CERCETĂRI PRIVIND SECURITATEA AFACERILOR ELECTRONICE. STANDARDE ŞI PROTOCOALE PENTRU SECURITATEA AFACERILOR ELECTRONICE

Prof. univ. dr. Floarea Năstase, Prof. univ. dr. Pavel Năstase, Prof. univ. dr. Adrian Vasilescu, Conf. univ. dr. Răzvan Zota, Lect. univ. dr.Carmen Timofte, ing. Octavian Paiu,
Asist. univ. drd. Mădălina Mlak, Prep. univ. Radu Constantinescu,
Prep. univ. Iulian Ilie-Nemedi, ec. drd. Jack Timofte

1. Considerații privind securitatea informațională

Dezvoltarea tot mai accentuată a Internet-ului a determinat apariția unor noi modalități de a realiza afaceri. Astfel, companiile au simțit o oarecare presiune din partea pieței de a fi prezente pe Web, dar în acelaşi timp de a se asigura că această conexiune la rețeaua mondială nu presupune nici un risc de securitate pentru ele.

Măsurile de securitate informatică au ca scop reducerea riscurilor de utilizare a datelor unui sistem informatic de persoane/programe neautorizate. Introducerea mecanismelor de protecție nu garantează eliminarea completă a oricărui risc, dar poate să-l reducă la un nivel acceptabil. Riscurile pot fi externe (ascultarea purtătoarei de informație, falsificarea documentelor, virusarea softului) sau interne (accidente de manevrare, agresiuni cu intenție).

Securitatea unei sistem informatic poate fi amenințată prin acțiuni cu sau fără rea intenție. Astfel, calamitățile naturale, defectarea unor echipamente, erorile de operare sunt incluse în categoria acțiunilor fără o intenție distructivă.

În schimb, acțiuni de tipul: *spionarea rețelei* (*ascultarea canalului*) pentru a avea acces la datele în clar şi la parole; *falsa identitate* (*impostura*) pentru a avea acces neautorizat la date sau pentru lansarea de e-mail, comenzi neautorizate etc.; *refuzarea serviciului* resurse ale rețelei devin neoperaționale; *reluarea mesajelor* pentru a fi accesate şi a le schimba în tranzit; *depistarea parolelor* pentru accesarea de informații şi servicii care nu sunt permise; *depistarea cheilor* pentru accesarea datelor şi parolelor criptate; *lansarea de viruşi* pentru distrugerea datelor, intră în categoria acțiunilor rău intenționate.

In general, un mediu de securitate trebuie să respecte următoarele cerințe:

- **identificarea –** procedura prin care entitatea care doreşte să acceseze resursele unui sistem trebuie să se identifice;
- **autentificarea –** există procedură pentru verificarea identității entității care solicită acces la un sistem, procesul prin care sistemul validează informațiile de conectare oferite de entitatea utilizatoare;
- **autorizarea –** setul de tranzacții prin care entității autentificate i se permite să folosească resursele solicitate;
- **integritatea –** procedurile prin care informația nu poate fi modificată;
- **confidențialitatea –** protejează conținutul mesajului transmis în rețea împotriva citirii sau interceptării neautorizate;
- **auditarea** – procesul de înregistrare a tuturor tranzacțiilor astfel încât fiecare problemă poate fi analizată după ce a avut loc;
- **non-repudierea –** garantează originea şi integritatea tranzacției din punctul de vedere al expeditorului.

Modelul conceptual al unui sistem de securitate poate fi prezentat ca în figura 1.1, unde infrastructura pentru tehnologia informației dintr-o organizație se poate reprezenta ca o serie de niveluri interconectate.

