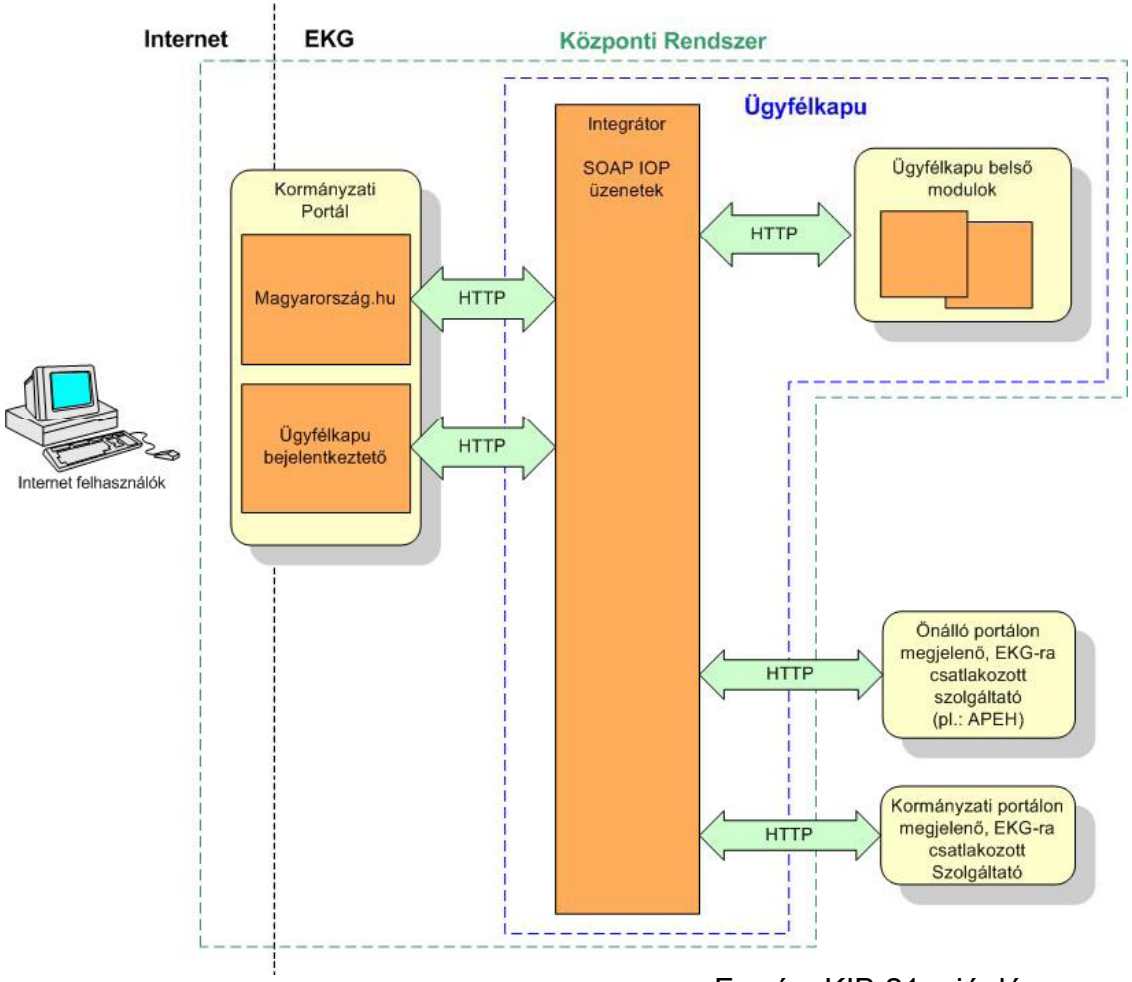
Web service fenyegetések e-közigazgatási környezetben

Krasznay Csaba
IT biztonsági tanácsadó
HP Magyarország Kft.

