Paweł Rajba
pawel@ii.uni.wroc.pl
http://kursy24.eu/

Application Security
WS-Trust & WS-Federation

Agenda

- WS-Trust
  - Actors
  - Flow
  - Terminology
- WS-Federation
  - Introduction
  - Profiles
  - Trust topologies
  - Attributes and Pseudonyms services

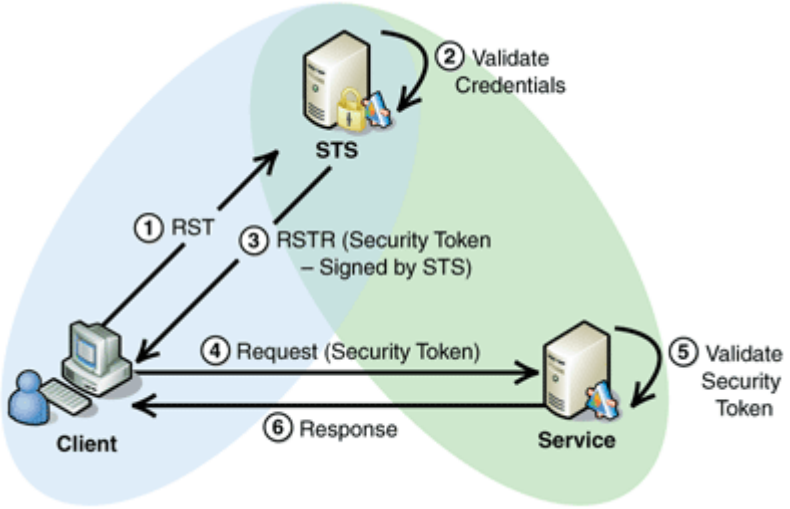
WS-Trust

- Actors
  - A wine web service (W-WS) with a policy
    - Policy says that a SAML token is required with
      - Age
      - Department Of Driving License
  - A DODL web service (D-WS) with a policy
  - A user (U) that wants wine
- Every actor has a certificate with a private key

Based on: http://channel9.msdn.com/Shows/Going+Deep/Vittorio-Bertocci-WS-Trust-Under-the-Hood

WS-Trust

- The flow (simplified)
  - U gets metadata from W-WS
  - U asks D-WS for a security token which fulfill policy
  - U authenticates and gets the security token
  - U uses the security token and buy a wine in W-WS



WS-Trust

- The flow (in details)
  - Using WS-MEX (metadata exchange) U gets a policy from W-WS
    - To know what requirements are and ensure if user is able to complaint these requirements
  - U send a RST (request for security token) to D-WS
    - Signed with a private key of U
    - And encrypted with certificate of D-WS
  - D-WS send a RSTR (RST response) to U with
    - SAML Token for W-WS with
      - New key SK and claim about age which required by policy
        - Encrypted by public key of W-WS
        - Signed by private key of D-WS
    - Proof Token for U with
      - New key SK
        - Encrypted by public key of U
        - Signed by private key of D-WS
  - U gets the response
    - Extract proof token, check signature, decrypt SK
    - Send to W-WS
      - SAML Token
      - Request for wine signed with SK and encrypted with public key of W-WS
  - W-WS gets the request
    - Verify that SAML token is signed by DoDL
    - Decrypt content of SAML token (i.e. SK and claim with age)
      - After these 2 points the policy of W-WS is fulfilled
    - Check signature wine request, decrypt signed SK, check signature
  - U and W-WS has a trust and start conversation

WS-Trust

- Terminology
  - D-WS we usually call Security Token Service (STS)
    - Or Identity Provider (IP)
  - W-WS we usually call Relying Party (RP)
  - U we usually call client

WS-Trust References

- A very good video
  - http://channel9.msdn.com/Shows/Going+Deep/Vittorio-Bertocci-WS-Trust-Under-the-Hood
- Some introductions
  - http://fusesource.com/docs/esb/4.4.1/cxf_security/WsTrust-Intro.html
  - http://msdn.microsoft.com/en-us/library/bb498017.aspx
  - http://msdn.microsoft.com/en-us/library/ff650503.aspx
  - http://documentation.progress.com/output/Iona/artix/5.5/security_guide_java/WsTrust-SSO-Example.html
- How to create a STS
  - http://msdn.microsoft.com/en-us/magazine/dd347547.aspx

