: webové služby a XML rozhraní

Webové služby využívající nejnovější internetový formát XML patří k nejmodernějším principům výměny dat ve stále otevřenějším informačním světě. Implementace doplňujících technologií standardizovaných okolo zmíněného formátu XML – tedy XML schéma (XSD), XSL transformace, a další, umožňují významnou měrou automatizovat komunikační procesy v rámci rozsáhlých projektových řešení. Využití jednoho z doplňujícího standardu – "XML signature" pak umožňuje dosáhnout vysoké úrovně bezpečnosti příslušného systému prostřednictvím aplikace autentizačních mechanismů a vyšších norem bezpečnosti zpráv prostřednictvím digitálního podpisu.

Projekt vOKO™2004

Nejnovější generace aplikačně-serverového řešení nezávislého komunikačního XML rozhraní vyvíjeného v rámci interního projektu vOKO™ firmy PDS již od roku 1999 (viz [1], [2] a [3]) je v současné době již vysoce výkonným a robustním nástrojem využívajícím právě výše uvedené technologie webových služeb postavených okolo standardu XML. V posledních měsících vývoje bylo celé schéma řešení doplněno o interní doplňující šifrovací a identifikační mechanismy výrazně zvyšující bezpečnost celého systému, podstatným způsobem byly dopracovány systémové prvky archivace celého spektra komunikačních procesů, stejně jako skupina interních monitorovacích prvků zajišťujících mnohem flexibilnější správu vlastního monitoringu provozu serverové části. Celé řešení se tak stalo velmi výkonným komunikačním systémem s rozsáhlými možnostmi vlastního nastavení dle požadavku zákazníka.

Projekt vOKO™ je interním vývojovým projektem společnosti PDS s.r.o., jehož prezentace (první dokumentovaný a veřejně prezentovaný přenos dat ve formátu XML v resortu zemědělství, s velkou pravděpodobností i v celém IS VS) byla v listopadu 2000 impulsem pro zahájení projektu „XML Rozhraní IS CEDR a dalších IS pro evidenci dotací na registry UIR-ADR a ARES realizované on-line prostřednictvím síťového prostředí GOVBONE/Internet“ na Ministerstvu financí a byl jednou z klíčových součástí tohoto projektu. Aplikační vybavení vyvinuté v rámci tohoto projektu bylo první, prostřednictvím kterého bylo realizováno komunikační spojení s využitím autentizačních prvků digitálního podpisu.

Základní principy a technologické schéma řešení

Celé systémové řešení komunikací prostřednictvím „XML rozhraní“ je postaveno na několika základních požadavcích a principech:

- Maximální otevřenost celého řešení
- Nezávislost na DB/OS platformách příslušných systémů
- Model KLIENT-SERVER/SLUŽBA
- Primární schéma komunikace: DOTAZ-ODPOVĚĎ (request-response model)
- Maximální bezpečnost systému a autorizovaný přístup

Maximální otevřenost celého řešení - celé řešení je v maximální možné míře vyvíjeno jako kombinace obecných otevřených standardů primárně z oblasti nejnovějších internetových technologií (postavených především okolo nejmodernějšího formátu XML) doplněných pouze v míře nezbytné o interní řešení (aplikováno především v oblasti bezpečnosti).

Základní standardy:

- (1) **XML 1.0 (standard W3C)** – standard pro základní formát dat, nezávislý na softwarové platformě a hardwarovém řešení. Primárním znakem dokumentu XML je oddělení dat od procesů. Vlastní XML dokument nenese žádnou informaci o tom, jak s daty nakládat.
- (2) **XML Schema (standard W3C)** – standard pro definici pravidel, podle kterých se řídí struktura i obsah XML dokumentů. Standardizaci XML dokumentů je možno dělit přinejmenším do dvou úrovní: (a) standardizace datových typů a (b) standardizace celých dokumentů (jedná se o vyšší úroveň standardizace, kdy schéma dokumentu je materializací dohody mezi komunikujícími subjekty o tom, která data a v jakém formátu se budou mezi nimi přenášet). Aktuálně se využívá několika-úrovňová hierarchie XML schémat pro validaci oboustranně přenášených dokumentů.
- (3) **XSL(T) (standard W3C)** – standard pro transformaci XML dat do jiného formátu. Pro účely „XML rozhraní“ je jazyk XSLT využit dvěma způsoby: (a) pro transformaci XML dokumentů, a (b) pro doplňkovou validaci pomocí XSLT šablon. V některých případech je validace XML dokumentů pomocí XML schémat slabá. Řešením, založeným na XML, je použití validačních XSLT šablon.

Standardy pro interkonektivitu a bezpečnost:

- (4) **Komunikační protokoly (HTTP(S), (S)MIME)** - pro přenos zpráv XML rozhraní je v současné době používán přenosový protokol HTTP (resp. HTTPS) a v nejbližší době se předpokládá využití protokolů SMTP–MIME (resp. SMTP–S-MIME).

- (5) **SOAP (standard W3C)** – protokol, sloužící k výměně informací v decentralizovaném distribuovaném prostředí, založený na XML. SOAP je obecně obálkou pro vlastní přenášaná data. Umožňuje definovat logiku zpracování zprávy včetně ošetření chyb.
- (6) **BizTalk (standard biztalk.org)** – standard, založený na XML, sloužící k integraci obchodních aplikací a k elektronickému obchodování. Zahrnuje implementaci XML schémat a vlastní sadu XML značek, sloužících k zasílání zpráv mezi aplikacemi. Definuje schéma výměny informací včetně obousměrné komunikace, vynucení odpovědí a zpřesnění definice životního cyklu dokumentů.
- (7) **XML Signature (standard W3C)** – standard pro elektronický podpis ve formátu XML. Specifikuje syntaxi a pravidla zpracování při tvorbě a použití digitálních podpisů XML dokumentů. Podpis ve formátu XML Signature je element XML, nesoucí veškerá relevantní data, vložený do záhlaví SOAP.

