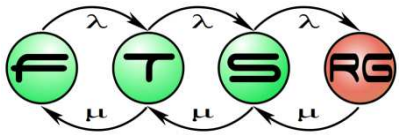
Szolgáltatás technológiák (WS, WS-*)



Elosztott rendszerek

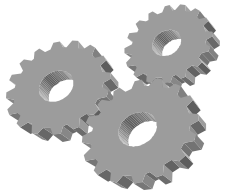
- Elosztott rendszerek
  - Egy *hálózat*on lévő számítógépek
    - Tipikus példa: Internet
  - Üzenet alapú kommunikáció
- Motiváció
  - Erőforrás megosztás
  - Skálázhatóság
  - Modularizáció
  - Együttműködés
- Követelmények
  - Kommunikációs réteg

XML webszolgáltatások

- Alkalmazások közötti adatcserére szolgáló protokollok és szabványok gyűjteménye
- Szabvány: XML alapúak
  - Strukturált szöveges állomány
  - Kötött formátum (séma)
- Nem csak nyílt Web-es környezetben
- Lazán csatolt alkalmazások
- Főbb fejlesztők
  - Apache, IBM, HP, SUN & Microsoft (.NET)
  - http://www.webservices.org/

Példák

E-mail küldés
Bemenet: levél adatai
Válasz: nyugta



Új alkalmazott felvétele
Bemenet: személyes adatok
Válasz: ID

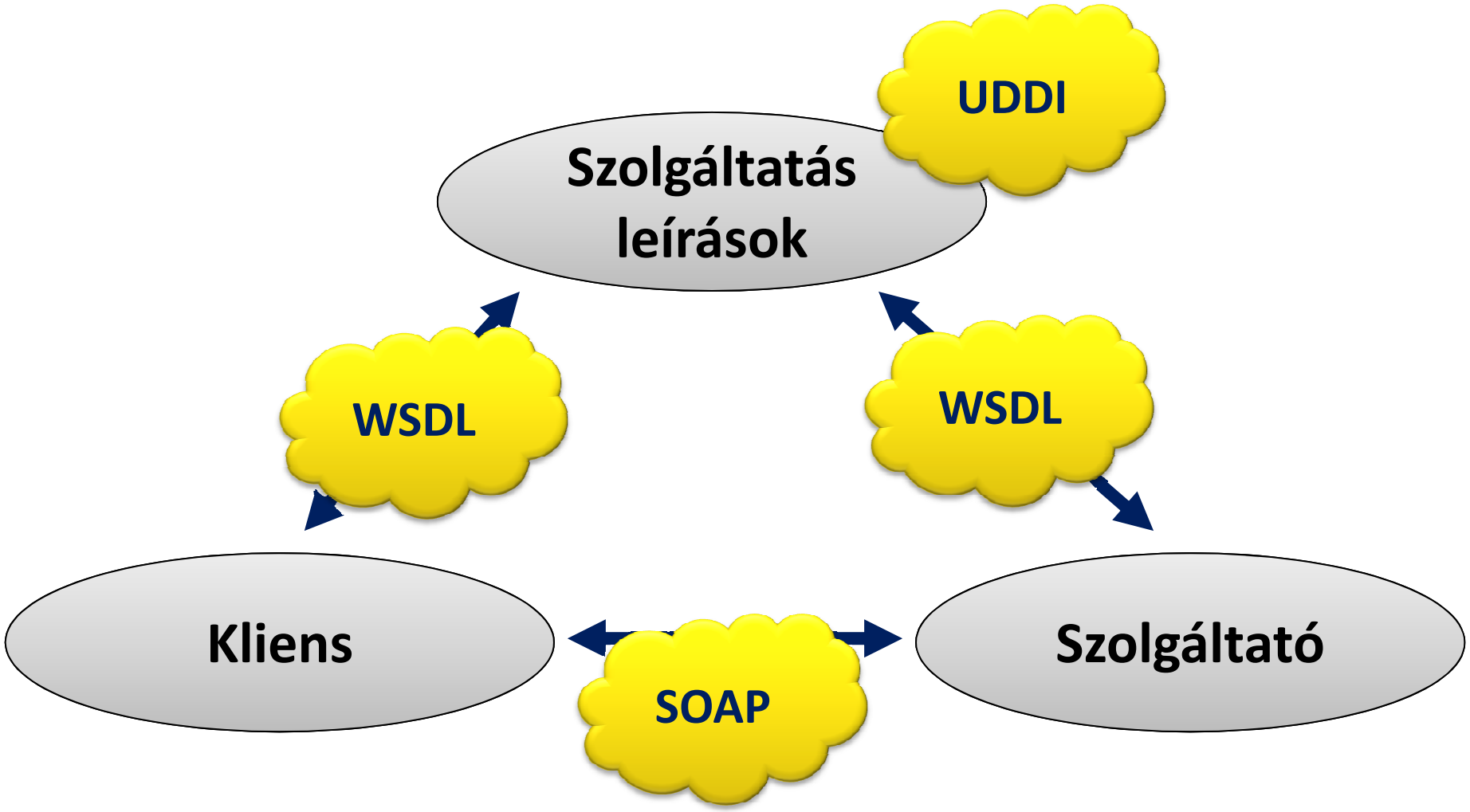
Vállalatirányítási rendszer elérése
Bemenet: beszállítók lekérdezése
Válasz: beszállítók listája, preferenciák

Infrastruktúra elérése
Bemenet: váratlan események lekérdezése
Válasz: riasztáslista

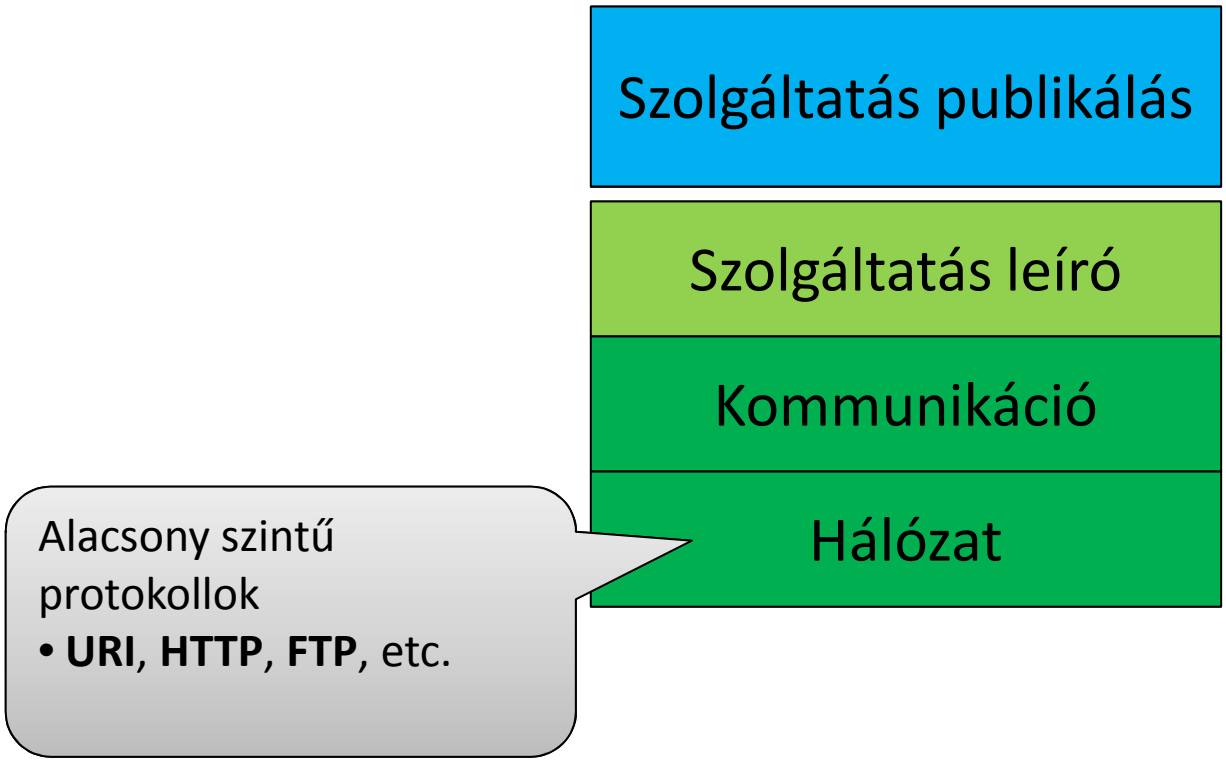
Lekérdező műveletek
Pl. időjárás előrejelzés, keresés,
repülőjegy árának lekérdezése, …
Bemenet: intervallum, hely
Válasz: csapadék, hőmérséklet, …