Bevezetés

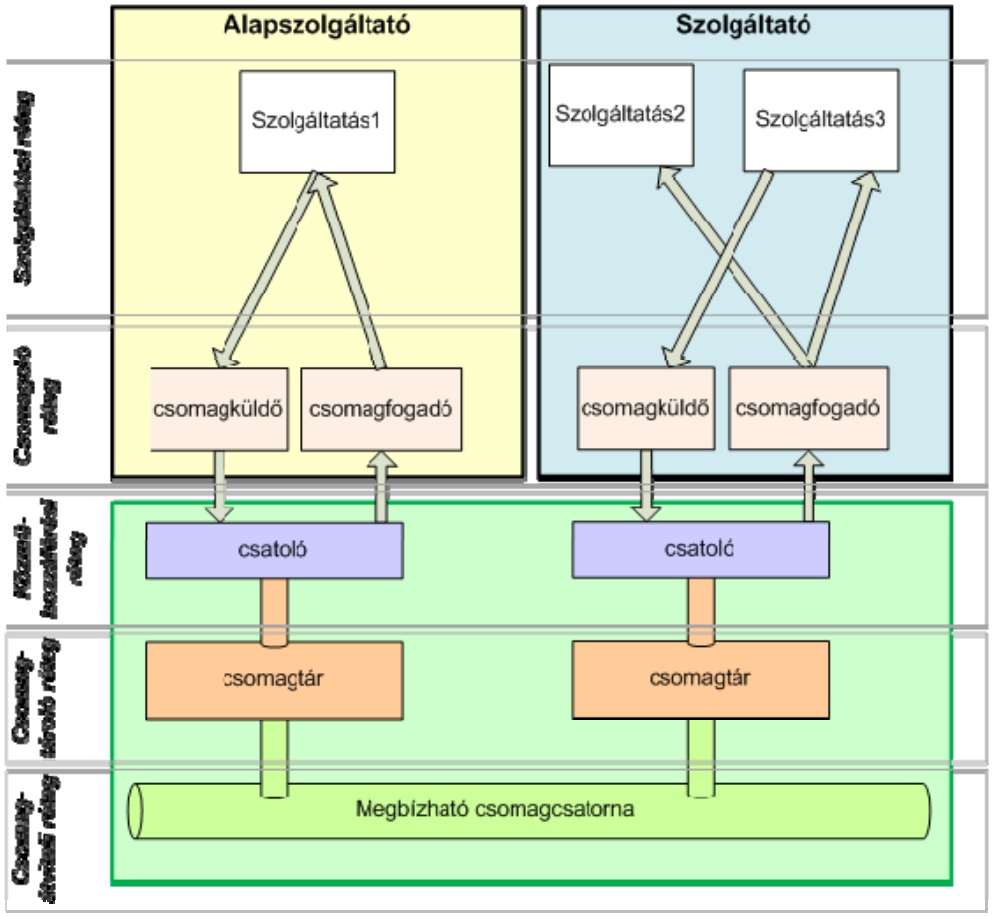
- A Magyar Köztársaság elektronikus közigazgatási rendszere az elmúlt években folyamatosan fejlődött
- 2009-2010-ben jelentős EU források állnak rendelkezésre a további fejlődéshez
- Pontosan lehet követni a fejlesztési tendenciákat
- 2009. tavaszán megjelent az az ajánláskötet, ami definiálja a fejlesztési követelményeket

Az e-közigazgatási rendszer felépítése



Forrás: KIB 21. ajánlás

Az e-közigazgatási rendszer felépítése



Forrás: KIB 28. ajánlás

Fejlesztési irányok

- A cél tehát az e-közigazgatási sín kialakítása
- Az eszköz pedig a szolgáltatás-orientált architektúra, és az azon elérhető web service-ek
- A web service interfészeket a csatlakozó alkalmazások fejlesztői definiálják
- Központi szolgáltatások:
  - Szolgáltatáskatalógus
  - Tokenszolgáltató
  - Hitelesítésszolgáltató
  - E-tár
  - Ügyfélkapu
  - Naplózási szolgáltatás