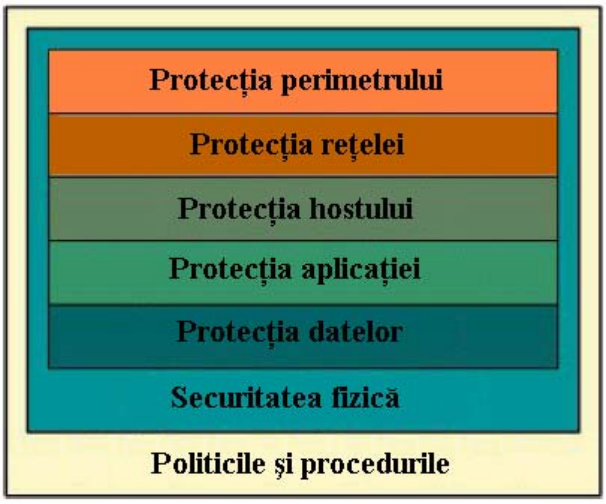

Figura 1.1 Modelul concepual pentru securitatea informațională

O viziune completă despre managementul securității informației este redată prin ISO-17799/BS-7799. În acest standard sunt tratate toate aspectele cu privire la riscurile necesare a fi măsurate şi controlate, pentru a se stabili un cadru adecvat managementului securității (figura 1.2).

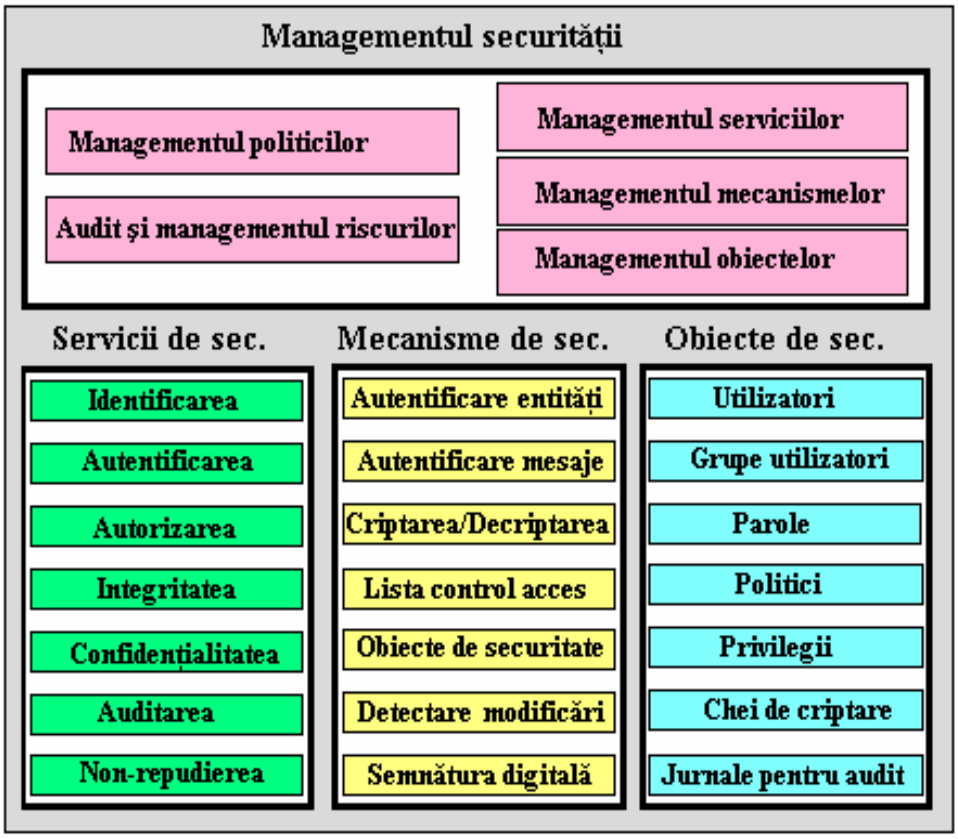

Figura 1.2 Arhitectura de securitate conform standardului ISO 7498-2

2. Evaluarea riscului în afaceri

Există tentația de a translata direct analiza amenințărilor într-o soluție tehnică. Dar în primul rând, trebuie studiate standardele prin prisma *politicii de securitate* a organizației. Politica de securitate la nivelul unei organizații joacă un rol esențial, fiind responsabilă chiar de managementul afacerii (vezi si figura 2.1).

