Securitatea serviciilor Web

Conf.dr. Razvan Daniel ZOTA
Catedra de Informatica Economica, A.S.E. Bucuresti

The new revolution within the Internet is on delivering information to systems (not only information to people). In this context, Web services are the methods with which businesses will drive system-to-system communication. By using a common language (XML) and a common transport protocol (HTTP), Web services act as a broker between two endpoints that wish to communicate. This communication must be secure; thus, an important focus is on Web services security. We present in this article the security specifications which are being developed to help promote secure Web services deployments.
Keywords: *Web Services, web services security, XML, XKMS, SAML.*

Introducere

Serviciile Web (Web Services) descriu o modalitate de acces la date si interactiunea cu programe ce ruleaza pe diferite platforme de operare în cadrul retelelor publice si de întreprindere. Spre deosebire de retelele extranet tipice, ce necesita interfete puternic integrate între membrii comunicarii, scopul serviciilor Web este acela de a oferi o singura interfata comuna care sa permita calculatoarelor sa ruleze programe, sa partajeze date si sa acceseze servicii diverse. Bazate pe un limbaj comun (XML) si un protocol comun de transport (HTTP), serviciile Web actioneaza ca un intermediar între cele doua entitati ce doresc sa comunice între ele.

Serviciile Web sunt bazate pe limbaje si protocoale specifice (în afara de XML si HTTP), printre care, cele mai cunoscute sunt: Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) si Universal Discovery, Description and Integration (UDDI). SOAP este practic un mecanism de transport pentru mesajele XML. Un plic SOAP este utilizat pentru a transporta mesaje XML ce includ date sau programe de-a lungul unei retele, de regula prin HTTP. UDDI este un registru bazat pe XML ce permite furnizorilor sa prezinte serviciile Web pe Internet. WSDL (care este bazat tot pe XML) reprezinta o modalitatea de descriere de conexiune a clientilor (dintr-o perspectiva software) la furnizorii de servicii Web. Împreuna cu XML si HTTP, aceste protocoale reprezinta fundamentul pe care se sprijina serviciile Web, permitând diverselor entitati sa caute si sa prezinte servicii, sa apeleze proceduri, sa ruleze programe si sa întoarca rezultate.

Necesitati de securitate

Credem ca nu mai este nevoie de o pledoarie în favoarea securitatii datelor, mai ales când este vorba de date sensibile care sunt transmise între cele doua entitati ce comunica. În general, serviciile Web asigura autentificarea, autorizarea, confidentialitatea si integritatea datelor. Autentificarea reprezinta procedeul prin care se stabileste identitatea uneia dintre partile implicate în comunicare. Dupa ce procesul de autentificare a luat sfârsit, autorizarea stabileste care sunt drepturile de actiune pentru acea entitate. Confidentialitatea implica faptul ca mesajele transmise de partile implicate în comunicare sunt transparente pentru alte entitati, fie intentionat sau nu. Cel mai utilizat mecanism pentru asigurarea confidentialitatii este criptarea. Integritatea presupune ca datele transmise nu au fost alterate – ele sunt primite de catre destinatar exact asa cum au fost trimise de expeditor – acest lucru se face prin intermediul semnaturilor digitale.

Noi specificatii de securitate

Serviciile Web sunt protejate de o serie de noi specificatii de securitate, printre care: XML Encryption, XML Signature, XML Key Management Specification (XKMS), Security Association Markup Language

(SAML) si Web Services Security (WS-Security). Aceste noi specificatii se bazeaza pe mecanisme dezvoltate anterior (cum ar fi Public Key Infrastructure - PKI) pentru a asigura elementele de securitate pentru mesajele XML si transportul SOAP.

Criptarea XML

Criptarea XML (XML Encryption) reprezinta o specificatie dezvoltata de Consortiul World Wide Web (www.w3.org) care descrie procesul criptarii datelor si reprezentarea acestora în format XML. Aplicatiile care respecta aceasta specificatie trebuie sa asigure criptare simetrica si asimetrica, precum si algoritmi uzuali de criptare ca AES (Advanced Encryption Standard) sau Triple DES. Specificatia XML Encryption precizeaza ca implementarile ofera suport pentru standarde uzuale de chei de criptare, precum Diffie-Hellman. De asemenea, în cadrul acesteia se definesc mecanisme pentru criptarea întregului mesaj sau doar a unei parti a acestuia. Acest lucru permite un acces flexibil la datele din cadrul mesajelor XML. Într-o tranzactie cu o carte de credit, spre exemplu, o aplicatie poate necesita acces la numele clientului, numarul cartii de credit, limita de credit si nu acces la alte informatii, cum ar fi cele legate de alte achizitii. Un alt tert implicat în tranzactie poate sa aiba acces doar la numele clientului si la limita de credit, nimic în plus.

