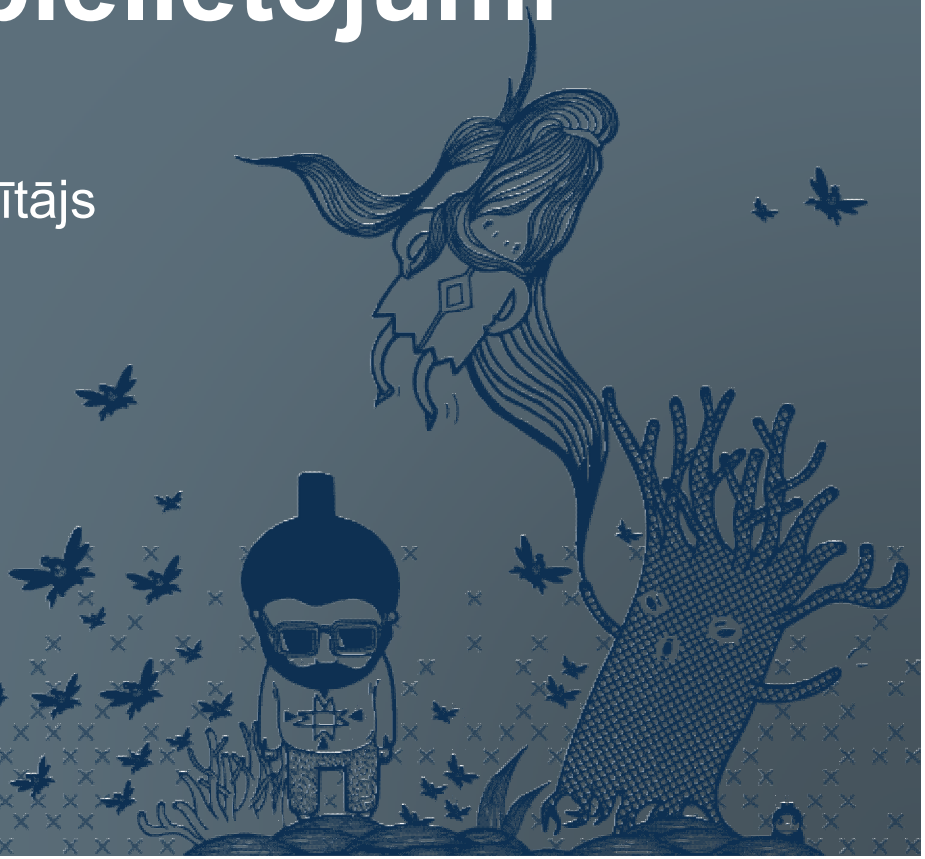
Federatīvās autentifikācijas priekšrocības un pielietojumi