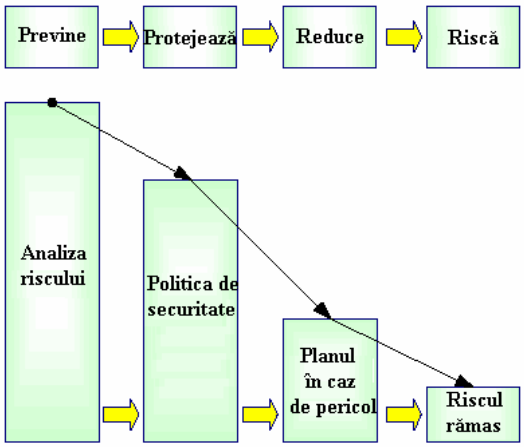

Figura 2.1 Reducerea riscurilor

Documentul "Orange Book" defineşte şapte clase de sisteme de securizare:

- **clasa "D" - *protecţie minimă*** - acele sisteme care au fost evaluate, dar au renunţat să introducă echipamente pentru un nivel de securitate mai înalt;
- **clasa "C1" - *protecţie discreţionară*** - acele sisteme care introduc control exact de cât au nevoie şi susţin separarea utilizatorilor de date;
- **clasa "C2" - *protecţia controlului accesului*** - sisteme ce au implementat pentru controlul accesului clasa C1, şi contabilizează acţiunile utilizatorilor prin proceduri de login;
- **clasa "B1" - *protecţie etichetată de securitate*** - sisteme care implementează un model de politică de securitate formal, şi facilitează etichetarea datelor şi prescrierea controlului accesului peste numirea subiectelor şi obiectelor;
- **clasa "B2" - *protecţie structurată*** - sisteme care includ toate caracteristicile găsite în B1 şi în care se aşteaptă ca toate subiectele şi obiectele să fie sisteme relative ADP;
- **clasa "B3" - *domenii de securitate*** - sisteme care satisfac cerinţele de monitorizare şi includ instrumente adminstrative de securitate, mecanisme, abilitatea de a semnala evenimente curente relevante;
- **clasa "A1" - *proiectarea verificării*** - sistem similar cu B3, dar cu trasături arhitecturale adiţioanale şi cerinţe asociate cu specificaţii de proiectare formale şi verificarea tehnicilor.

Principalele organizaţii internaţionale de standardizare a securităţii informaţiei sunt:

- **ISO – International Organization for Standardization,**
- **IEC – International Electrotechnical Commission,**
- **ITU** – International Telecommunications Union.

La nivel european cele trei organizaţii care corespund pentru ISO, IEC şi ITU-T sunt:

- **CEN – Comité Européen de Normalisation,**
- **CENELEC – Comité Européen de Normalisation Eléctrotechnique,**
- **ETSI –** European Telecommunications Standards Institute.

Standardul **Common Criteria** oferă o taxonomie pentru evaluarea funcţionării securităţii printr-un set de funcţii şi de cerinţe. Common Criteria include urmatoarele clase funcţionale de cerinţe:

Auditul securităţii; Comunicaţia; Suport pentru criptografie; Protecţia datelor utilizatorului; Identificarea şi autentificarea; Managementul funcţiilor de securitate; Confidenţialitatea; Protecţia funcţiilor de securitate; Utilizarea resurselor; Accesul la componente; Căi şi canale încredinţate.

3. Securitatea aplicaţiilor distribuite

Aplicaţia distribuită este definită ca o aplicaţie în care părţi ale ei sunt rulate pe entităţi de calcul distincte şi autonome conectate în reţea. Sistemul distribuit este o colecţie de entităţi de calcul (hardware şi software) autonome, dispersate din punct de vedere geografic, şi conectate prin medii de comunicaţie.

Aplicaţiile distribuite tipice sunt: 2-tier (folosesc arhitectura *client-server*), 3-tier (utilizează arhitectura *client-middleware-server*) şi n-tier (*client-multiple middleware-multiple servers*).

