atbusiness

Web Services tietoturvahaasteet

atbusiness Tietoturvatorstai
27.11.2003

Jari.Pirhonen@atbusiness.com
Tietoturvallisuuspäällikkö ja -konsultti, CISSP, CISA
AtBusiness Communications Oyj

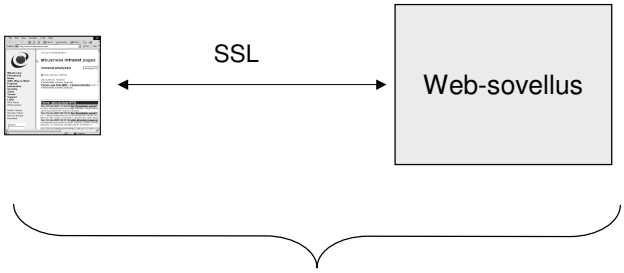
www.atbusiness.com
www.iki.fi/japi/

Web Services

atbusiness

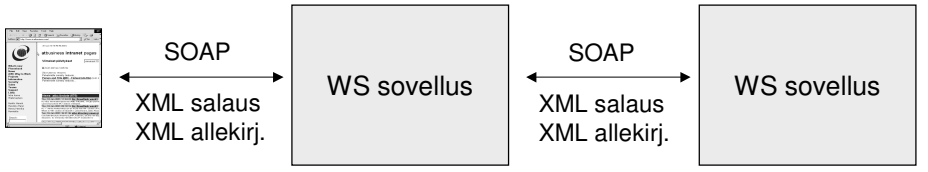
- ”Sovelluskomponentteja, jotka on kuvattu WSDL-esitystavalla ja käytettävissä SOAP-protokollan avulla standardien verkkoprotokollien yli”
- Web Services = XML + WSDL + SOAP (+ UDDI)
- Löyhä sidos sovellusten välillä
  - toteutustavalla ei merkitystä
  - vrt. Java RMI, CORBA, DCOM

Perinteinen web-sovellus



Tietoliikenteen salaus ja eheys (point-to-point)

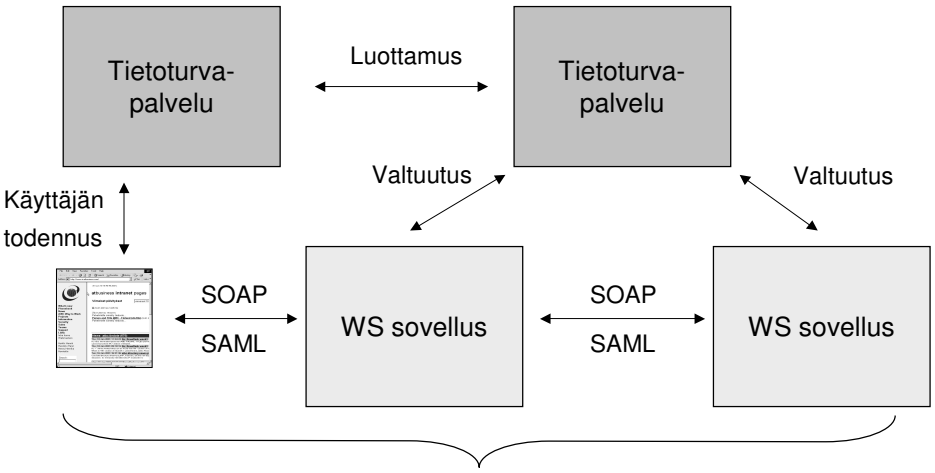
Web Services
perusmalli



Viestien salaus ja eheys (end-to-end)