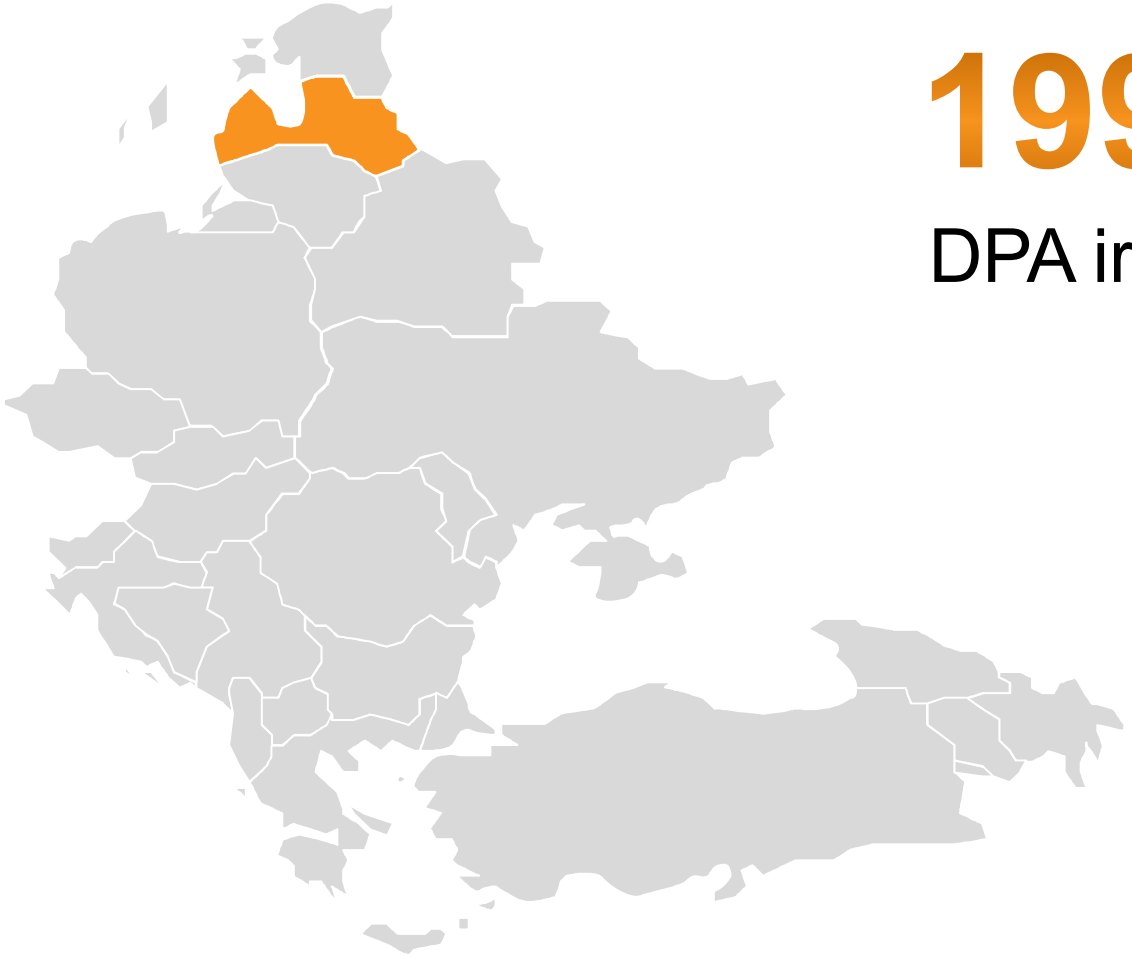
Latvijas piemēri un nākotnes vīzija.