Există mai multe protocoale care asigură servicii de securitate, majoritatea similare în ceea ce priveşte serviciile oferite şi algoritmii criptografici folosiţi, ele diferind prin maniera de furnizare a serviciilor şi prin situarea lor în raport cu ierarhia de protocoale TCP/IP (figura 3.1).

La nivel de client securitatea este implementata, in mod uzual, de programele de tip "browser" (cum este, de exemplu, Internet Explorer).

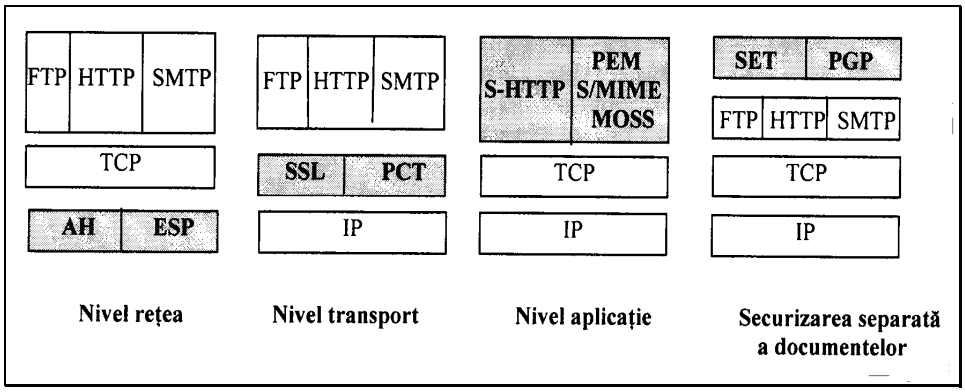

Figura 3.1 Soluții de integrare a serviciilor de securitate în ierarhia de protocoale

4. Infrastructura de chei publice (PKI)

Infrastructura de chei publice (PKI – Public Key Infrastructure) oferă un cadru tehnic (incluzând protocoale, servicii şi standarde) pentru a sprijini realizarea de aplicaţii care îndeplinesc cele cinci proprietăţi de securitate: autentificarea utilizatorilor, confidenţialitatea datelor, integritatea datelor, non-repudierea şi managementul cheilor.

O structură simplificată de afaceri care implementează PKI este reprezentată în figura 4.1.

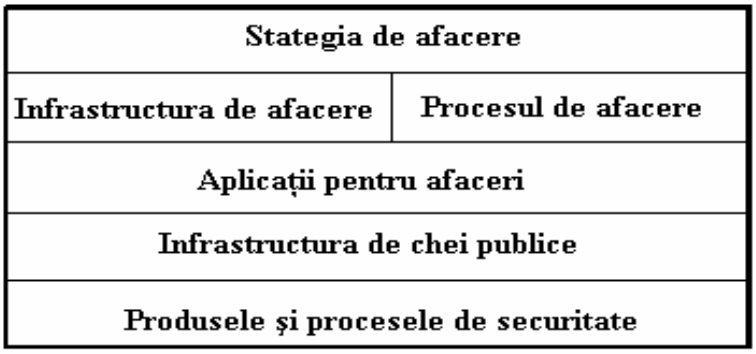

Figura 4.1 Infrastructura de chei publice în afaceri

Deşi PKI este relativ nou, el a fost dezvoltat şi implementat în multe din protocoalele de comunicaţie în reţea, prin includerea algoritmilor de criptare care folosesc cheile publice.

Bazat pe standarde deschise (open standard - open software - acces liber asupra surselor, conceptelor si algoritmilor conţinuţi), PKI ofera: Standardizarea aplicaţiilor de reţea. Aceasta oferă securitatea comunicaţiilor pe Internet pentru orice reţea a oricărei firme; Suport pentru comerţ electronic, de exemplu folosind protocolul de plaţi SET sau protocolul de securitate SSL; Un mediu sigur şi scalabil pentru aplicaţiile de securitate; Administrarea cheilor şi a certificatelor între mai multe aplicaţii; Infrastructura de securitate care are mari şanse să fie recunoscută şi acceptată ca standard de facto de către mediul de afaceri şi de către autoritaţile guvernamentale.