Biztonsági feladatok

- Az ajánlás szerint foglalkozni kell:
  - Az állampolgárok személyiségi és adatvédelmi jogaival (megfelelő authentikáció és authorizáció),
  - A szolgáltatások biztonságával (titkosítás, erős authentikáció),
  - Az e-közigazgatási közmű biztonságával (jogosultságmenedzsment, naplózás)
- Egy csatlakozó szervezetnek tehát minimálisan meg kell oldania:
  - Az erős authentikáció megvalósítását
  - A tokenszolgáltatóhoz történő integrációt
  - A PKI alapú működést (pl. SSL/TLS)
  - A belépést a központi jogosultságmenedzsment rendszerbe
  - A naplóadatok automatikus vagy manuális kiadását

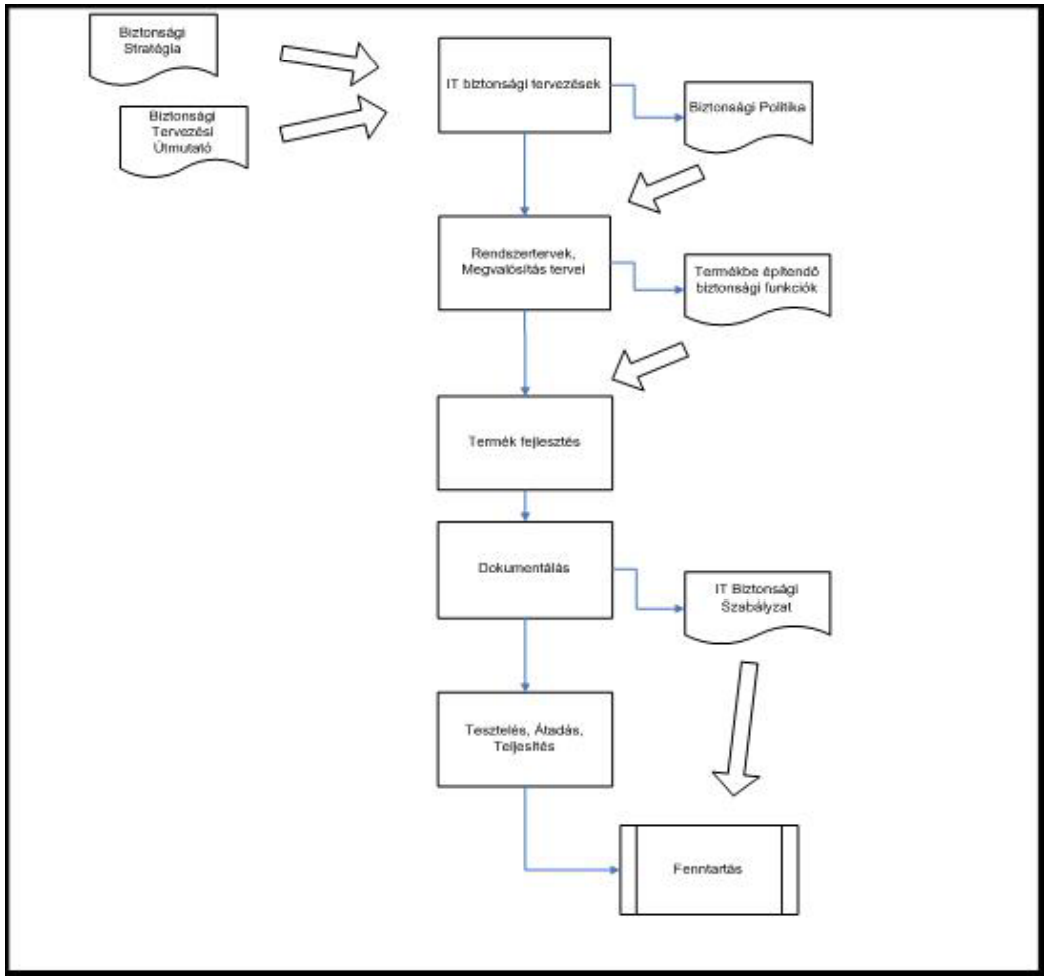
IT biztonsági a pályázat szemszögéből

1. Pályázati felhívás (projekt megfogalmazásakor) összeállításakor be kell építeni azokat a megvalósítandó feladatokat, amelyek garantálják a biztonsági követelmények kielégítését. Pályáztató feladata
2. A pályázat kötelező elemévé kell tenni a biztonság megvalósításához szükséges erőforrások tervezését a pénzügyi keret tervezésékor. Pályáztató feladata
3. A projekt monitoring követelményeiben szerepeltetni kell a biztonsági indikátorokat és azok rendszeres jelentését kötelezővé kell tenni. Pályáztató feladata