Mārtiņš Orinskis, SIA DPA projektu vadītājs

2012.gada 8. novembris



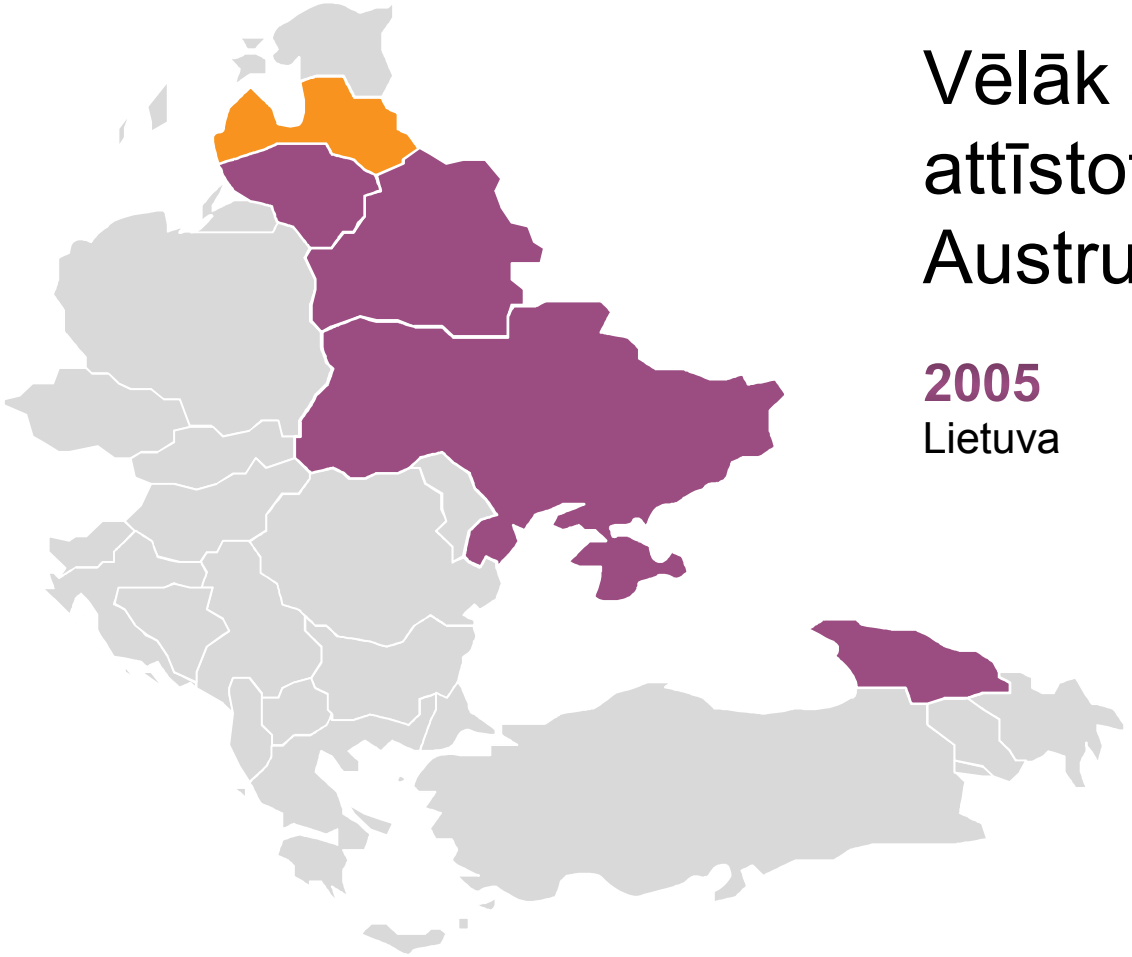
Mūsu stāsts



1997

DPA ir dibināts **Latvijā**

Mūsu stāsts



Vēlāk strauji attīstoties Austrumeiropā:

2005	2007	2009	2011
Lietuva	Ukraina	Baltkrievija	Gruzija

Mūsu risinājumi un pakalpojumi

Mēs varam palīdzēt saviem klientiem ar:

- IT infrastruktūras plānošanu, ieviešanu un uzturēšanu
- Kopdarbības, ziņapmaiņas un informācijas vadības risinājumiem
- Drošības risinājumiem un auditiem
- Specializētu programmizstrādi un testēšanu
- Biometrijas risinājumiem
- Programmatūras licencēšanu

Saturs

- Federatīvā autentifikācija
- Federatīvās autentifikācijas pamatprincipi
- Projekta realizācijas piemērs Latvijā
- Federatīvā autentifikācija lielākā mērogā