5. Protocolul de transfer securizat SET

Protocolul SET *(Secure Electronic Transaction)*, folosit pentru plati electronice, defineşte relaţiile intre părţi si modul lor de acţiune.

Relaţiile dintre entităţile care participa la tranzacţii se pot imparti in trei tipuri:

1. *Relaţii contractuale.* Acestea reprezintă contracte legale semnate intre diferite părţi pentru a oferi servicii si a-si asuma responsabilităţi. Nu au nimic de a face cu protocolul de plaţi SET doar ca SET pleacă de la premiza ca aceste contracte au fost stabilite anterior.

2. *Relații administrative.* Aceste relații trebuiesc stabilite inainte de începerea procesului de plați SET. De asemenea, aceste relații păstrează mediul de afaceri in siguranța. Anumite relații sunt conținute in protocolul de plăți SET.
3. *Relații de tip operațional.* Aceste relații sunt constituite pe termen scurt si au loc atunci când trebuiesc făcute plați. Toate acestea sunt definit in protocolul de plați SET.

SET a fost creat, in primul rand, pentru a permite comercianților plata pentru bunurile si serviciile vândute intr-un mod sigur, de incredere si consistent. Cerințele pentru realizarea unui mediu propice afacerilor sunt satisfăcute de SET prin folosirea criptarii si a altor tehnici.

6. SSL (Secure Sockets Layer)

Protocolul SSL a fost inițial dezvoltat de Netscape iar apoi a fost utilizat ca standard pentru autentificare si criptare pe Internet intre serverele Web si clienții reprezentați de browsere. Noul standard propus de Internet Engineering Task Force se numește *Transport Layer Security* (TLS) si are la baza protocolul SSL. Pe de alta parte, protocolul SSL a ajuns la versiunea 3 si reprezintă cea mai uzitata metoda la ora actuala de criptare/autentificare bazata pe infrastructura de chei public (PKI).

Protocolul SSL rulează peste TCP/IP si sub alte protocoale de nivel inalt cum ar fi HTTP sau IMAP si permite serverelor ce au suport pentru SSL sa se autentifice către clienții SSL, de asemenea clinetii sa se autentifice către servere si intre clienți si servere sa se stabilească o conexiune criptata (figura 6.1).

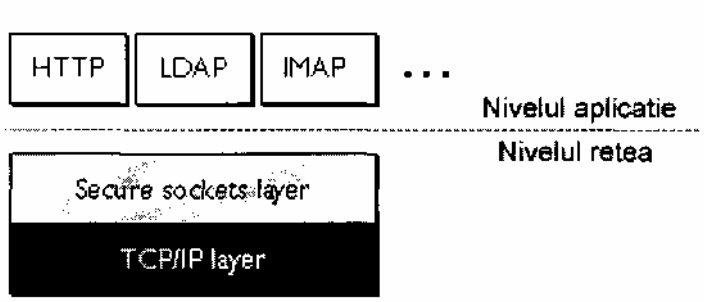

Figura 6.1 Protocolul SSL

Cei mai folosiți algoritmi de criptare de protocolul SSL sunt: *DES* - Data Encryption Standard 40/54 biți; *DSA* - Digital Signature Algoritm, parte a standardului de autentificare digitala folosit de Guvernul SUA; *KEA* - Key Exchange Algorithm; MD5 - Message Digest (functie hash) dezvoltat de Rivest pe 128 biți; RC2 si -RC4 - Rivest Encryption Ciphers dezvoltat de RSA Data Security - 40/128 biți; RSA - Un algoritm bazat pe chei publice folosit pentru criptare si autentificare, dezvoltat de Rivest, Shamir si Adleman; *RSA key exchange* - Un algoritm de schimb de chei bazat pe RSA dezvoltat pentru SSL; *SHA-1* - Secure Hash Algorithm - functie hash pe 160 biți; *SKIP JACK* - un algoritm secret bazat pe chei simetrice implementat in platformele hardware FORTEZZA; *Triple-DES* - Algoritm ce aplica de trei ori DES 168 biți.