Web Services
monimutkaisempi malli

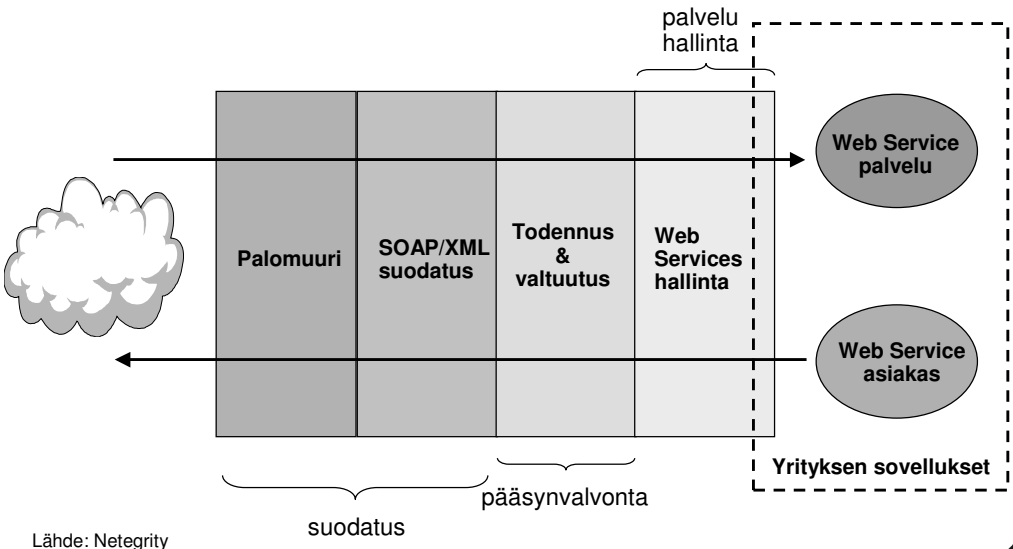
atbusiness



Viestien salaus ja eheys, käyttöoikeuksien delegointi, valtuutus

Web Services arkkitehtuuriehdotus

atbusiness



Lähde: Netegrity

Lähtökohta

- XML, SOAP ja Web Services - tietoturva mietitty jälkikäteen
- Web Services tietoturva <> WS Security
- Analyytikot (Gartner, Forrester, Hurwitz, Burton Group, ZapThink) nimeävät Web Services tietoturvan yhdeksi yritysten suurimmista haasteista lähivuosina.
- Ensimmäiset sovellukset lähellä ”perinteisiä” web-sovelluksia.
- Tuotteissa luvataan enenevässä määrin tukea Web Services tietoturvaan liittyville standardeille (XML, SAML, XKMS,..). Yhteensopivuus todennäköinen ongelma.
- Standardointi käymistilassa – standardeissa päällekkäisyyksiä
- Nykyinen WS-Interoperability dokumentti (Basic Profile Version 1.0a, 8.8.2003) kuittaa tietoturvan SSL-käyttömahdollisuudella.

Haasteita

- Monimutkaisuus
  - Sovellusten vaikeuskerrointa nostetaan taas
- Kypsymättömyys
  - Standardit elävät
  - Työkaluja ja valmiita rajapintoja vähän
  - Yhteensopivuusongelmat
- Hype
  - Palveluita halutaan nopeasti. Mietitäänkö riskejä?
  - Tuotteisiin halutaan nopeasti Web Services ”leima” => yhteensopivuusongelmat, kehittyneet piirteet puuttuvat, bugeja.
- Sovellusten välinen kommunikointi
  - Web Services lupaus piilee sovellusten välisessä kommunikoinnissa.
  - Useita osapuolia ja sovelluksia tiedonkäsittelyketjussa.
  - Tapahtumien aikaleimat, kellojen synkronointi.