Szenzorok lekérdezése
Bemenet: épületrész állapota
Válasz: hőmérséklet, páratartalom,…

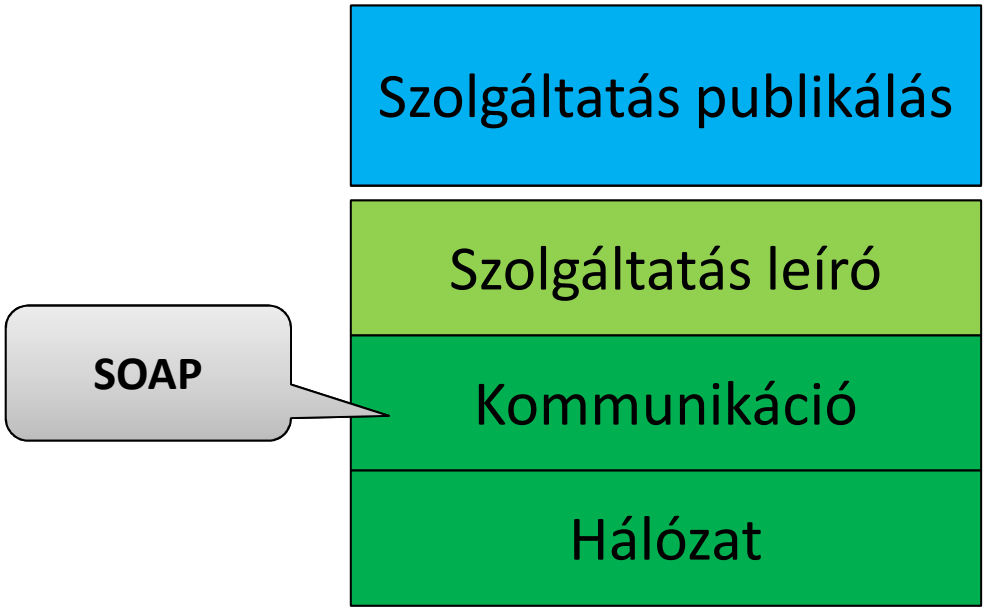
Megvalósítás



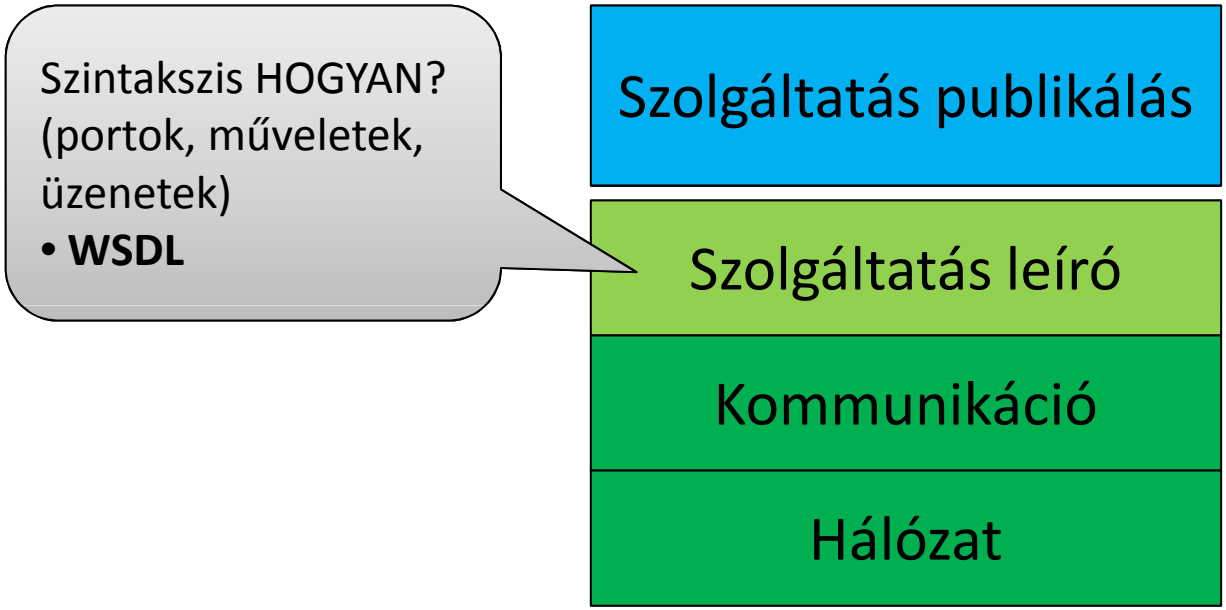
Web service stack



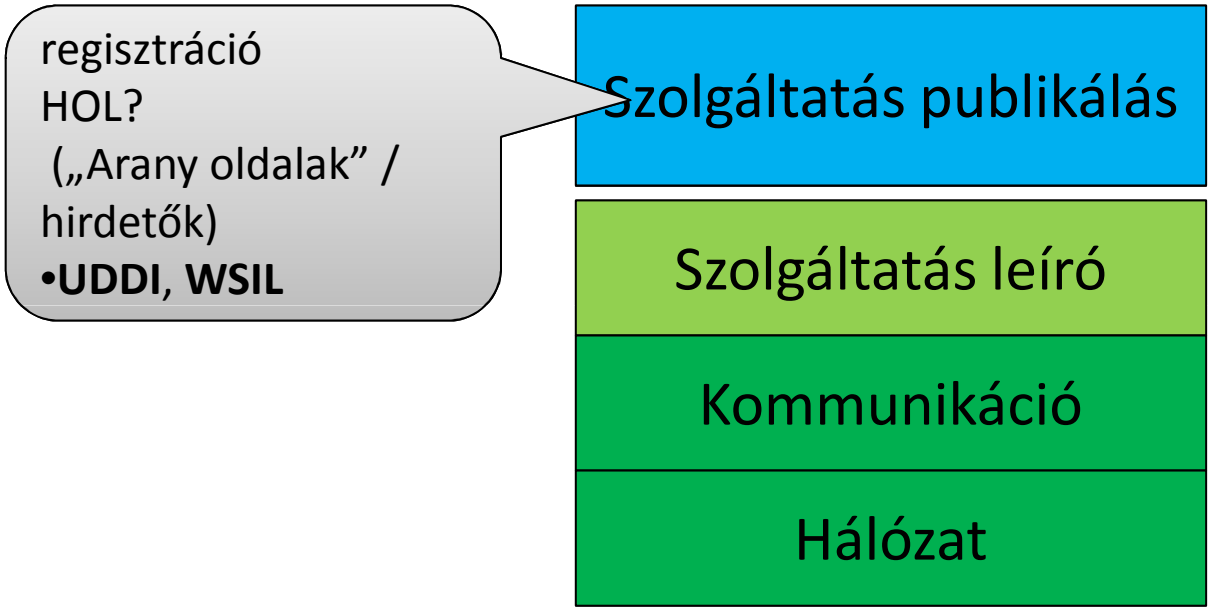
Web service stack



Web service stack



Web service stack



SOAP

- Simple Object Access Protocol
  - 1.1 verzió: 2000 óta
- Általános kommunikációs protokoll
- XML „Boríték”
- Fejléc
  - Címzett/feladó
  - Formátum
  - Kiegészítő információk
    - titkosítás, time-to-live, stb.
- Törzs

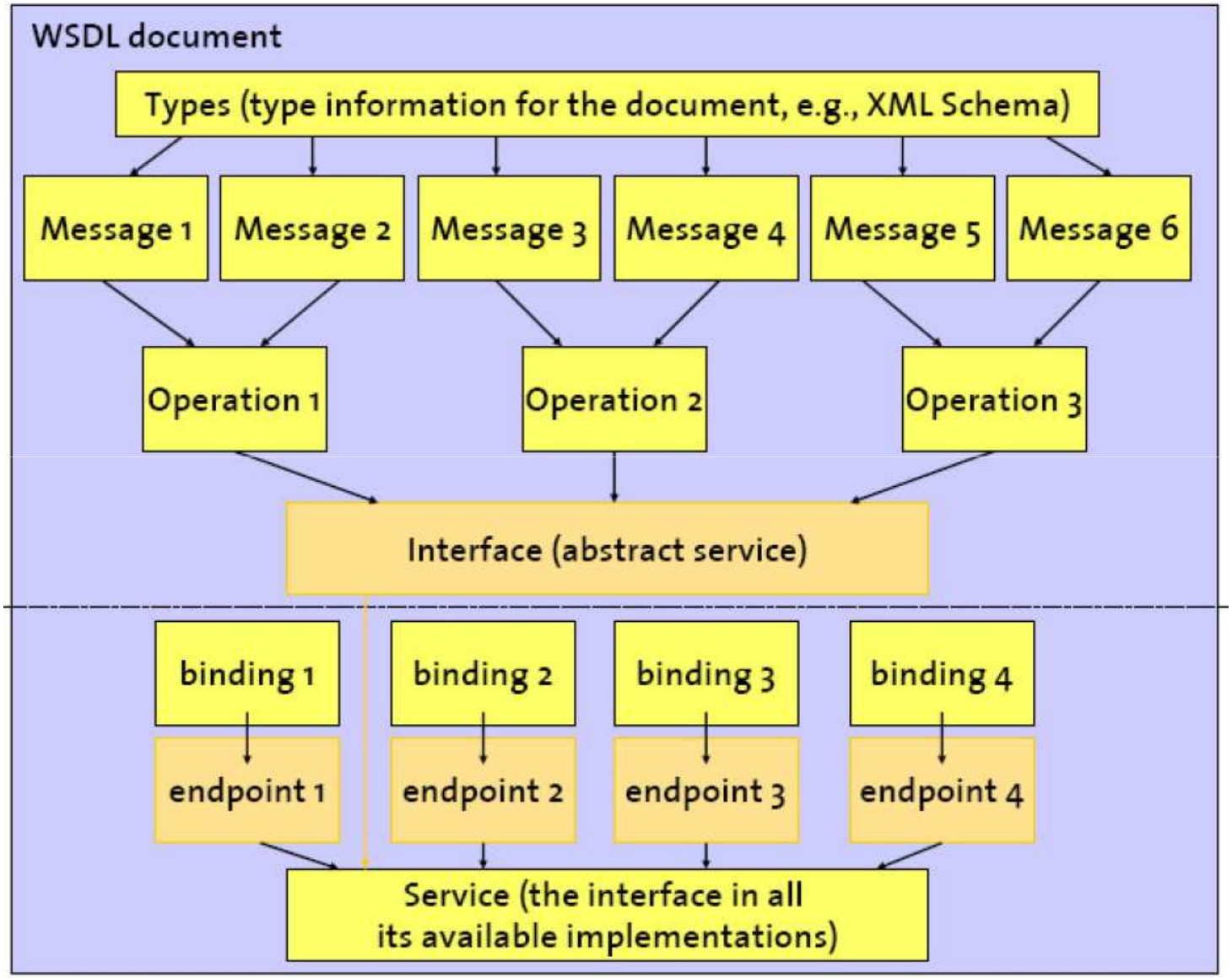
Web Services Description Language

- Interfészdefiníció
- Kérdés-válasz párok leírása
- „Port” típusok megadása
- Generálható az osztály publikus metódusai alapján
- Kliens (proxy) generálásához szükséges
- Lekérdezhető szolgáltatás tárakból

WSDL

- Adattípusok leírása
  - Séma (XSD) hivatkozás
- Portok leírása
  - Összetartozó műveletek halmaza
  - Pl. ÁrfolyamLekérdezőPort
- Műveletek (operations) leírása
  - Pl. UtolsóHónapÁtlagosÁrfolyama
- Üzenetek (típusának) deklarálása
  - Pl. ÁrfolyamKérdés
- Binding
  - Konkrét protokollhoz kötés, leggyakrabban SOAP

