Biztonsági kiegészítések szolgáltatás orientált architektúrák Enterprise Service Bus-on keresztüli kommunikációjához

Óbudai Egyetem, Neumann János Informatikai Kar

Diplomamunka (2016)

Tóth Géza

Konzulens:
Dr. Szenes Katalin

Motiváció

- Napjaink elosztott informatikai rendszereinek biztonságát alapvetően befolyásolja, hogyan oldható meg az összetett rendszeren belüli kommunikáció bizalmas és hiteles voltának biztosítása.

- A dolgozatban bemutatott megoldásom a SOA architektúrák azon esetével foglalkozik, mikor a rendszeren áthaladó információk különböző részei biztonsági szempontból eltérő kezelést igényelnek.

Áttekintés

- SOA architektúra, szolgáltatás alapú tervezés
- ESB, az integrációs middleware
- SOA architektúrák biztonsági kérdései
- ESB biztonság

Elérendő cél

Elsődleges szempont a kommunikáció bizalmas és hiteles voltának biztosítása, vagyis annak elérése, hogy csak az tudja elolvasni az üzenetet, akinek szól, de ugyanakkor meg tudjon győződni arról is, hogy az üzenet attól érkezett, akitől várta.

További elvárás, hogy az üzenet útközben jogosulatlan szereplő általi lehallgatásának, illetve manipulációjának lehetőségét a minimálisra csökkentsük.

Megoldandó probléma

Tekintsük azt az esetet, amikor egy szervezeten belül olyan rendszer került kialakításra, amely SOA alapokon építkezik, és a szolgáltatás hívások ESB közreműködésével jutnak el a kliensektől a kiszolgálókhoz.

Továbbá minden üzenetben a kliens küld olyan bizalmas információkat is a szervernek, amelyeknek az ESB számára olvashatatlannak kell látszódniuk.

Ezzel szemben az üzenet olyan adatokat is tartalmaz, melyeken az ESB-nek műveleteket kell végezni, tehát ezen adatokat el kell tudnia olvasnia, de ezen adatok bizalmassági foka egyben olyan is, hogy az ESB-n kívül más szereplő számára rejtettnek kell maradniuk.

Felhasznált módszerek

- Üzenetek felosztása
- Szolgáltatástár
- Tanúsítványok
- ESB használat kikényszerítése

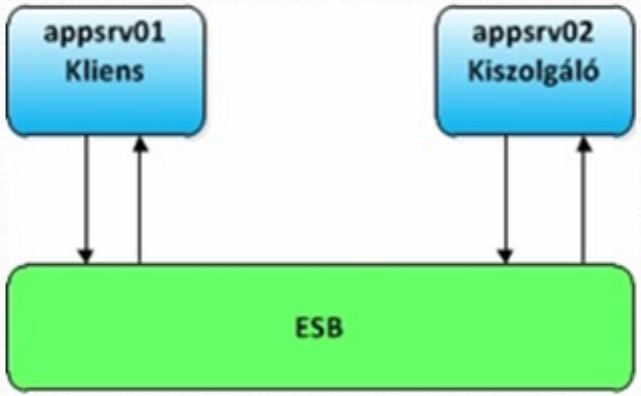
Specifikáció

- Minden üzenet aláírásra kerül, és minden feldolgozás megkezdése előtt az aláírások ellenőrzésre kerülnek (hitelesség).
- Minden feldolgozás esetén ellenőrzésre kerül a szolgáltatástárból, hogy az üzenet a cím alapján valóban attól érkezett, akitől várnánk, és a feladónak joga van ilyen kérés kezdeményezni (hitelesség).
- Minden üzenetben szereplő adat a megfelelő besorolás szerint kerül titkosításra, oly módon, hogy csak a címzett tudja elolvasni (bizalmasság).