4. A pályázatok elbírálásakor az IT biztonsági követelményekre vonatkozó elvárásokat meg kell jelentetni és megfelelő súllyal kell az elbíráláskor, a támogatás odaítélésekor figyelembe venni. Elbíráló feladata
5. A finanszírozási, támogatási szerződésben meg kell jelentetni a biztonságra vonatkozó követelményeket és a be nem tartáskor alkalmazandó szankciókat. Támogató feladata
6. A pályázati anyag összeállításakor figyelembe kell venni a kiírásban megjelent követelményrendszert. Pályázó, projektgazda feladata

IT biztonsági a pályázat szemszögéből

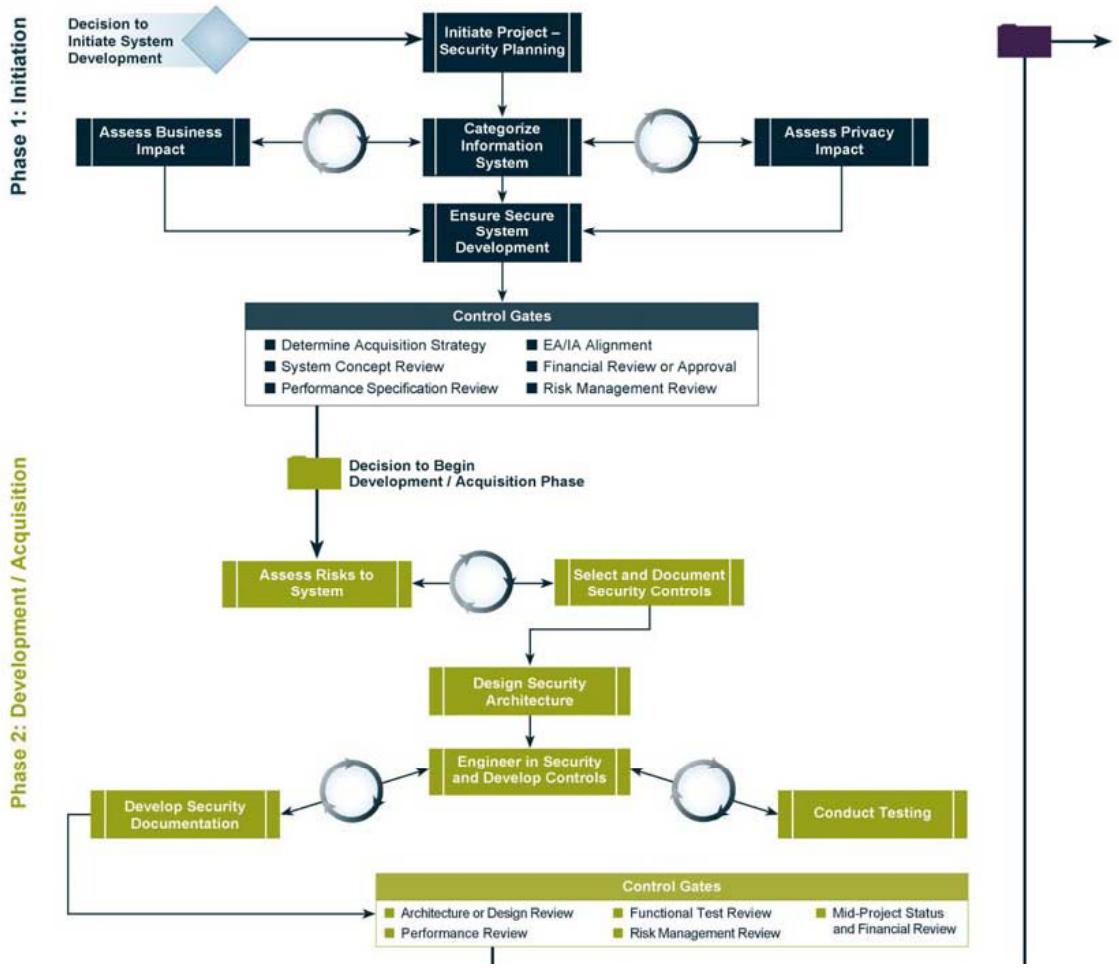
7. A megvalósítás tervezésekor be kell tervezni a biztonságra vonatkozó követelmények megvalósítását is. Pályázó, projektgazda feladata
8. Implementációs munkák során meg kell valósítani a biztonságra irányuló követelményeket, funkciókat. Pályázó, projektgazda, implementációt végző feladata
9. Az eredmények átvételekor, rendszer élesítéskor csak a biztonsági követelményeket igazoltan kielégítő rendszert szabad élesbe állítani. Pályázó, projektgazda, átvevő feladata
10. A támogatási összeg folyósítása előtt meg kell győződni a biztonságra vonatkozó követelmények érvényesüléséről. Felügyelő, támogató, projektgazda feladata
11. A megvalósított biztonsági szint fenntartása érdekében biztonsági rendszert kell üzemeltetni. Pályázó, projektgazda feladata