Semnatura XML

Semnatura XML este o specificatie elaborata de W3C si IETF si reprezinta o metoda de reprezentare a semnaturilor digitale folosind sintaxa XML. De asemenea, tot aici se descriu procedurile de calcul si de verificare a acestor semnaturi. O semnatura digitala asigura integritatea si autentificarea mesajului. Aceasta este creata prin rularea unui algoritm *hash* pe un set specific de date (document) si criptarea mesajului rezultat cu cheia privata de expeditorului. Destinatarul ruleaza acelasi algoritm *hash* asupra documentului ce conduce la un alt rezultat al mesajului. Destinatarul utilizeaza acum cheia publica a expeditorului pentru a decripta primul mesaj rezultat. Daca cele doua rezultate coincid, atunci expeditorul este asigurat ca datele au fost receptionate corect. O componenta importanta în cadrul specificatiei Semnaturii XML este aducerea la forma canonica. Metodele clasice de analiza morfologica pot duce la pierderea de informatii neesentiale într-un mesaj XML sau poate duce la schimbarea prezentarii acestuia chiar daca sensul ramâne acelasi. Acest lucru reprezinta o problema pentru semnaturile digitale deoarece, daca analizorul morfologic modifica chiar si cu un bit mesajul XML, rezultatul calculat la destinatar va fi diferit de cel de la expeditor si astfel mesajul nu va fi autentificat. Aducerea la forma canonica creeaza o forma denormalizata a documentului. Într-o tranzactie expeditorul creeaza si semneaza o forma canonica a documentului, apoi se trimite atât documentul cât si varianta semnata. Destinatarul aduce la forma canonica documentul si apoi compara rezultatul obtinut cu forma semnata.

XML Key Management Specification (XKMS)

Specificatia XKMS este, de asemenea, redactata de W3C si descrie procesul de distributie si înregistrare a cheilor publice utilizate împreuna cu Semnatura XML si specificatiile de Criptare XML. Scopul acestei specificatii este acela de a simplifica modalitatea de validare a unei aplicatii, evitându-se schema complicata PKI. Acest lucru presupune faptul ca, decât sa se forteze validarea unui certificat digital sau sa se verifice statutul sau, aplicatia poate pasa aceste functiuni unui tert de încredere. XKMS are doua sub-componente: XML Key Information Service Specification (X-KISS) si XML Key Registration Service Specification (X-KRSS).

X-KISS defineste protocolul prin care un serviciu de încredere specifica informatia de chei publice implementata de specificatia XML Signature. În consecinta, X-KISS permite unei aplicatii sa devina client al unui tert – de regula o autoritate de certificare sau un furnizor de servicii. Acest tert poate manipula activitatile legate de PKI. X-KISS este compatibil cu standardul X.509 de certificate digitale si sistemul de chei PGP (Pretty Good Privacy).

X-KRSS descrie procesul prin care un serviciu Web înregistreaza informatia de chei publice. Perechile de chei publice înregistrate prin intermediul X-KRSS pot fi utilizate împreuna cu X-KISS si alte servicii de autorizare. Daca un client genereaza perechea de chei, X-KRSS necesita dovada ca acel client detine cheia privata. Daca serviciul de înregistrare genereaza cheia pereche, specificatia ofera o modalitate de a transmite cheia privata direct clientului. Protocolul de înregistrare poate fi, de asemenea, utilizat pentru refacerea unei chei private atunci când este cazul. În plus, un client al unui serviciu de înregistrare poate face o cerere ca o anumita informatie sa fie legata de o cheie publica (un nume, identificator sau alt atribut). X-KRSS specifica înregistrarea cheilor RSA si DSA. Are, de asemenea, un cadru pentru extinderea procesului de înregistrare pentru a oferi suport si altor algoritmi, precum Diffie-Hellman sau criptografia folosind curbe eliptice.