Implementáció

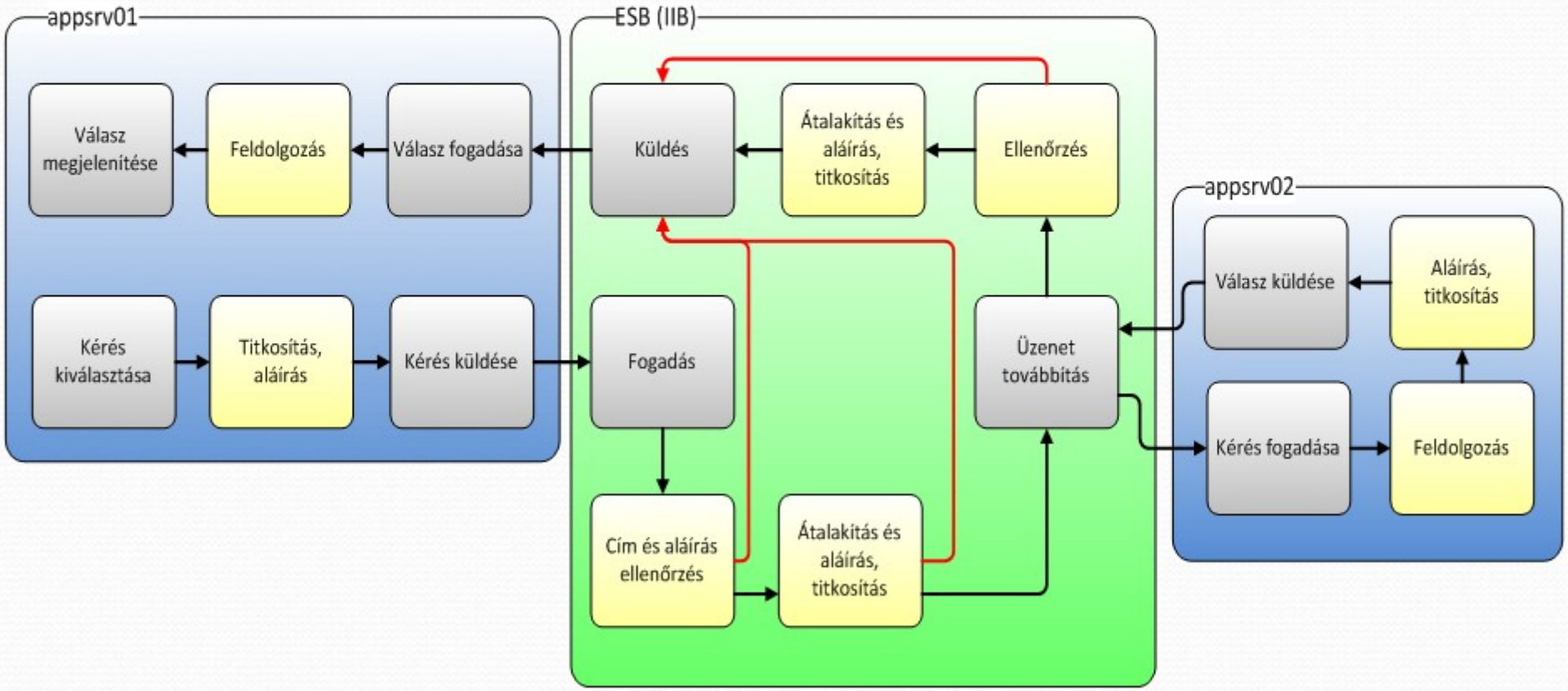
- Java programnyelv
- Bouncycastle csomag
- Valódi szolgáltatás tár helyett egy az ESB-be implementált IP alapú (fájlban tárolt adatokra alapuló) ellenőrzés került felhasználásra.
- A tanúsítványok lokálisan kerültek eltárolásra minden komponens estében.

Architektúra



Minimális architektúra, amely csak a legszükségesebb komponenseket tartalmazza.

Folyamatmodell



Összefoglaló

- ESB ellenőrző szerepének bevezetése
- A komponensek csak azt tudják elolvasni, amivel tennivalójuk van.
- Végigkövethető az adat útja a rendszerben.
- A hitelesség vagy bizalmasság sérülése esetén könnyebben feltárható a kritikus pont.

Továbbfejlesztési lehetőségek

- Tranzakciós azonosító bevezetése és szerepeltetése az eltitkosított üzenetrészekbe
- Teljes értékű szolgáltatás tár implementálása
- Tanúsítványtár alkalmazása
- Rendszeren belül HTTPs használata
- Hálózati architektúra átalakítása a biztonsági elvárásoknak megfelelően

Irodalomjegyzék:

- Dr. Szenes Katalin: A szolgáltatás - orientált architektúrák biztonsági kérdései Az Informatikai biztonság kézikönyve
- Dr. Szenes Katalin: Supporting Applications Development and Operation Using IT Security and Audit Measures
- Jameela Al-Jaroodi, Alyaziyah Al-Dhaheri: Security Issues of Service-Oriented Middleware
- Mehdi Azarmi: An End-to-End Security Auditing Approach for Service Oriented Architectures
- Fumiko Satoh: Methodology and Tools for End-to-End SOA Security Configurations
- Jens Müller: Secure Business Processes in Service-Oriented Architectures – a Requirements Analysis
- Jeremy Epstein : Software Security and SOA: Danger, Will Robinson!
- Jothy Rosenberg, David Remy: Securing Web Services with WS-Security: Demistifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption
- Juliana Georgieva, Mariana Geronova: Security as a Service Model in SOA.

Köszönöm a figyelmet