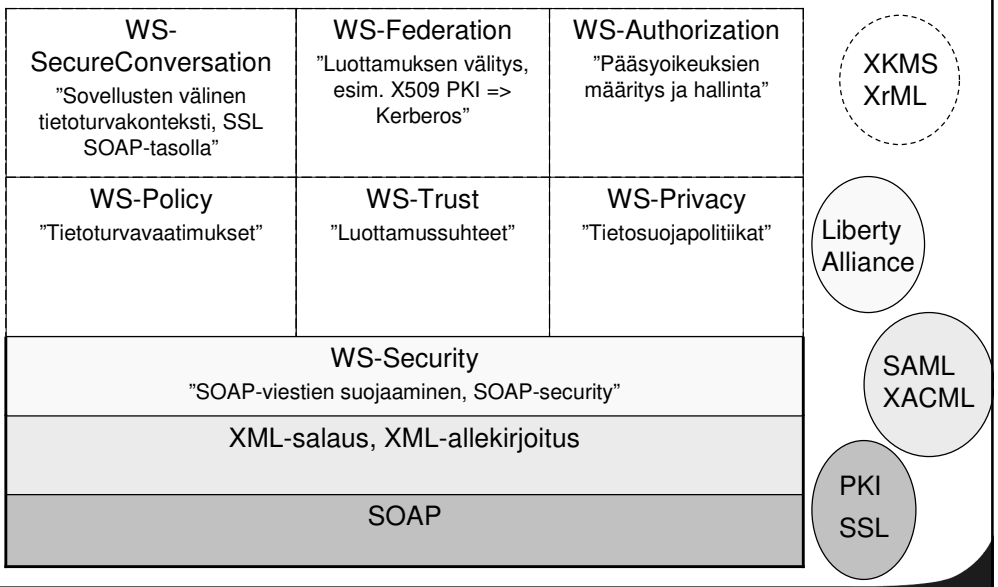
Haasteita

- Tietoturvafokus muuttuu
  - Haasteena ei ole ulkopuolisten pääsyn estäminen, vaan kommunikoivien osapuolten varmistaminen ja valtuutus.
  - Käyttäjätietojen, valtuuksien ja tietoturvavaatimusten käsittely sovellusten välillä.
  - Käyttäjätietojen hallinta
  - Käyttäjäoikeuksien delegointi.
- Roolipohjainen valtuutus (RBAC)
  - Ison yrityksen tarvittavien roolien löytäminen sovellustarpeisiin on haasteellinen tehtävä
  - Vastuut, toimintamallit,…

Haasteita

- PKI
  - SSL ei välttämättä enää riitä
  - Salaus ja digitaaliset allekirjoitukset välttämättömyys monimutkaisissa (hyödyllisissä) sovelluksissa.
  - XML-salauksen ja –allekirjoitusten käyttöönotto vaatii salausteknologioiden perusosaamista: salausalgoritmit, tiivisteet, varmenteet, sähköiset allekirjoitukset, sulkulistat,…
- Luottamuksen hallinta
  - Kuinka osoitat tietoturvan olevan kunnossa?
  - Kuinka varmistat eri osapuolten tietoturvan?
  - Luottamuksen väärinkäyttömahdollisuudet minimoitava.
  - Onko luottamus siirrettävissä? Luottaako yrityksesi yhteistyökumppaniensa kumppaneiden kumppaneihin?

Ratkaisuja



SOAP

- XML-pohjainen viestivälitys
- Ei ota kantaa tietoturvaan
- Ei kiinnitä kuljetuskerrosta
  - HTTP, SMTP, FTP, JMS,…
- HTTP suosittu, ”palomuuriystävällinen” kuljetuskerros
  - SOAP ”salakuljetus” palomuurin läpi
  - Speksi suosittelee porttinumeron vaihtamista SOAP-tarkoitukseen
- Voidaan käyttää sekä RPC että viestinvälitystarkoitukseen
  - ”Not a glue, but an email between applications”
- SOAP-viestit voidaan reitittää usean toimijan kautta
  - Skaalaus, protokollamuunnokset, viestisisällön esitystavan muunnos
- SOAP-liikenteen suodatus
  - Molempiin suuntiin
  - Checkpoint, Vordel, WestBridge, Forum Systems, DataPower

XMLENC
XML Encryption

- XML dokumentin tai sen osan salaus
  - Elementti tai elementin sisältö
- Dokumenttiin linkitetyn tiedon salaus
  - Myös salattu tieto voidaan tallettaa ”raakana” XML-dokumentin ulkopuolelle
- Kuinka yhdistät salauksen ja allekirjoituksen?
  - Allekirjoitat ensin, sitten salaat sekä tiedon että allekirjoituksen?
  - Allekirjoitat ensin, sitten salaat vain tiedon, et allekirjoitusta?
  - Salaat ensin ja allekirjoitat salatun tiedon?
  - Allekirjoitat – salaat – allekirjoitat uudestaan?

XMLDSIG
XML Digital Signature

- XML dokumentin tai sen osan digitaalinen allekirjoitus
- Dokumenttiin linkitetyn tiedon allekirjoitus (URI)
- XML-muoto vs. käyttäjälle esitetty muoto
- Myös käytettävä DTD allekirjoitettava
- XML:n allekirjoitus tehdään kanoniselle (canonical) muodolle
- Allekirjoitus esitetään XML-muodossa
  - Ei esim. PKCS#7
- XMLDSIG on joustava ja monikäyttöinen mekanismi
  - Mahdollistaa myös virheet ja harhaanjohtamisen
- XAdES – ETSI:n XML-määritys laatu-varmenteisiin liittyviin allekirjoituksiin (2/2002)

WS-Security

- Määrittelee ”vain” tietoturvatiedon sisällyttämisen SOAP-viesteihin
  - Käyttäjätunnus
  - Kerberos-lippu
  - X509-varmenne
  - SAML-kuvaus
  - XrML-kuvaus
- SOAP-viestiosan salaus ja allekirjoitus
- Hyödyntää XML-salausta ja –allekirjoitusta