IT biztonság a fejlesztés szemszögéből



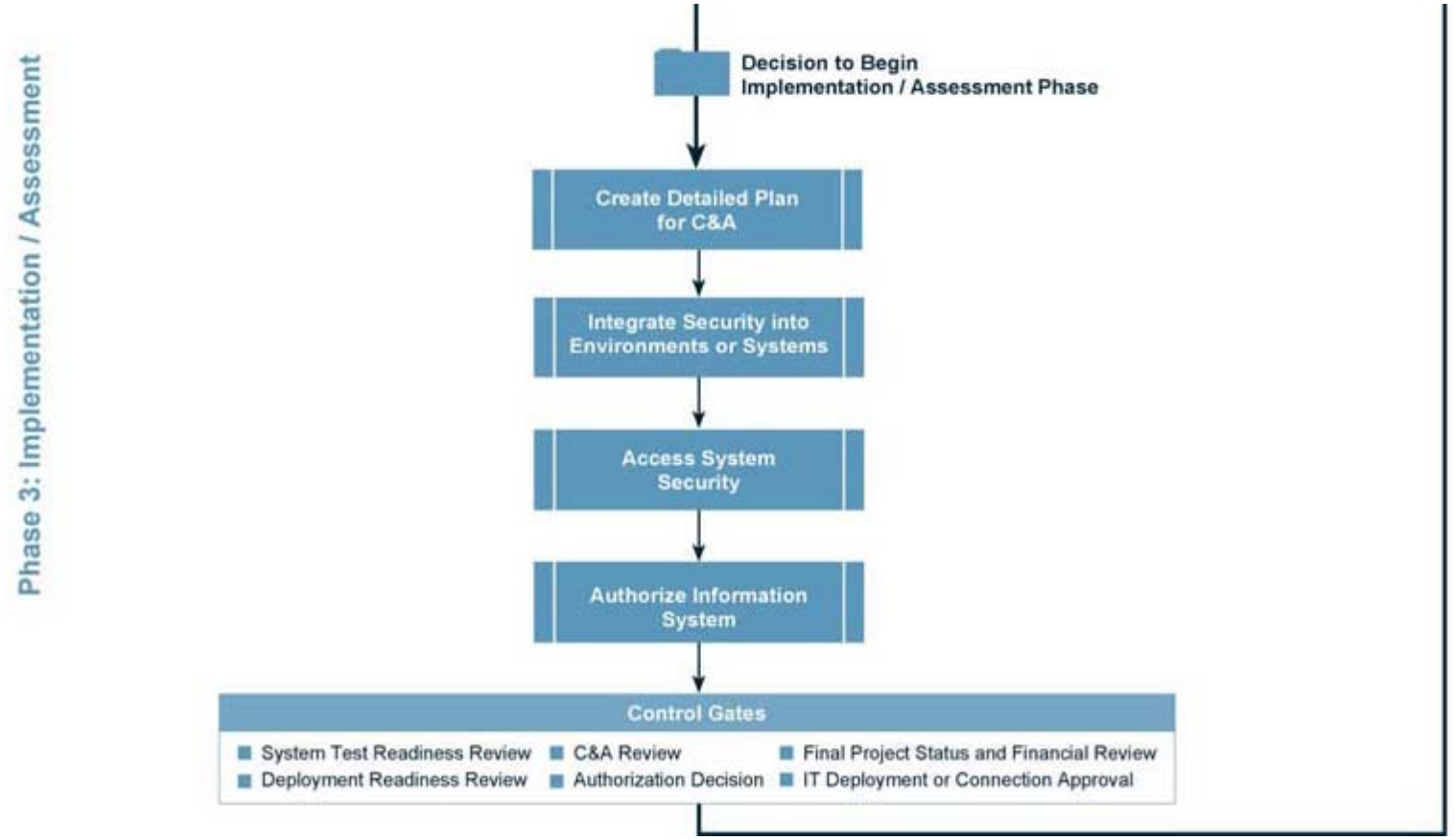
Forrás: KIB 28. ajánlás