Protocolul de inregistare SSL (figura 6.2) este folosit pentru transferul datelor aplicației si a celor de control intre client si server. In prima faza se fragmentează datele in unități mai mici sau se combina mai multe mesaje de nivel inalt intr-o singura unitate. Datele vor fi compresate, semnate digital si apoi criptate inainte de transmisia prin TCP.

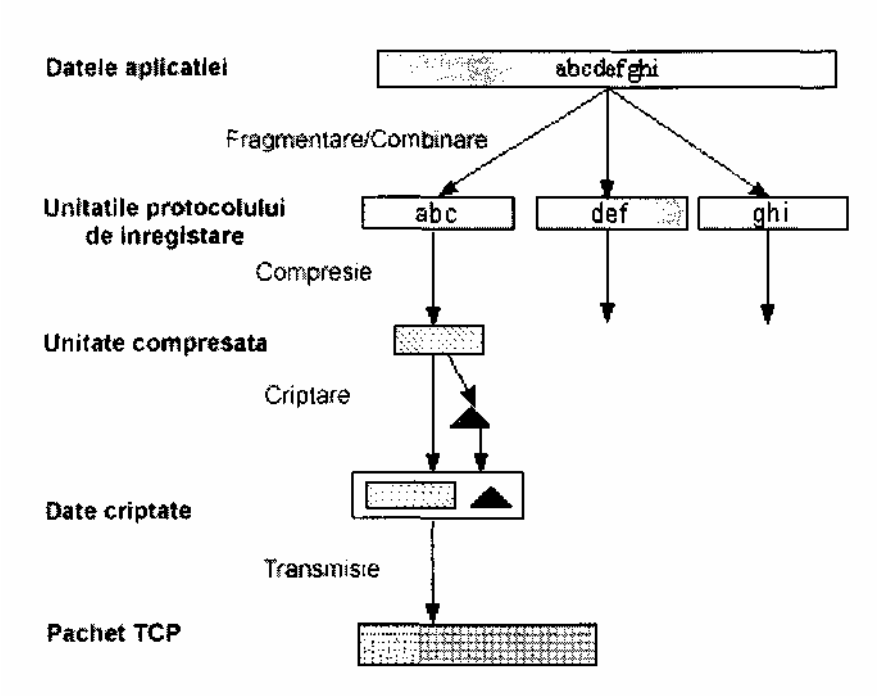

Figura 6.2 Protocolul de înregistrare SSL

7. Securitatea serviciilor Web

Serviciile Web (Web Services) descriu o modalitate de acces la date şi interacţiunea cu programe ce rulează pe diferite platforme de operare în cadrul reţelelor publice şi de întreprindere. Spre deosebire de reţelele extranet tipice, ce necesită interfeţe puternic integrate între membrii comunicării, scopul serviciilor Web este acela de a oferi o singură interfaţă comună care să permită calculatoarelor să ruleze programe, să partajeze date şi să acceseze servicii diverse. Bazate pe un limbaj comun – XML (eXtensible Markup Language) şi un protocol comun de transport – HTTP (HyperText Transfer Protocol), serviciile Web acţionează ca un intermediar între cele două entităţi ce doresc să comunice între ele.

Sunt bazate pe limbaje şi protocoale specifice (în afară de XML şi HTTP), printre care, cele mai cunoscute sunt: Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) şi Universal Discovery, Description and Integration (UDDI). SOAP este practic un mecanism de transport pentru mesajele XML. UDDI este un registru bazat pe XML ce permite furnizorilor să prezinte serviciile Web pe Internet. WSDL (care este bazat tot pe XML) reprezintă o modalitatea de descriere de conexiune a clienţilor (dintr-o perspectivă software) la furnizorii de servicii Web. Împreună cu XML şi HTTP, aceste protocoale reprezintă fundamentul pe care se sprijină serviciile Web, permiţând diverselor entităţi să caute şi să prezinte servicii, să apeleze proceduri, să ruleze programe şi să întoarcă rezultate.

Din punctul de vedere al securitatii, serviciile Web asigură autentificarea, autorizarea, confidenţialitatea şi integritatea datelor.