Autentifikācijas dārdzība

Ārējo lietotāju konti

Paroļu uzturēšana

Jauni autentifikācijas veidi

Federatīvā autentifikācija reālajā dzīvē

Federatīvās autentifikācijas ieguvumi

Autentifikācijas nodalīšana no autorizācijas

Vispārpieņemtu standartu izmantošana

Ārējo lietotāju pārvaldība

Anonimitātes nodrošināšana

Netiek mainīti eksistējošie lietotāju autentifikācijas veidi

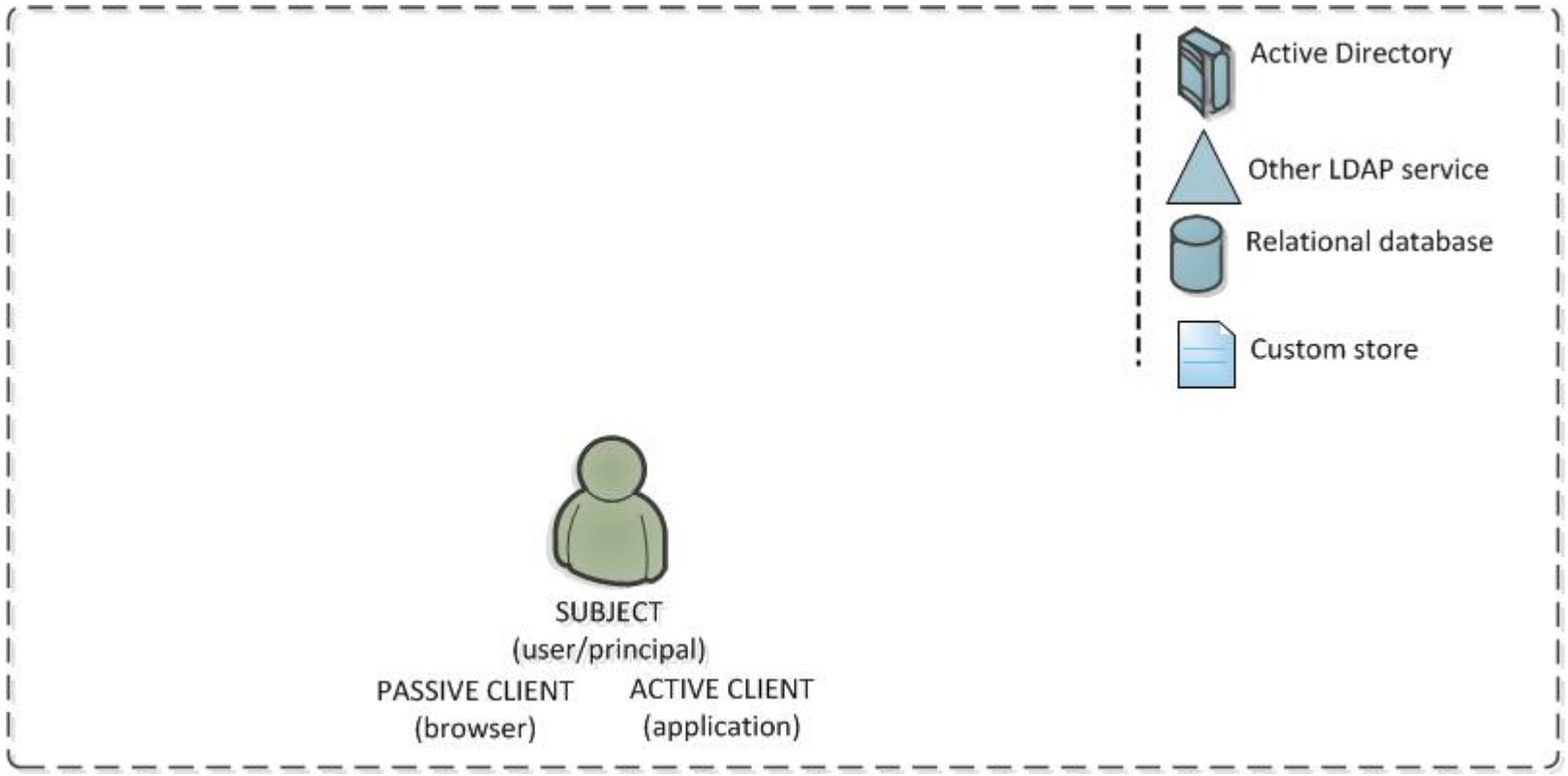
Pamatprincipi:
OASIS standarti - WS*

- WS-Security
- WS-Trust
- WS-SecureConversation
- WS-Federation

OASIS
Advancing open standards for the information society

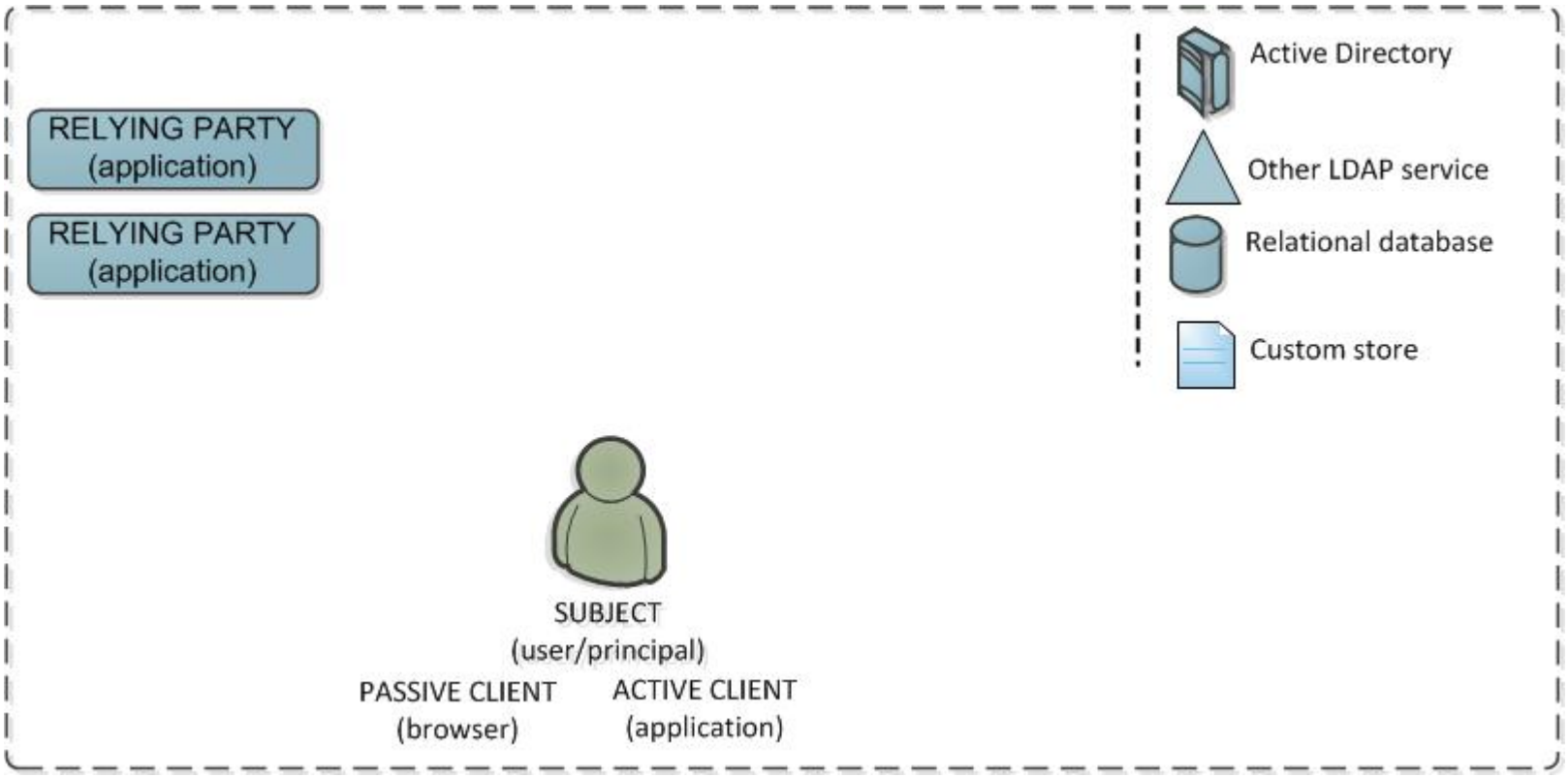
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