WSDL struktúra



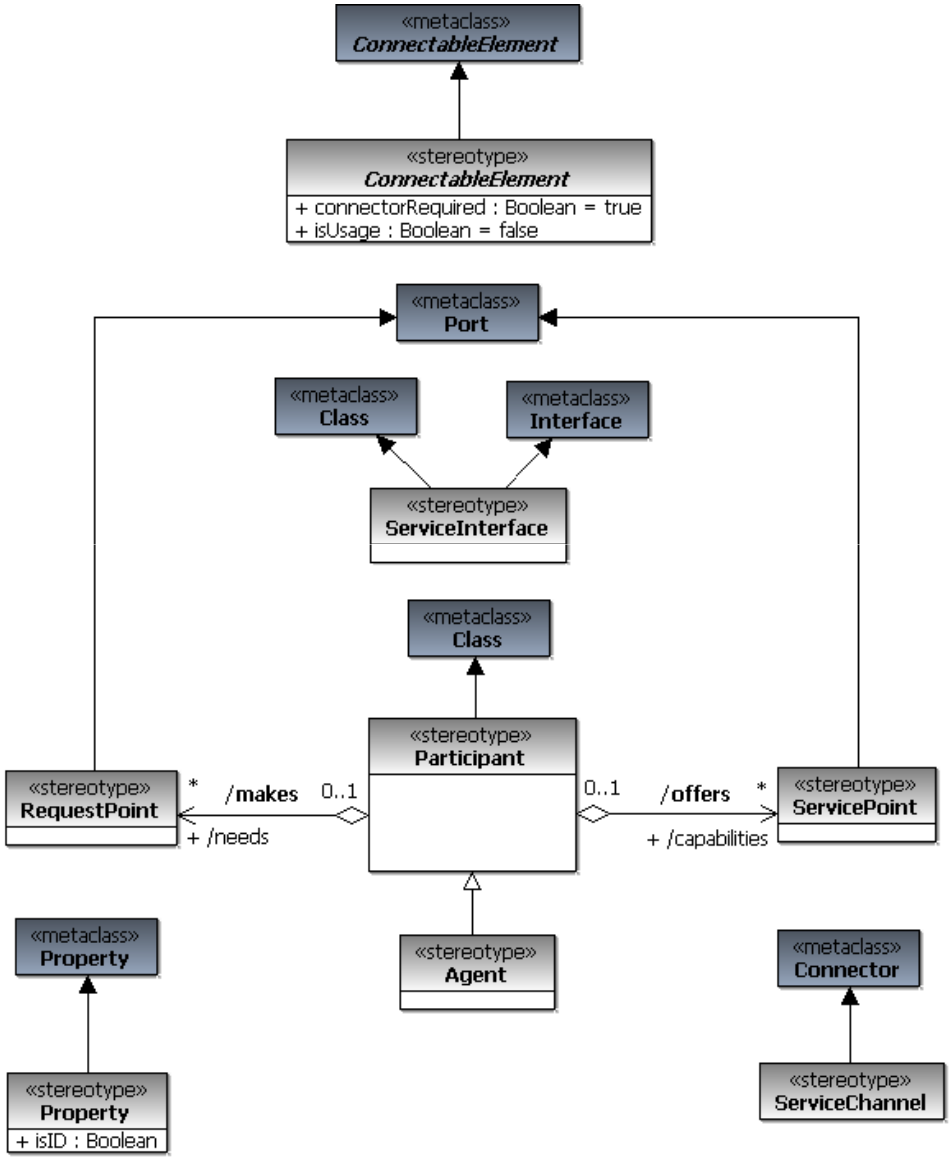
Webszolgáltatások felhasználása

- Példa
  - Google API
  - http://www.mnb.hu/arfolyamok.asmx?WSDL
- Pl. Amazon EC2 Cloud API
  - Maga a cloud management is webszolgáltatás alapon történik
  - http://ec2.amazonaws.com/doc/2009-03-01/AmazonEC2.wsdl
  - „Do NOT try to read or edit this file ”
- Publikus webszolgáltatások
  - http://www.webservicex.net/WS/wscatlist.aspx
  - http://www.service-repository.com/
  - http://www.xmethods.net/ve2/Directory.po
  - https://www.thedacs.com/databases/url/key/5440/5443/5537

WS fejlesztés tipikus lépései

- Szolgáltatás interfészek, adatstruktúrák tervezése
  - WSDL, XSD
- Implementáció/integráció
  - Ezek alapján generálható a WSDL
- Kliens/szerver oldali csonkok elállítása
  - API hívással
  - XML konfiguráció alapján
- Futási idben (middleware)
  - SOAP üzenetek elállítása
  - SOAP boríték elküldése
  - SOAP üzenet transzformálása a szolgáltatás bemeneti formátumára