WS-Federation

- Federation
  - A collection of domains with a trust
  - Allows interactions between users, applications and other players
- Main goal:
  - Single Sign-On inside trust boundaries
  - Although using different identites revelant to each domain

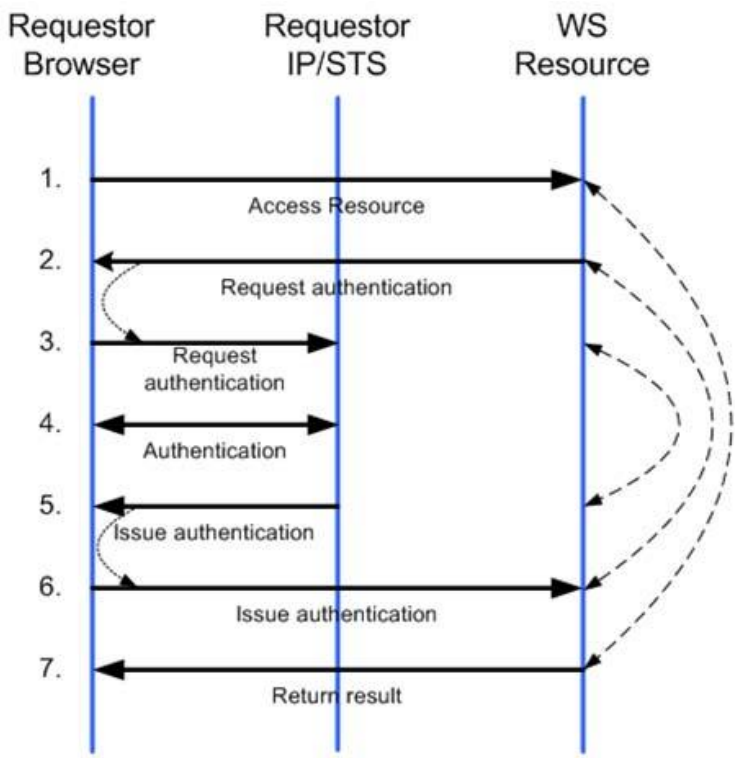
Based on:
http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf
http://www.cs.virginia.edu/~acw/security/doc/Tutorials/WS-Federation.ppt

WS-Federation

- WS-Trust makes possible to have a federation between IdP and RP
  - But still some requirements are not fulfilled
- WS-Federation
  - Adds Federation Metadata to simplify the setup of federated trust relationship between parties
  - Adds Single Sign On & Single Sing Off
  - Adds profiles for classic web applications
  - Adds mechanism for better discovery
  - Adds services for attributes and pseudonyms

