

Köztesréteg adatbiztonsági protokollok megvalósítására

Genge Béla és Haller Piroska
“Petru Maior” egyetem,
Marosvásárhely, ROMÁNIA

{bgenge, phaller}@upm.ro

Adatbiztonsági protokollok?

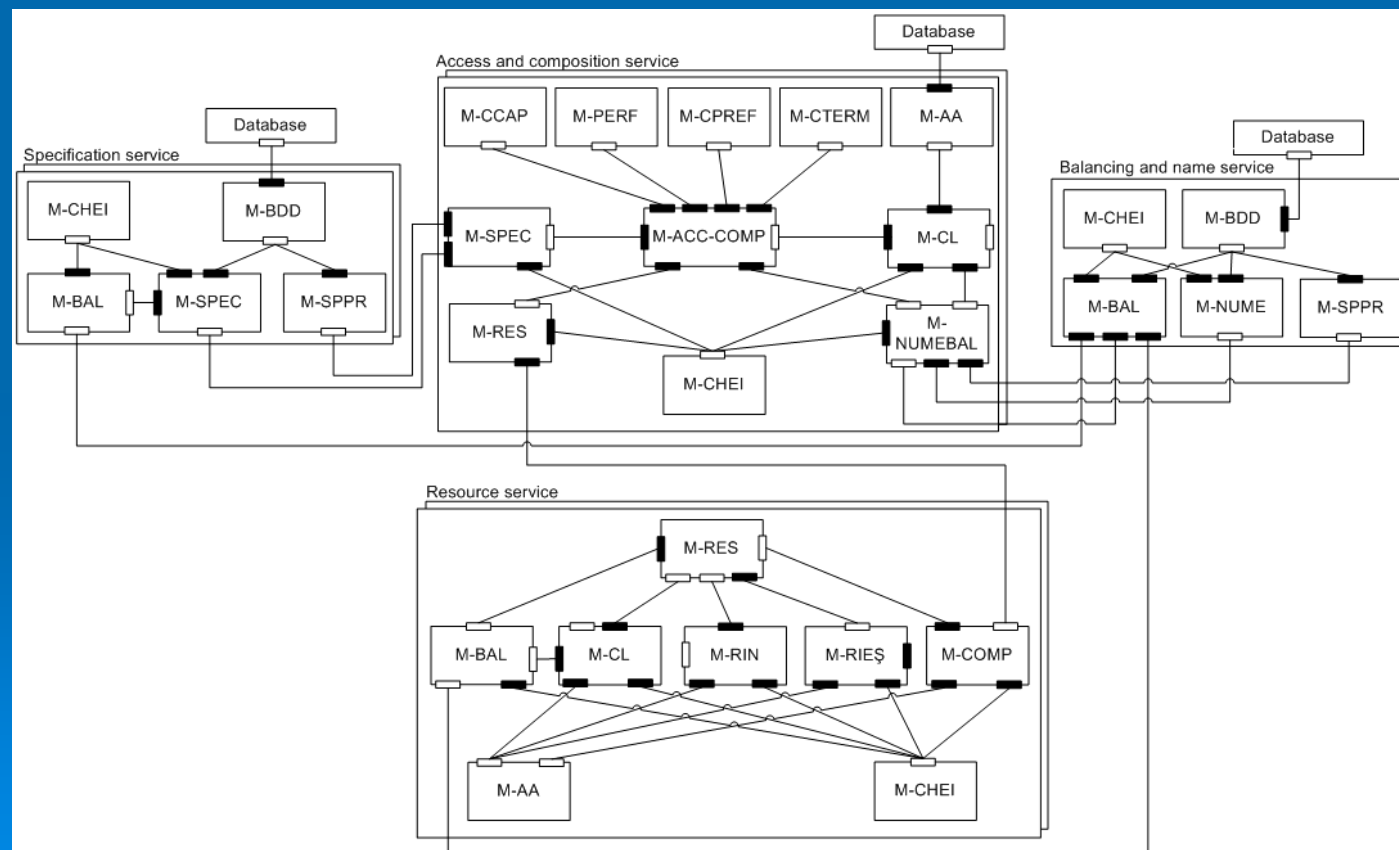
- Kommunikáció protokoll + kódolás
- Legismertebb protokoll típusok:
 - Kulcs-csere
 - Autentifikálás
 - Titkosítás
 - Integritás
- Protokollok megvalósítása általában “off-line” történik:
 - Változások vagy új protokollok esetében szükséges a rendszer komponenseit módosítani