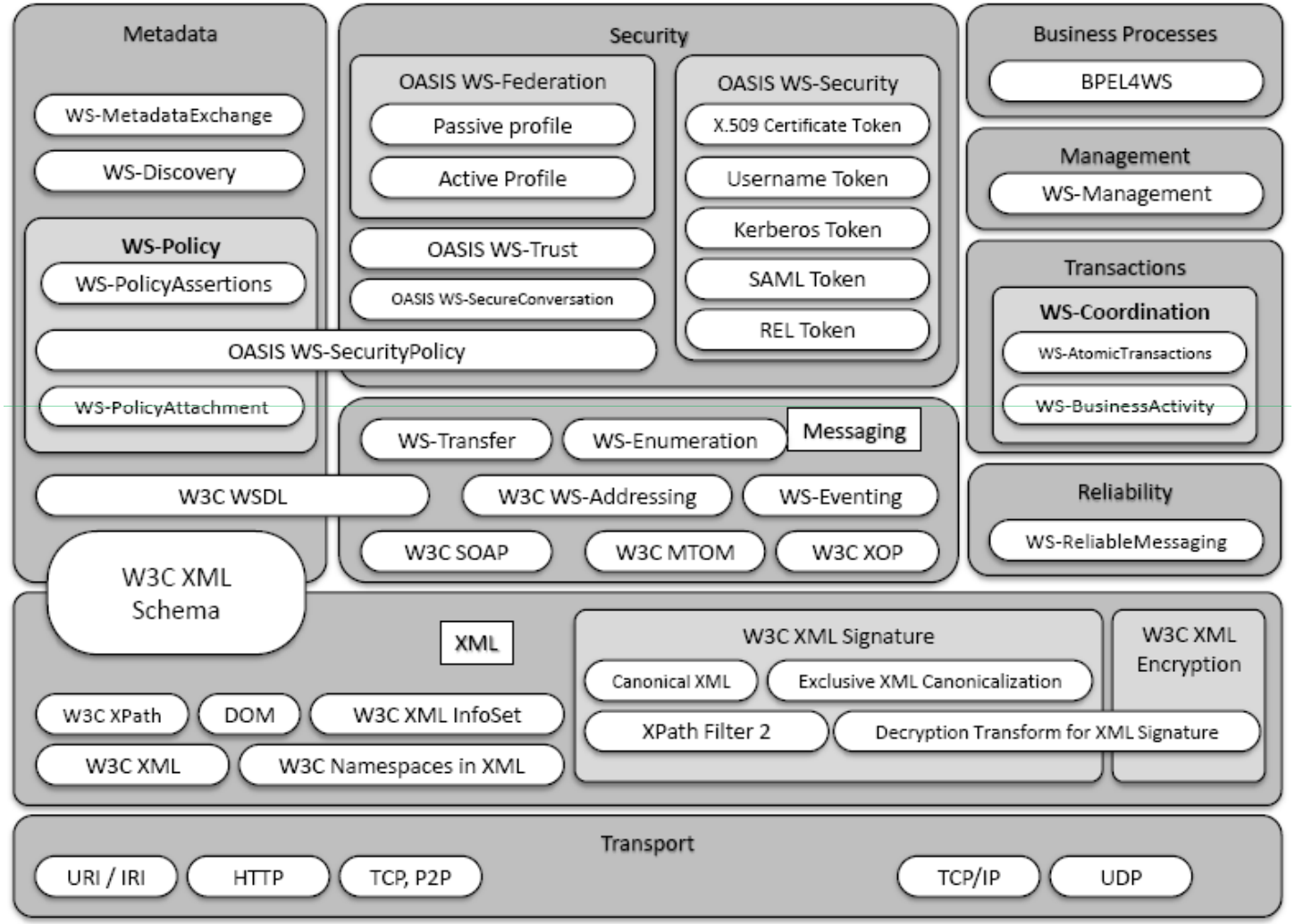
Modellezés: OMG: SoaML



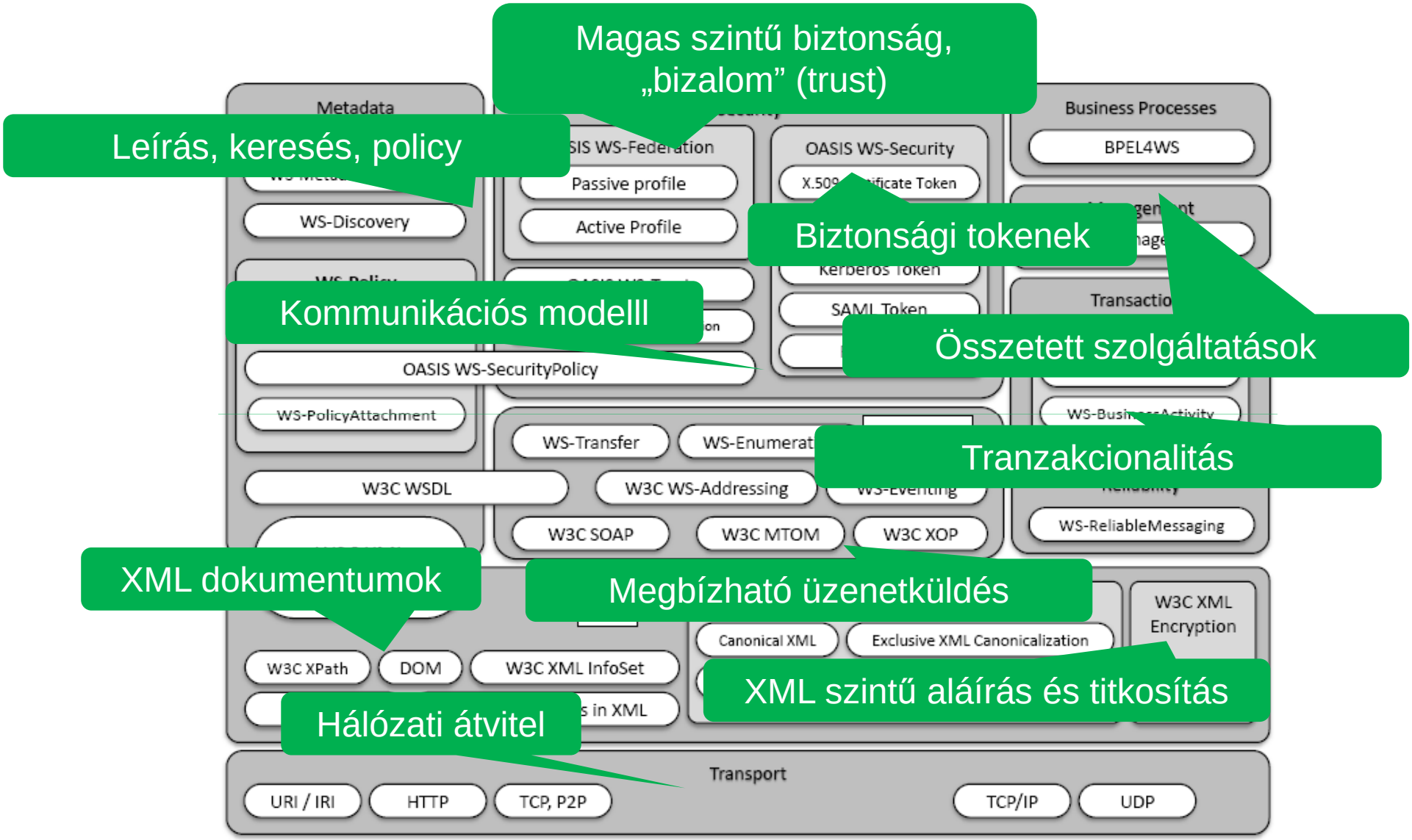
WS-*

- Hogyan adjunk alkalmazás szint garanciákat az integrációra?
  - Ne függjön a hálózattól
  - Ne függjön az implementációtól
  - Az alkalmazás logika határozza meg
- Feladatok
  - Tranzakciókezelés
  - Session kezelés
  - Biztonság
  - Titkosítás
  - Szolgáltatások kombinálása
  - Szolgáltatások szemantikája
  - Loggolás

Szabványok


Metadata
WS-MetadataExchange
WS-Discovery
WS-Policy
WS-PolicyAssertions
WS-PolicyAttachment
W3C WSDL
W3C XML Schema
Security
OASIS WS-Federation
Passive profile
Active Profile
OASIS WS-Trust
OASIS WS-SecureConversation
OASIS WS-SecurityPolicy
OASIS WS-Security
X.509 Certificate Token
Username Token
Kerberos Token
SAML Token
REL Token
Business Processes
BPEL4WS
Management
WS-Management
Transactions
WS-Coordination
WS-AtomicTransactions
WS-BusinessActivity
WS-Transfer
WS-Enumeration
Messaging
W3C WS-Addressing
WS-Eventing
W3C SOAP
W3C MTOM
W3C XOP
Reliability
WS-ReliableMessaging
XML
W3C XPath
DOM
W3C XML InfoSet
W3C XML
W3C Namespaces in XML
W3C XML Signature
Canonical XML
Exclusive XML Canonicalization
XPath Filter 2
Decryption Transform for XML Signature
W3C XML Encryption
Transport
URI / IRI
HTTP
TCP, P2P
TCP/IP
UDP

Szabványok


Magas szintű biztonság, „bizalom” (trust)
Leírás, keresés, policy
Biztonsági tokenek
Kommunikációs modelll
Összetett szolgáltatások
Tranzakcionalitás
XML dokumentumok
Megbízható üzenetkültés
XML szintű aláírás és titkosítás
Hálózati átvitel
Metadata
WS-Discovery
OASIS WS-Federation
Passive profile
Active Profile
OASIS WS-Security
Kerberos Token
SAML Token
OASIS WS-SecurityPolicy
WS-PolicyAttachment
Business Processes
BPEL4WS
Transactio
WS-ReliableMessaging
WS-Transfer
W3C WSDL
W3C WS-Addressing
W3C SOAP
W3C MTOM
W3C XOP
W3C XML Encryption
Canonical XML
Exclusive XML Canonicalization
W3C XPath
DOM
W3C XML InfoSet
Transport
URI / IRI
HTTP
TCP, P2P
TCP/IP
UDP