XACML

eXtensible Access Control Markup Language

- XML-muotoiset pääsylistat (ACL)
  - Ei tietoturvaa XML-dokumentteihin vaan XML-formaatti pääsylistoille
  - Suojauskohteiden ei tarvitse olla XML-dokumentteja
- Tekijä, kohde, toiminto (luku, kirjoitus, luonti, tuhoaminen)
- Kohde jopa XML-dokumentin yksi elementti

SAML

Security Assertion Markup Language

- Sovellusten (ja organisaatioiden) välinen oikeustietojen välitys
- Single Sign-On
  - Mahdollisuus tuotteiden yhteensopivuuteen
- Tunnistus
  - ”Käyttäjä X on todennettu salasanalla ajanhetkellä T”
- Attribuutit
  - ”Käyttäjä X kuuluu yrityksen Y tietoturvatiimiin”
- Valtuudet
  - ”Käyttäjällä X on lukuoikeus CRM-järjestelmän asiakastietoihin”

Federation

- Luottamussuhteiden välittäminen organisaatioiden välillä
  - luottamuksen ja istunnon hallinta, todennuksen laatu, organisaatioiden todennus,…
- Microsoft Passport
  - Microsoftin keskitetty käyttäjärekisteri
  - TrustBridge – Security Proxy (AD-AD, AD-Passport)
- Liberty Alliance Identity Federation Framework (ID-FF)
  - ”Open Standards Community”: Sun, HP, Verisign, BEA, Nokia,…
  - SAML + laajennokset
- WS-Federation
  - Microsoft, IBM, BEA, Verisign, RSA
  - WS-Trust, WS-SecureConversation, WS-SecurityPolicy

XKMS

XML Key Management Specification

- XML-pohjainen PKI
  - X509, PGP, SPKI
  - Ei tarvitse ASN.1:tä
- Tavoitteena poistaa avainten ja varmenteiden käsittely client-sovellukselta
  - Sopii paremmin myös puhelimille ja PDA-laitteille
- X-KRSS: XML Key Registration Service Specification
  - Avainten generointi, rekisteröinti, mitätöinti ja toipuminen
  - Ei massarekisteröintimahdollisuutta (XBULK)
- X-KISS: XML Key Information Service Specification
  - Avainten haku, avainten voimassaolo, luottamuspolkujen käsittely
- XKMS on *avain-keskeinen,* perinteinen PKI *varmenne-keskeinen*
  - Luottamus XKMS -palveluun

Yhteenveto

- Sovellusten monimutkaisuus lisääntyy
  - Tietoturva on huomioitava koko sovelluskehitysprosessissa
  - Haluttu tietoturvataso on *määriteltävä*
  - Hallittu tietoturva-arkkitehtuuri auttaa
- Web Services-sovelluksiin siirtyminen tuo uusia riskejä
  - Paljon uutta opittavaa
  - Uudet sovellusalueet ja tietoturvafokus
- Kasvavaa kiinnostusta uusille tietoturvaratkaisuille
  - Käyttäjätietojen hallinta
  - SSO, keskitetyt valtuutusratkaisut, RBAC
  - Luottamuksen hallinta
  - SOAP-liikenteen tarkistus ja suodatus

Standardien tila

Standardi	Status	Tukijat
XMLDSIG	W3C recommendation, 2/2002	IBM, Microsoft, Verisign, Sun,…
XMLENC	W3C recommendation, 12/2002	IBM, Microsoft, Verisign, BEA, RSA,…
SAML 1.1	OASIS standard, 9/2003	Entrust, BEA, Sun, RSA, Netegrity, Baltimore,…
XACML v.1.0	OASIS standard, 2/2003	BEA, Entrust, IBM, SUN,…
SOAP v.1.2	W3C recommendation, 6/2003	Microsoft, Sun, IBM,…
WS-Security	OASIS draft, 3/2003	IBM, Microsoft, Verisign, HP, BEA, RSA, Sun,…
XKMS	W3C working draft, 4/2003	Verisign, RSA, Microsoft,…
UDDI v.2	OASIS standard 7/2002	IBM, Microsoft,…
XCBF v.1.1	OASIS standard, 9/2003	IBM, Objective Systems,…

http://www.w3.org/TR/, http://www.oasis-open.org/