Szolgáltatás-orientált köztesréteg

- Javasolt megoldás: köztesréteg
- Köztesréteg biztosítja a leírások biztonságos:
 - Lekérdezését
 - Értelmezését
 - Automatikus kezelését
- A köztesréteg komponensei: Web-szolgáltatások, melyek biztosítják a protokollok:
 - Meghírdetését
 - Megtalálását
 - Létrehozását
 - Komponálását
 - Végrehajtását

Köztesréteg architektúrája

➤ Szolgáltatás-orientált architektúra



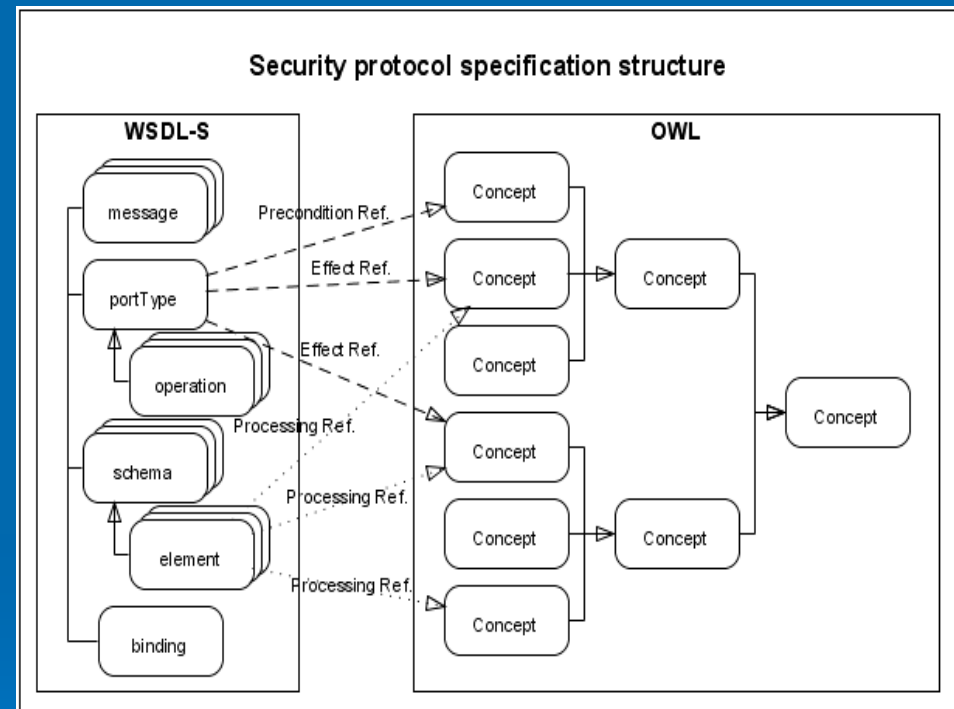
A leírások strukturális felépítése (1/2)

➤ Követelményeknek:

- Tartalmazza az üzenet minden komponensének a típusát
- Megnevezi a protokoll résztvevőit
- Leírja a használt kriptográfiai algoritmusokat
- Leírja az üzenet felépítését
- Megadja a résztvevők elérhetőségét és a használt adatátviteli protokollt
- Tartalmazza az előfeltételeket és a végrehajtás hatását

A leírások strukturális felépítése (2/2)

- Javasolt leírás két részből áll:
 - Szekvenciális rész (WSDL-S)
 - Szemantikus rész (OWL)
- Egy leírásnak a felépítése az informális specifikációból indul ki



„BAN” adatbiztonsági protokoll leírásának a felépítése (1/3)

- Kiindulunk az informális leírásból
- A szekvenciális leírás tartalmazza:
 - Üzenet szekvenciákat
 - Elő- és utó-feltételeket
- A szemantikus leírás tartalmazza:
 - Üzenetek felépítési módszereit
 - Üzenetek értelmezését

$$\begin{aligned} A \rightarrow B: A, N_a \\ B \rightarrow A: \{N_a, K, B\}_{K_{AB}} \\ A \rightarrow B: \{N_a\}_K \\ B \rightarrow A: N_b \end{aligned}$$