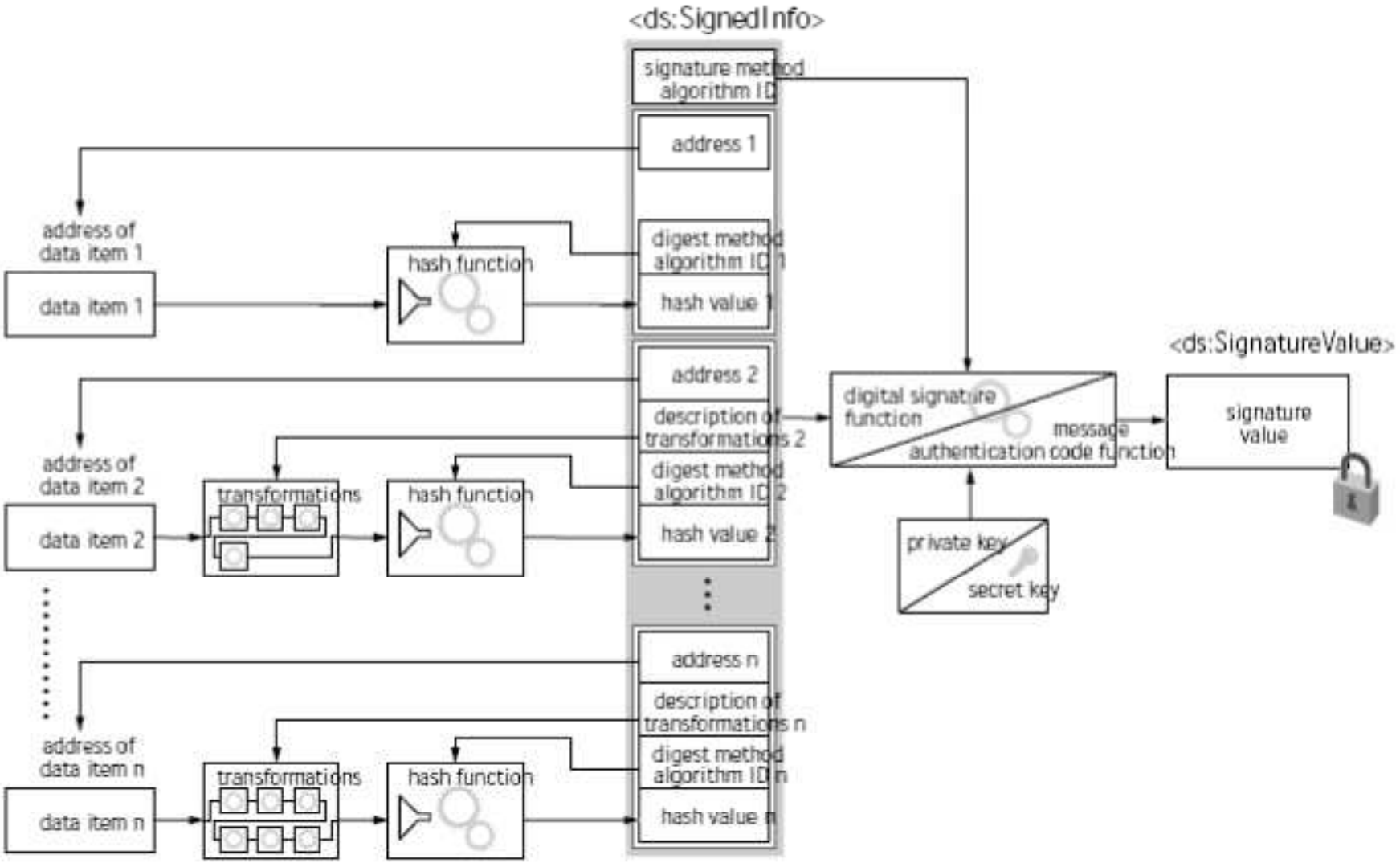
XML encryption

- W3C szabvány
- Szimetrikus kulcsú (pl. 3DES)
- Aszimetrikus kulcs (RSA)
- Fő elemek
  - SignedInfo
  - EncryptedData
  - EncryptedKey
- Tipikusan XML signature-el együtt használják