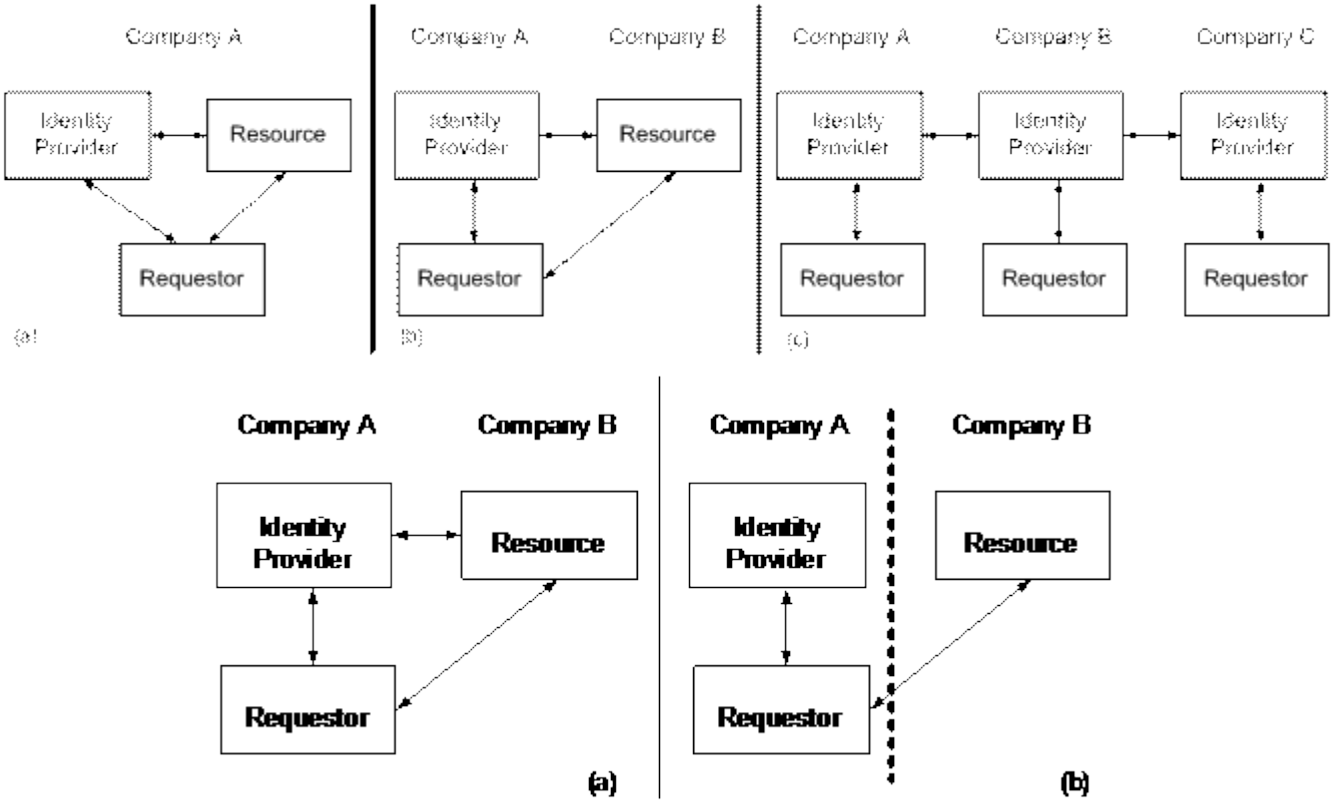
WS-Federation Profiles

- Active Requestor Profile
  - Focus on SOAP Web Services
- Passive Requestor Profile
  - Dedicated for browser client
  - Based on URLs
  - Uses redirections to send messages



WS-Federation

- Supports different scenarios



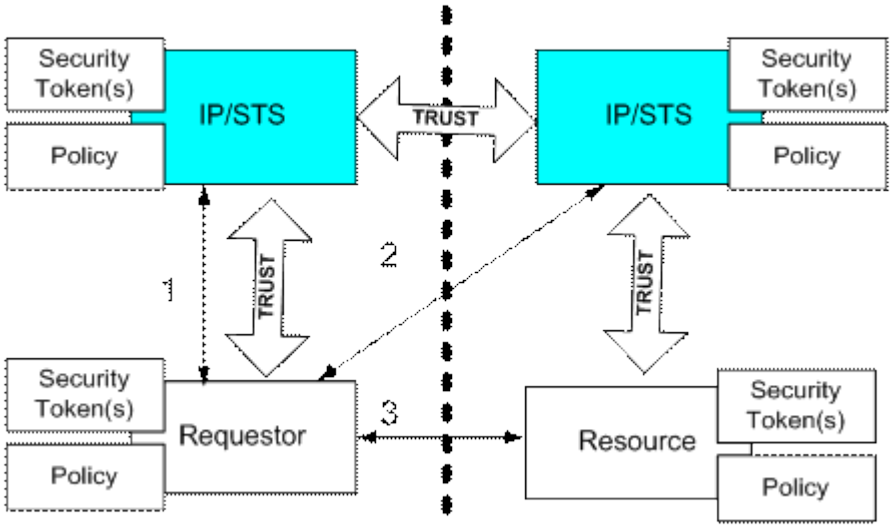
(a) Direct connection (b) Firewall in between, trust by using certificates

WS-Federation

- Architecture of federation should be able to
  - Model business requirements
  - Leverage existing infrastructure
- Main trust topologies
  - Direct trust
    - Exchange
    - Validation
  - Indirect trust
  - Delegation