Serviciile Web folosesc o serie de noi specificaţii de securitate, printre care: XML Encryption, XML Signature, XML Key Management Specification (XKMS), Security Association Markup Language (SAML) şi Web Services Security (WS-Security). Aceste noi specificaţii se bazează pe mecanisme dezvoltate anterior (cum ar fi, de exemplu, PKI) pentru a asigura elementele de securitate pentru mesajele XML şi transportul SOAP (figura 7.1).

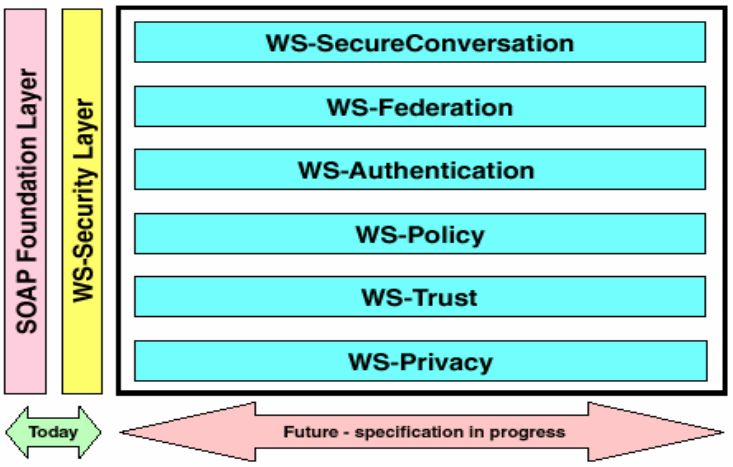

Figura 7.1 Modelul de securitate pentru Web Services

Procesele de afaceri sunt ultimele în care se defineşte necesarul pentru securitate. Procesul de securitate constituie deseori sursa unor discuţii tehnice de detalii. La baza cerinţelor de securitate pentru afaceri se regăsesc necesitatile de eliminare ale unui risc particular.

Procesul de afacere defineşte faza prin care se încearcă să se obţină caracteristicile de securitate prin colaborarea la cel mai înalt nivel. În fluxul ebXML curent, modelul informaţional este apoi translatat într-o reprezentare XML şi combinat cu alte informaţii ale mediului (figura 7.2).

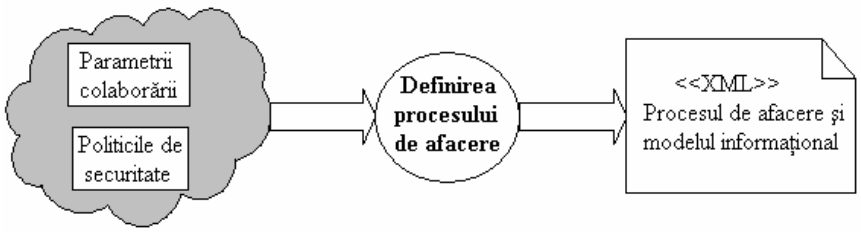

Figura 7.2 Procesul de afacere defineşte caracteristicile de securitate

Generarea profilului protocolului de colaborare este condusă prin modelul informaţional al procesului de afacere (şi conţine o referinţă la model prin structura sa) (figura 7.3).

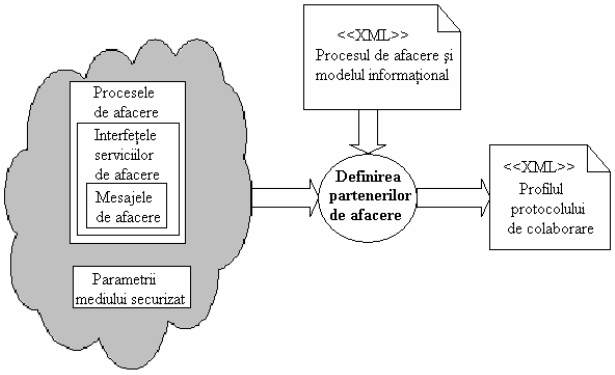

Figura 7.3 Generarea profilului protocolului de colaborare