XML Signature szerkezete

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
    (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
   </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
  </Signature>
```

XML Signature



WS-Security

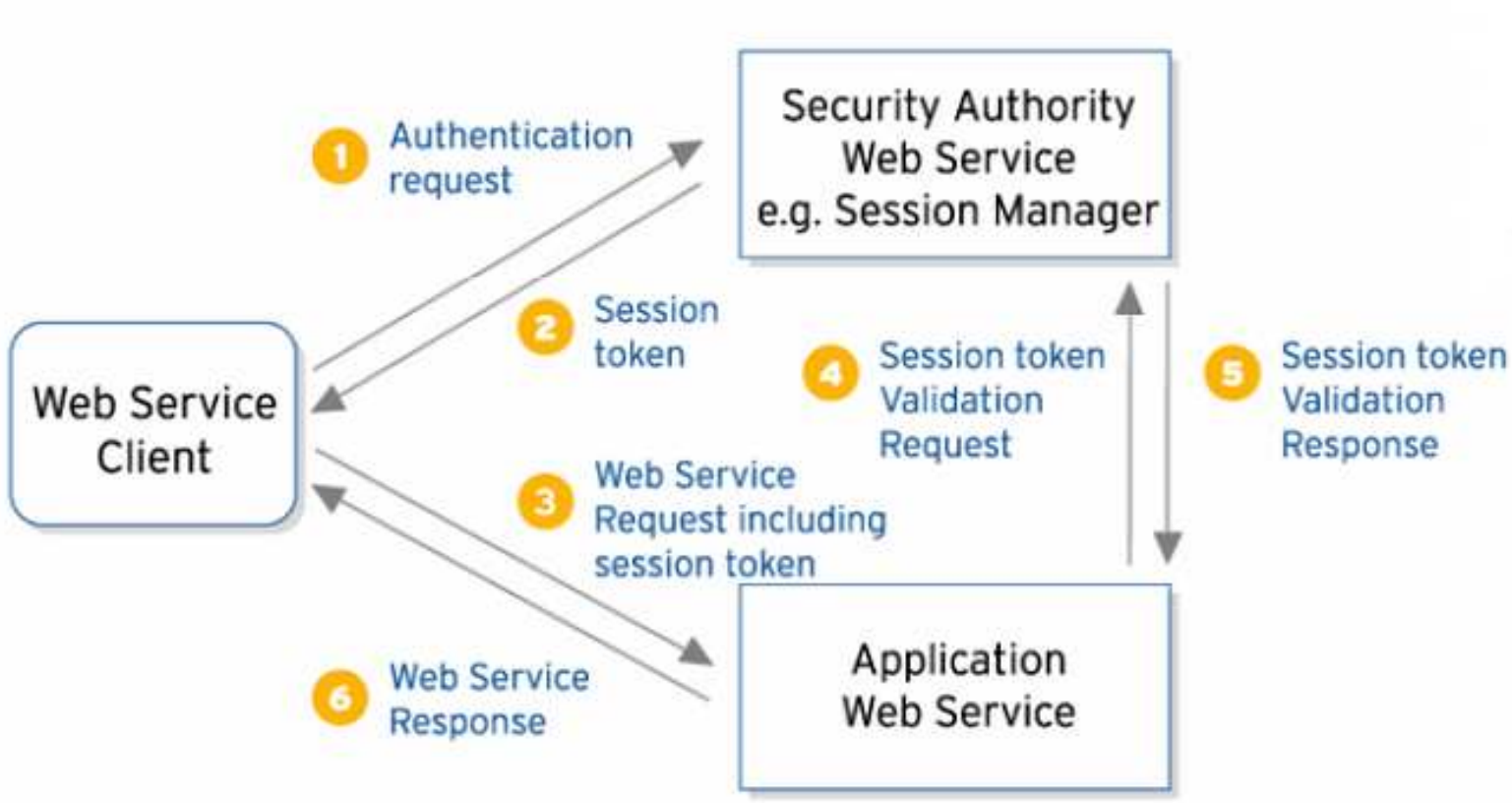
- Önmagában nem az üzenetet védi
  - „Hogyan igazoljuk, hogy védett az üzenet”
  - Használ más szabványokat
- Azonosítás és autentikáció
  - Milyen tokeneket használunk az üzenetben
- Integritás
  - XML signature
  - Időzítési védelem az újrajátszás ellen
- Titkosítás
  - WS-Encrpytion

Biztonsági tokenek

- Alkalmazás-specifikus
  - Usernév-jelszó
  - „unsigned”
- Aláírt biztonsági tokenek (bináris)
  - X.509 certificate
  - Kerberos
- XML tokenek
  - Pl. SAML
  - Általában „self-signed”

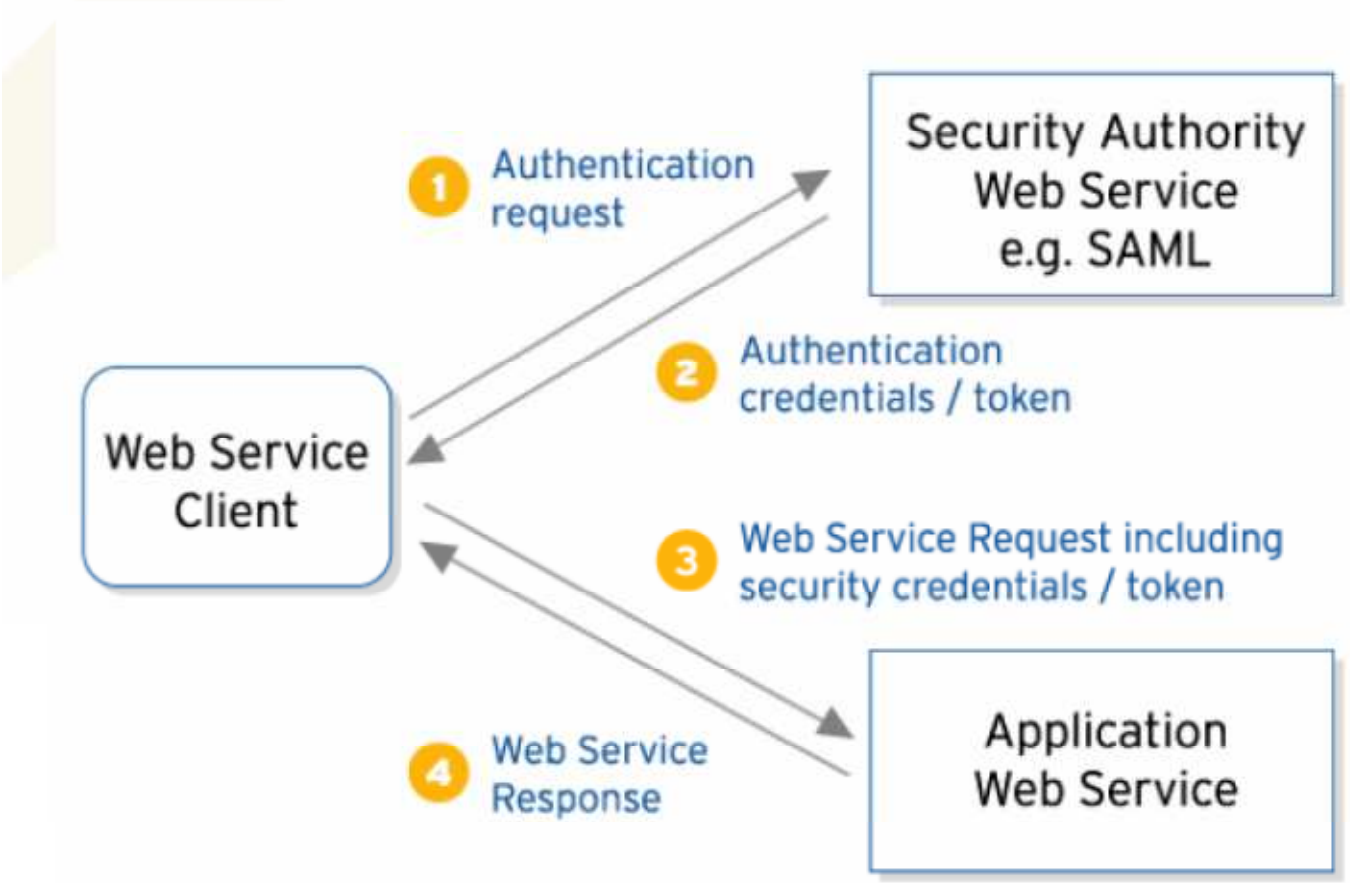
XML security párbeszéd

- Nem önhitelesítő tanúsítványok esetén (non self-validating credentials)



Szcenárió 2 – „self-validating credentials”

- Önhitelesítő tanúsítványok esetén (self-validating credentials)



WS-Security fejléc (SOAP)