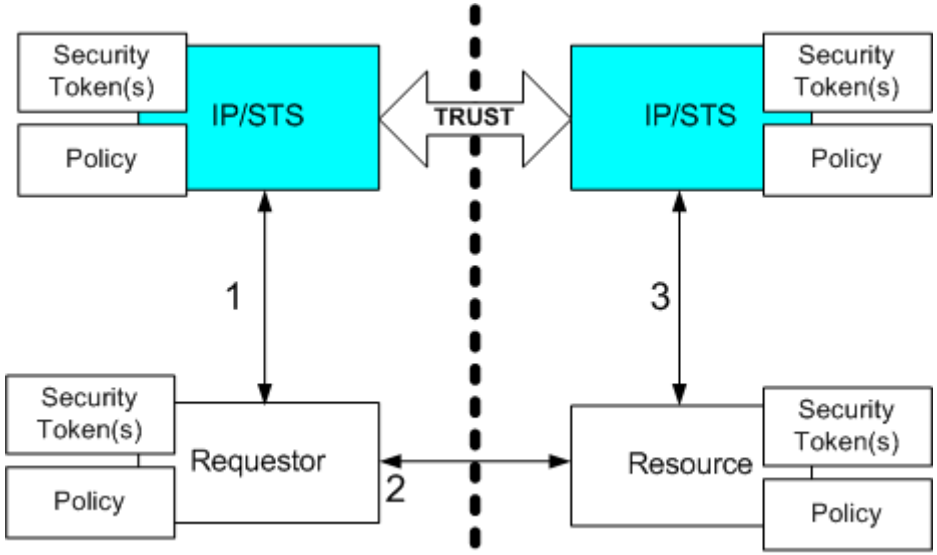
WS-Federation Trust Topologies

- Direct trust with token exchange



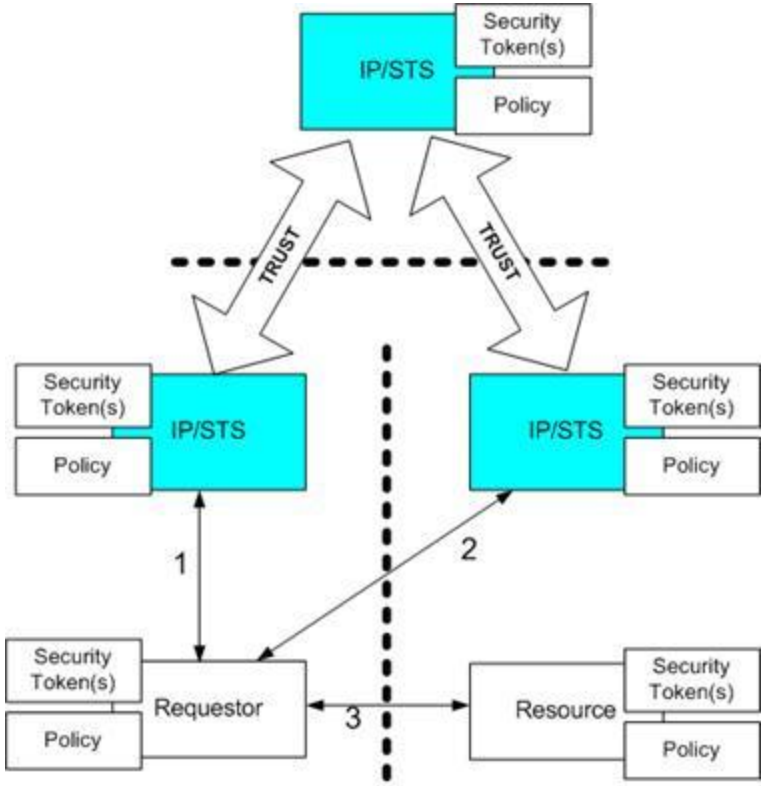
WS-Federation Trust Topologies

- Direct trust with token validation



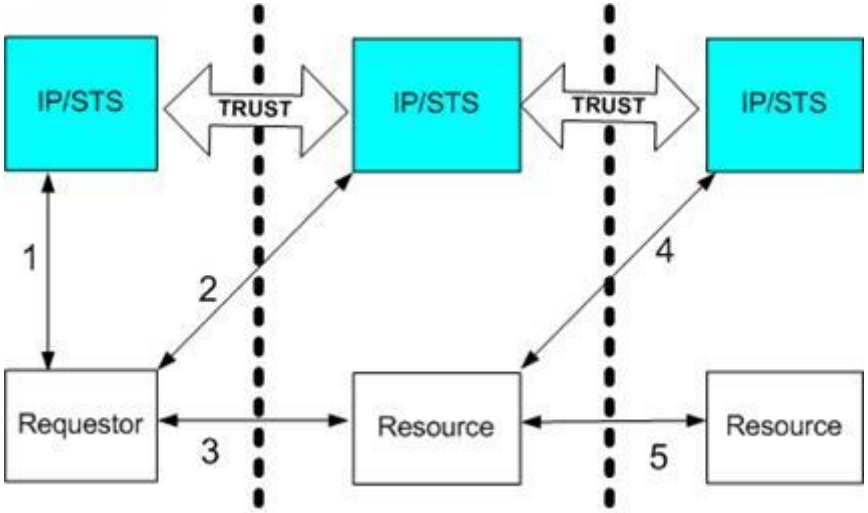
WS-Federation Trust Topologies

- Indirect trust



WS-Federation Trust Topologies

- Delegation



Attributes services

- Attributes give additional information about the requestor
- Scenario: You ask a weather service for the current weather (or visit a weather site); it provides a personalized response because it knows your zip code
- Why it worked:
  - Policy indicated an attribute service
  - Identity information was used to find zip code
  - Weather service was authorized to access zip code (opt-in)

Attributes services

- Attributes scoping

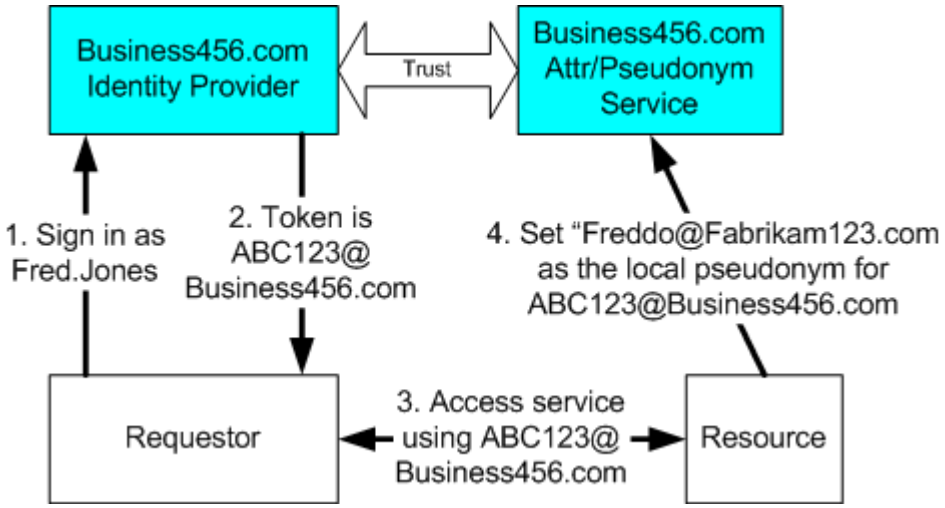
Zip: 12309
FN: Fred
ID: 3442
Nick: Freddo
ID: FJ454
Nick: Fredster
ID: 3-55-34
…

(fabrikam123.com)
(business456.com)
(example.com)

Model allows for attributes to be scoped

Pseudonyms services

- Allows to get pseudonym and access services using pseudonym instead of identity
- Pseudonym can be considered as a specialized attribute



DEMO

- Long, long time ago there was a WIF which allows to create a test STS and federated applications
- In Visual Studio 2012 where is no WIF, functionalities are available by Identity and Access Control templates
  - http://msdn.microsoft.com/en-us/library/hh545418.aspx
- In Visual Studio 2013 there is only integration with cloud
  - http://bartwullems.blogspot.com/2013/11/visual-studio-2013-where-is-identity.html
  - http://www.cloudidentity.com/blog/2012/03/15/windows-identity-foundation-in-the-net-framework-4-5-beta-tools-samples-claims-everywhere-2/
  - http://hanskindberg.wordpress.com/2014/02/25/use-the-wif-sdk-site-templates-in-visual-studio-2013/
  - http://msdn.microsoft.com/en-us/library/hh873305.aspx

WS-Federation References

- Documentation
  - http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf
- Tutorials & presentation
  - http://msdn.microsoft.com/en-us/library/bb498017.aspx
  - http://msdn.microsoft.com/en-us/library/ff359108.aspx
  - http://www.cs.virginia.edu/~acw/security/doc/Tutorials/WS-Federation.ppt