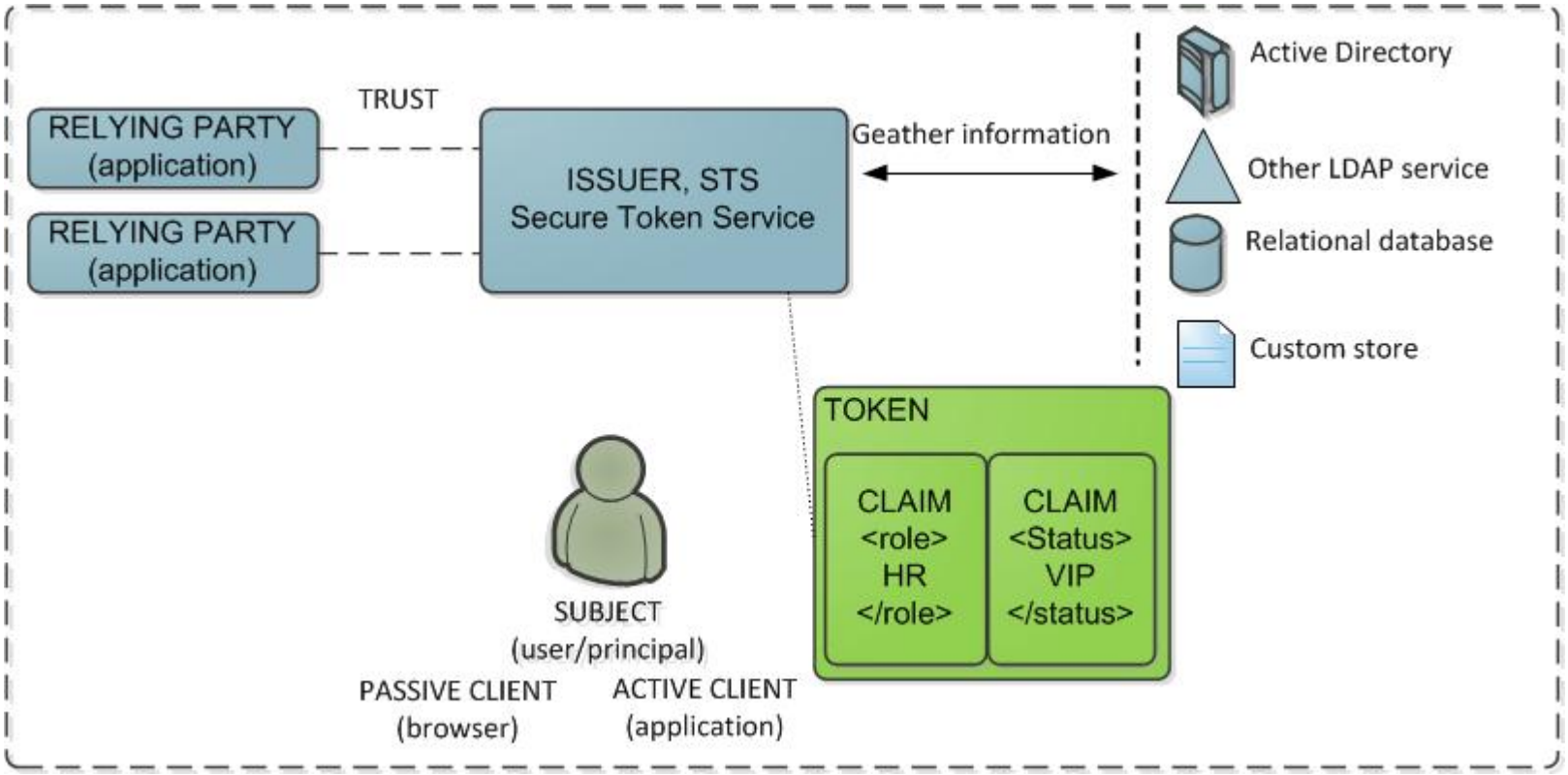
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