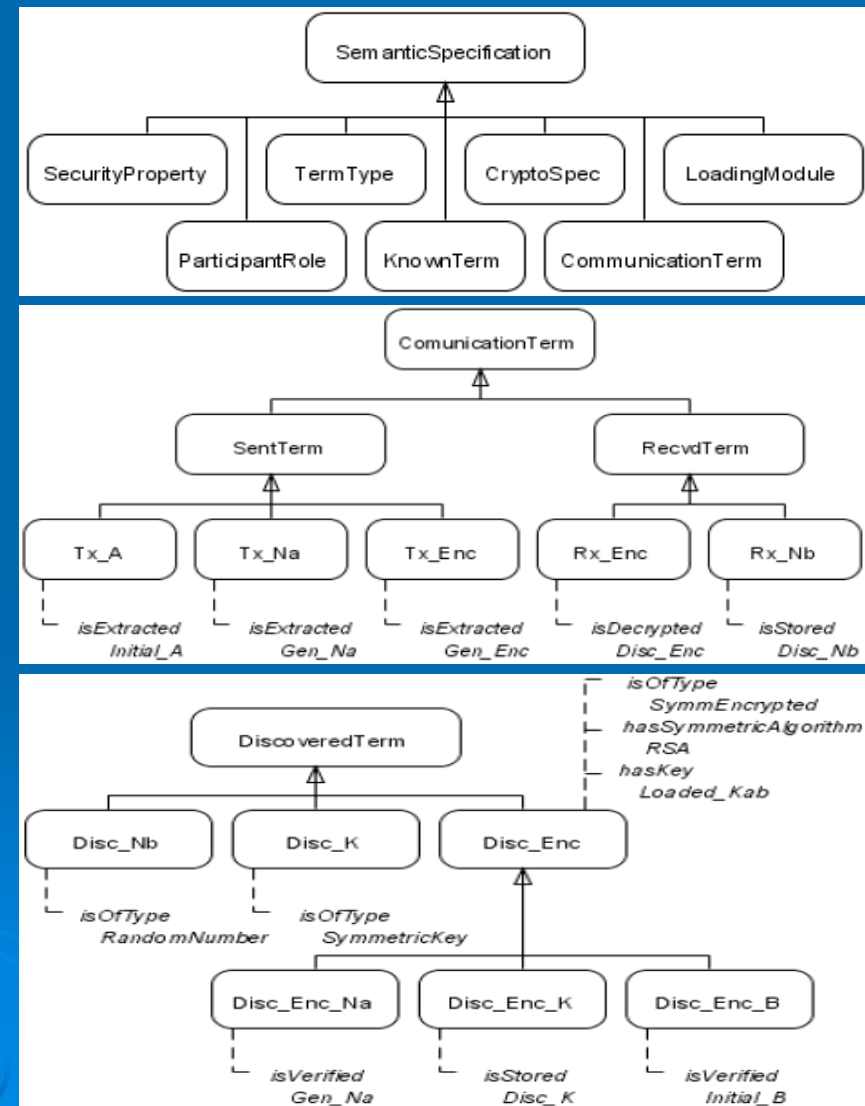
„BAN” adatbiztonsági protokoll leírásának a felépítése (2/3)

- Szekvenciális leírás WSDL-S formában
- Feltüntetett előfeltétel a kezdeményező szerepe: *Initiator_role*
- A protokoll végrehajtásának a hatása egy kulcscsere a protokoll résztvevői között
- A szekvenciális leírás minden eleméhez (előfeltétel, küldött vagy fogadott tag, hatás...) tartozik egy ontológia fogalma

```
...
<complexType name="Msg1Request">
  <sequence>
    <element name="Participant A" type="xsd:string"
      wssem:modelReference=".../SecProt.owl#Sent_A"/>
    <element name="Random" type="xsd:base64Binary"
      wssem:modelReference=".../SecProt.owl#Sent_Na"/>
  </sequence>
</complexType>
...
<wsdl:portType name="Encrypted communication">
  <wsdl:operation name="Msg1">
    <wsdl:output message="tns:Msg1Request"/>
  </wsdl:operation>
  ...
  <wssem:precondition name="Initiator"
    wssem:modelReference=".../SecProt.owl#
      Initiator_role"/>
  <wssem:effect name="SessionKeyExchange"
    wssem:modelReference=".../SecProt.owl#
      Session_key_exchange"/>
</wsdl:portType>
```

„BAN” adatbiztonsági protokoll leírásának a felépítése (3/3)

- Szemantikus leírás OWL formában
- Kiindul egy általános ontológiából
- Tartalmazza az üzenetekhez rendelt fogalmakat, felépítési módszereket és tulajdonságokat



Következtetések

- A köztesréteg tesztelésére 13 adatbiztonsági protokollt írtunk le
- A leírásokhoz erőforrás szolgáltatásokat rendeltünk
- A kliens minden esetben több erőforráshoz akart csatlakozni
- A kompozíció szolgáltatás letöltötte a megfelelő leírásokat, felépítette az összetett protokollt
- A tesztek bizonyították hogy a leírások elég információt tartalmaznak a protokollok sikeres végrehajtásához

Köszönöm a figyelmüket!