Vagy ahogy az USA-ban elképzelik...



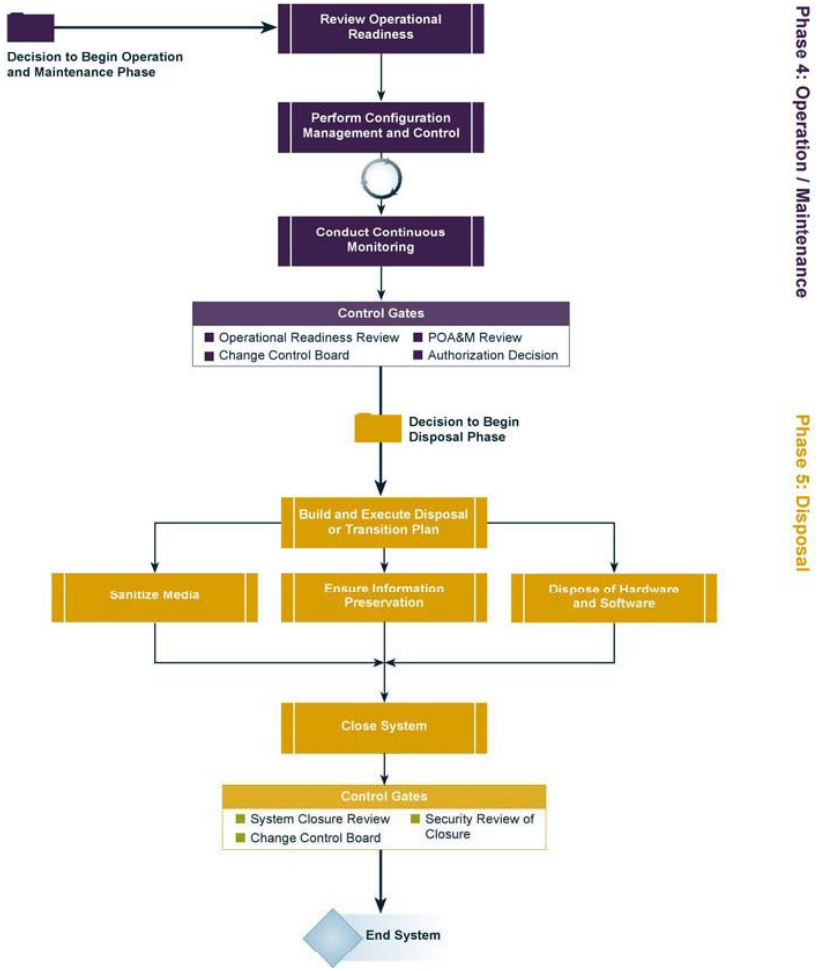
Forrás: NIST SP 800-64

Vagy ahogy az USA-ban elképzelik...