Nezávislost na DB/OS platformách komunikujících systémů - nezávislost na DB/OS platformách

komunikujících systémů je jednou ze základních vlastností XML rozhraní. Svým fyzickým oddělením od vlastního systému a zajištěním funkčnosti systémem vazeb s vlastním zdrojem zajišťuje skutečnou nezávislost komunikujících stran na systémovém i databázovém prostředí jednotlivých propojených IS.

Model KLIENT-SERVER/SLUŽBA – celé řešení „XML rozhraní“ je postaveno na schématu „KLIENT-

SERVER/SLUŽBA“. **Serverem** je v tomto případě míněna sdílená „čekačí“ aplikace vystavená na definované HTTP(S) adrese (případně komunikující prostřednictvím jiného protokolu – například (S)MIME), která zprostředkovává komunikaci mezi klientem a službou. **Služba** – je přesně definovaná funkce (programově definovaný prvek) příslušného serveru provádějící na vyžádání klienta přesně definovanou akci. **Klient** žádá službu o nějakou akci (poskytnutí dat, vložení zaslaných dat apod.). Klienti pouze vznášejí požadavky na služby a nenaslouchají ostatním účastníkům. Pokud chtějí využívat konkrétních služeb, musejí při komunikaci s nimi dodržovat pravidla, stanovená službou. Klientem může být "živý" koncový uživatel vybavený patřičným uživatelským rozhraním (SW, aplikací), nebo jiná aplikace (vyhodnocování provádí přímo „logická“ část aplikace bez zásahu uživatele).

Základní schéma komunikace: DOTAZ-ODPOVĚĎ (request-response model) – základní schéma

komunikace prostřednictvím XML rozhraní je dvoufázový režim „dotaz-odpověď (request-response proces)“. To znamená, že klient (klientská aplikace) zasílá dotaz na definovanou adresu příslušné aplikace, která po kontrole oprávněnosti přístupu (autentizaci a autorizaci přístupových práv) a získání příslušných dat z připojených zdrojů vytvoří odpověď v předem definovaném formátu a tuto odpověď pošle zpět klientovi. Tím je jeden komunikační cyklus uzavřen.

Bezpečnost systému – celý systém je navržen (a v současné době realizován) tak, aby bylo možno implementovat široké spektrum bezpečnostních požadavků:

- **Důvěrnost** komunikace je zajištěna pomocí protokolu HTTPS.

- **Integrita** přenášených dat je zajištěna pomocí HTTPS, a na obou stranách prověřována kontrolními HASH funkcemi.
- **Identifikace a autentizace** pro následnou **autorizaci** je řešena pomocí osobních certifikátů. Pouze registrovaní uživatelé jsou oprávněni podávat požadavky na službu. V rámci projektu vOKO™2004 jsou pak implementovány vlastní doplňující autentizační a autorizační mechanismy.
- **Nepopíratelnost** je řešena pomocí XML Signature (digitální podpis).

Celé řešení XML rozhraní v rámci projektu vOKO™2004 je v současné době doplněno o interní mechanismus šifrování dat, které umožňuje šifrování jak na úrovni specifikovaných koncových elementů, tak na úrovni celých přenášených dokumentů. Dále je využito interního schématu doplňující identifikace výrazně zvyšujícího bezpečnost celého identifikačního a autentizačního procesu. Předpokládá se také implementace služby externích autorizačních databází (EAD) pro autentizaci uživatelů, a to především ve spolupráci s Ministerstvem financí.

Sdílený komunikační server XML rozhraní MZe

V posledních měsících se právě výše uvedené XML rozhraní (vyvíjené v rámci projektu vOKO™2004) stalo jedním z klíčových prvků budoucího informačního systému "agrární platební agentury" (IS APA) aplikujícího principy integrovaného administrativního a kontrolního systému (IACS). Komunikační systém XML rozhraní je ve schématu uvedeného IS zprostředkujícím subsystémem celého komplexu IS APA realizující informační vazby mezi jednotlivými administrativními systémy APA a klíčovými registry MZe (IRZv, LPIS, ...). Vlastní rozhraní je v současné době nejen vlastním "přenosovým" systémem, ale definované komplexní služby již v mnoha případech přebírají logickou stránku zpracování dat pro potřeby kooperujících systémů.

Literatura

- [1] Strnad, V. – Oujezdský, P.: Projekt "vOKO" – vize připojení IS MZe na vnější informační zdroje. In: Sborník konference "Informační systémy v zemědělství a lesnictví". HELP SERVICE – Education, s. r. o., Seč u Chrudimi, 2001, str. 79 – 82.
- [2] Strnad, V. – Oujezdský, P.: Projekt "vOKO" – model nezávislého analytického a kontrolního systému. In: Sborník konference "Informační systémy v zemědělství a lesnictví". HELP SERVICE – Education, s. r. o., Seč u Chrudimi, 2002, str. 57 – 61.
- [3] Strnad, V. – Oujezdský, P.: Projekt "vOKO" – alternativy vyhodnocování informací v administrativně-kontrolních procesech (nejen) ve státní správě. In: Sborník konference "Informační systémy v zemědělství a lesnictví". HELP SERVICE – Education, s. r. o., Seč u Chrudimi, 2003, str. 36 – 37.