```
<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv=
"http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
<soapenv:Header>
        <wsse:Security xmlns:wsse="..." soapenv:mustUnderstand="1">
        <xenc:EncryptedKey Id="EncKeyId-229902">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
                <ds:KeyInfo xmlns:ds="...">
                                <wsse:SecurityTokenReference>…</wsse:SecurityTokenReference>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                <xenc:CipherValue>PpAOXj5P0W8ukm...</xenc:CipherValue>
                                </xenc:CipherData>
                <xenc:ReferenceList>
                <xenc:DataReference URI="#EncDataId-30957433" />
        </xenc:ReferenceList>
        </xenc:EncryptedKey>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"Id="Signature-17764792">
        <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm=…/>
                <ds:SignatureMethod Algorithm=… />
                <ds:Transforms>…/ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>+ECkM6R4GQ7AQ=...</ds:DigestValue>
        /ds:SignedInfo>
</ds:Signature>
<wsu:Timestamp../>
<soapenv:Body xmlns:wsu="..." wsu:Id="id-30957433">
        <xenc:EncryptedData Id="EncDataId-30957433”….>
</sopaenv:Body>
```

Titkosítatlan válasz

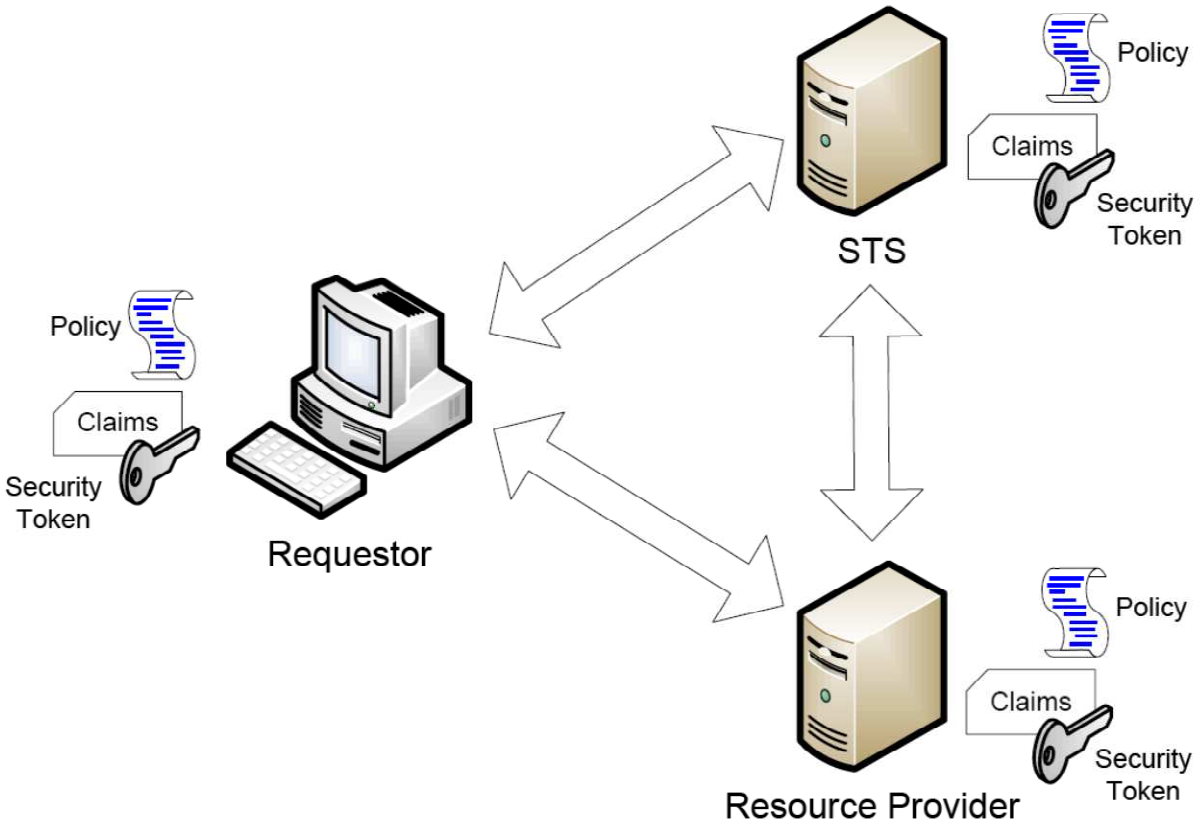
```
<?xml version='1.0' encoding='UTF-8'?>
   <soapenv:Envelope xmlns:soapenv=
   "http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
   <resp:numberOfArcticles xmlns:resp=
   "http://daily-moon.com/cms/" xmlns:tns=
   "http://ws.apache.org/axis2">
   42</resp:numberOfArcticles>
</soapenv:Body>
</soapenv:Envelope>
```

További specifikációk

- WS-SecurityPolicy
  - WS-policy alapon
  - Leírja a követelményeket
  - Milyen elemeket kell használni a többi nyelvből
- WS-SecureConversation
  - Hogyan történik a kulcsok igénylése, generálása, stb.
- WS-Interoperability
  - Különböző megvalósítások egymással kommunikálni tudjanak
  - Oracle és MS kölcsönösen tesztelik egymás platformját

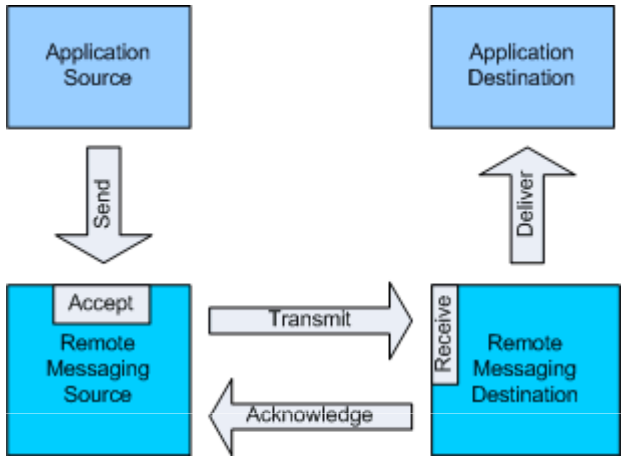
WS-Trust

- Szolgáltatók közti „bizalmasság”
- Biztonsági tokenek
  - Kibocsátása
  - Megújítása
  - Ellenőrzése
- Secure Token Service (STS)



Letagadathatatlanság: WS-RM

- „TCP réteg” webszolgáltatásoknak
- Megbízható üzenetküldés
  - Nyugtázás
  - Üzenetsorrendezés
  - Duplikátumok szűrése
  - Garantált kézbesítés



- Több szabvány egyesítése (MS, IBM)
- Implementációk
  - RAMP (IBM WebSphere Application Server 6-hoz)
  - Apache Sandesha (Axis2)
  - Microsoft Windows Communication Foundation
  - Bea WebLogic (→Oracle)

Biztonsági analízis

- Szisztematikus támadás WSDL alapján
  - Publikus információ felhasználása
- „Brute force” támadás (XML parsing)
  - Túlterhelés: a parse-olás a szűk keresztmetszet
- „XML injection”
  - Magának a feldolgozási folyamatnak a megváltoztatása
    - Pl. XPath, XSTL, XQuery használatával
- Külső referencia támadás
  - Dokumentum linkelése
- SOAP protokol szintű támadás
- Szállító réteg támadása

Milyen plusz feladatokat jelent

- Pl. Apache Axis2 konfiguráció esetén
- Szerver oldalon
  - Rampart, Sandesha modulok engedélyezése
  - services.xml konfiguráció beállítása
  - WSDL újragenerálása
  - Apache WSS4J
- Kliens oldalon
  - Apache WSS4J
- Mögöttes infrastruktúra
  - Pl. Keystore, üzenetsorok

WS Eszköztámogatás (példák)

- Apache: Apache Web Services Project
- IBM: WebSphere Application Server
- Microsoft: Windows Communication Foundation
- Oracle: METRO stack
- Eclipse: SOA Tools Platform
- Gyártók saját környezetei
  - Speciális célú, pl. adatbázis elérés
    - DB2
    - Oracle
    - MSSQL, stb.

Források

- http://ws.apache.org/axis2/modules/rampart/1_0/security-module.html
- http://ws.apache.org/sandesha/
- Sopera.de
- Security in a Web Services World: A Proposed Architecture and Roadmap (IBM & Microsoft whitepaper)
- Web Services Security Tutorial, Jorgen Thelin, CapeClear Software
- Standards and Practices in Operational Security, Yuri Demchenko, AIRG
- Understanding Web services Specifications –Part IV: security, Nicholas Chase (IBM whitepaper)