Forrás: NIST SP 800-64

Vagy ahogy az USA-ban elképzelik...



Forrás: NIST SP 800-64

Web service fenyegetések

- Az ajánlások nagyon keveset foglalkoznak a SOA környezetből adódó fenyegetésekkel
- Annak ellenére, hogy szoftver oldalról ez tűnik a leggyengébb láncszemnek
- A fő veszélyforrás az, hogy komplex, egymástól függetlenül fejlesztett rendszerek integrálódnak webes technikákkal, sokszor a nyílt interneten keresztül elérhető interfészekkel, melyek sokszor érzékenyek a sokak által ismert támadásokra

Web service fenyegetések

- Kliens oldali fenyegetések:
  - Ajax komponensek (pl.XSS, cross-site Request Forgery, Cross-Domain támadások)
  - Sérülékeny böngészők
- Struktúra szintű fenyegetések:
  - XML Node manipulálás (SQL injection, távoli kódvégrehajtás, XSS, parserek támadása)
- Protokoll szintű fenyegetések:
  - A protokoll fejlécének és tartalmának manipulálása
- Szerver oldali fenyegetések
  - Az alkalmazás szervert érintő támadások (pl. Buffer overflow)
  - Alkalmazás hibák (pl. hitelesítési, jogosultsági, beszúrásos, rendelkezésre állási, sessionkezelési, és adatszivárgási hibák)

E-közigazgatási aktorok

- Humán ügyfél: egy nevesített személy küld e-mailben vagy weboldalon keresztül üzenetet, és ezeken a felületeken tud üzenetet is fogadni.
- Humán ügyintéző: olyan köztisztviselő, aki e-mailben vagy weboldalon keresztül tud üzenetet küldeni és fogadni.
- Ügyfélkapu: a Hivatali Kapun keresztül tud üzeneteket küldeni és fogadni.
- Kliens alkalmazás: olyan, közigazgatásilag nem kontrollált alkalmazás, mely humán szubjektumhoz nem feltétlenül köthető módon küld és fogad üzeneteket, pl. web service interfészen keresztül.
- Közigazgatási alkalmazás: olyan, közigazgatásilag kontrollált alkalmazás, mely humán szubjektumhoz nem feltétlenül köthető módon küld és fogad üzeneteket, pl. web service interfészen keresztül.

Kommunikációs irányok

Küldő / Fogadó	Humán ügyfél	Humán ügyintéző	Ügyfélkapu	Kliens alkalmazás	Közigazgatási alkalmazás
Humán ügyfél		X	X		X
Humán ügyintéző	X	X	X	X	X
Ügyfélkapu	X	X		X	X
Kliens alkalmazás		X	X		X
Közigazgatási alkalmazás	X	X	X	X	X

Javasolt védelmi intézkedések

- Humán ügyféltől származó üzenet:
  - Input validálás programozott módon vagy eszköz felhasználásával
  - Erős authentikáció
- Humán ügyintézőtől származó üzenet:
  - Erős authentikáció
  - Josultsági rendszer
  - Felelősségek szétválasztása
  - Naplózás
- Ügyfélkaputól származó üzenet:
  - Formátumellenőrzés

Javasolt védelmi intézkedések

- Kliens alkalmazástól származó üzenet
  - WS-Security használata
  - Formátummegkötés
  - Adminisztratív szabályok
  - KIB 25. szerinti tanúsítás
- Közigazgatási alkalmazástól származó üzenet
  - KIB 28. megfelelőség
  - Örökölt rendszereknél speciális web service használata

Összefoglalás

- A SOA környezet biztonsági szempontból különös figyelmet érdemel
- Megjósolható, hogy a körültekintő tervezés, implementálás és üzemeltetés mellett is lesznek biztonsági incidensek, ami a SOA-ra vezethető vissza
- Ezért ne csak a preventív, hanem a detektív és korrektív védelmi intézkedések is kapjanak fontos szerepet!

Köszönöm.

E-mail:
csaba.krasznay@hp.com