SAML (Security Asserion Markup Language)

Acest standard este dezvoltat de Organizatia OASIS (Organization for the Advancement of Structured Information Standards) la initiativa companiilor IBM, Microsoft si VeriSign si reprezinta un sistem pentru asigurarea schimbului de informatii legate de securitatea unui subiect (persoana sau calculator), folosind HTTP. Aceste informatii sunt legate de actiunile legate de autentificarea subiectului, atribute si decizii de autorizare referitoare la accesul la resurse. Un scop major a specificatiei SAML este facilitarea SSO (Single Sign-On) în care autentificarea la un domeniu ofera acces la resurse din alte domenii fara a fi necesara o reautentificare. Conform specificatiilor SAML, informatiile cu privire la autorizare pot fi eliberate de doua tipuri de autoritati: autoritati de autentificare si autoritati de atribuire. Aceste autoritati (cunoscute sub numele de *puncte de decizii politice*) se pot baza pe surse de informatii externe pentru a elibera informatiile necesare – astfel de surse de informatii pot fi asa numitele magazine de politici. Utilizând protocoalele descrise în SAML, clientii folosesc cereri bazate XML pentru a aduna informatii de la autoritati. În prezent, SAML defineste comunicatii SOAP peste HTTP, dar poate fi deschis pentru a oferi suport pentru alte protocoale de transport. Parte integrala a fenomenului de autentificare, SAML poate indica metoda de autentificare folosita de mesaj, cum ar fi o parola, bilet Kerberos, jeton hardware sau certificat digital X.509. Acest lucru nu permite însa abilitatea de a face efectiv autentificarea. SAMS permite atribuirea unei perioade de timp sa fie aplicata informatiei. Aceasta valoare poate specifica fie perioada pentru care informatia este valida fie momentul la care expira. Informatiile care nu poseda o astfel de valoare se presupun ca sunt valide un timp nedefinit.

WS-Security

Specificatia Web Services Security dezvoltata tot de Organizatia OASIS se ocupa cu schimbul securizat de mesaje SOAP. Se permite aplicatiilor sa ataseze o semnatura digitala si headere de criptare mesajelor SOAP pentru integritate si confidentialitate. Atât header-ul cât si corpul mesajului SOAP pot fi criptate sau semnate, precum si alte entitati atasate mesajului SOAP. Specificatia descrie mecanisme de atasare a unor jetoane de securitate mesajelor SOAP. Aceste jetoane de securitate includ o varietate de informatii de securitate, de la nume de utilizatori pâna la certificate digitale X.509 sau tichete Kerberos. Jetoanele de securitate sunt folosite pentru a valida pretentiile exprimate de expeditor. De exemplu, un mesaj SOAP poate pretinde sa aiba acces la anumite resurse de calcul. Capetele comunicarii pot aplica politici de securitate pentru a cere jetoane speciale de securitate pentru validarea unor astfel de pretentii. WS-Security coopereaza cu specificatiile XML Signature si XML Encryption. De asemenea, ofera suport pentru utilizarea modelelor de securitate standard precum PKI, Kerberos, SSL (Secure Socktes Layer)/TLS (Transport Layer Security).

Pe lânga aceste specificatii mai exista si altele în faza de proiectare, printre care WS-Policy (descrie politicile de securitate dintre

corespondenti), WS-Trust (face referire la modele de încredere pentru o interoperare securizata) si WS-Privacy (permite furnizorilor de servicii Web sa-si stabileasca preferinte si practici personale).

Bibliografie

- Conry-Murray A. – *Web Services Security Specifications* – Network Magazine, URL: http://www.networkmagazine.com/article/NMG20021223S0014, 6 Ianuarie 2003
- Frandsen E., Kochmer C. – *Understanding Web Services* – Addison Wesley Professional, online: www.informIT.com, 9 August 2002
- http://www.oasisopen.org/committees/security/
- http://www.w3.org
- Skonnard A. – *The Birth of Web Services* – MSDN Magazine, Octombrie 2002, http://msdn.microsoft.com/msdnmag/issues/02/10/xmlfiles/default.aspx
- DevelopMentor - *Understanding Web Services* – White Paper, www.develop.co.uk, 2002
- *UDDI Technical White Paper*, Septembrie 2000, http://www.uddi.org,