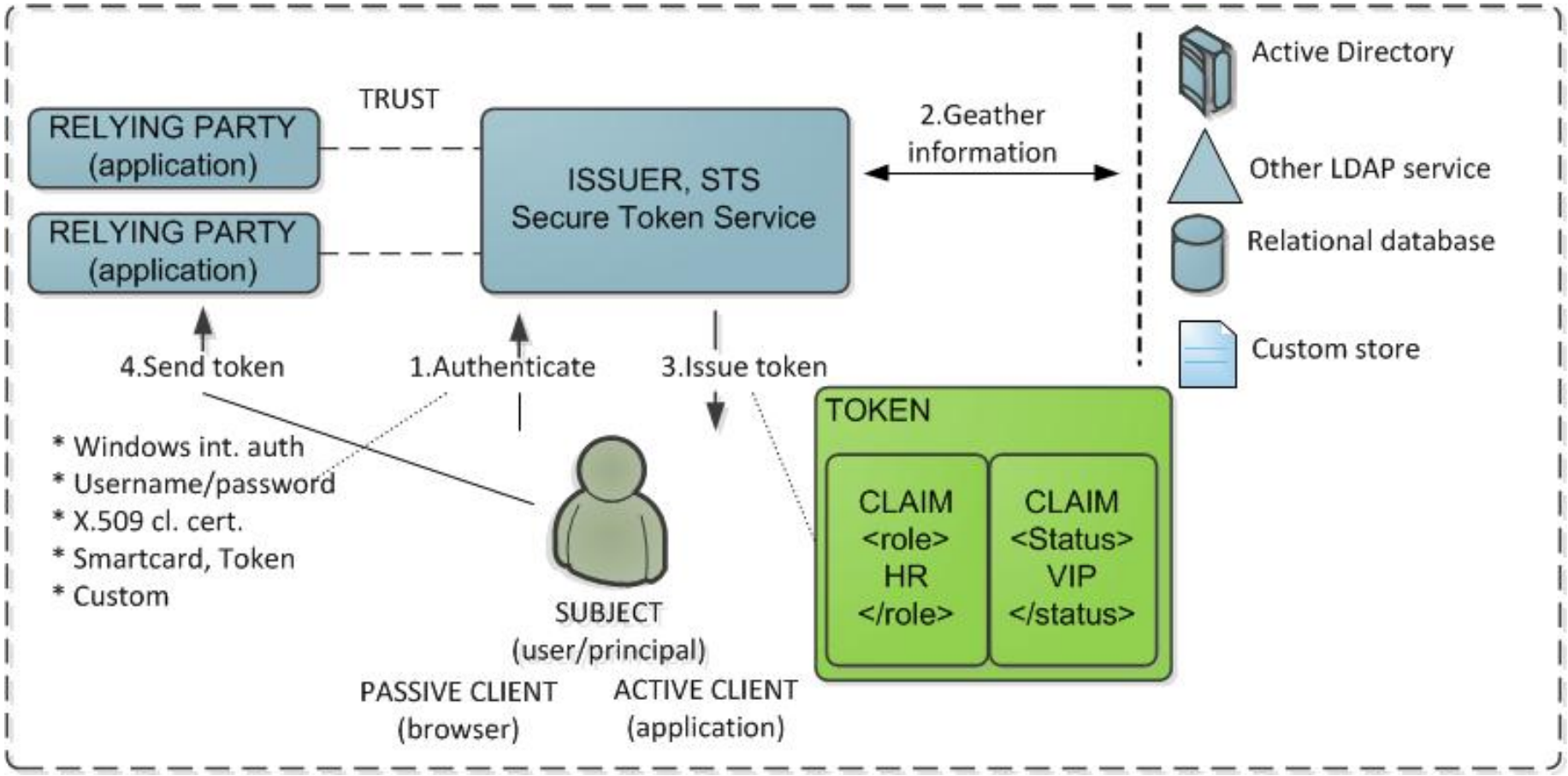
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



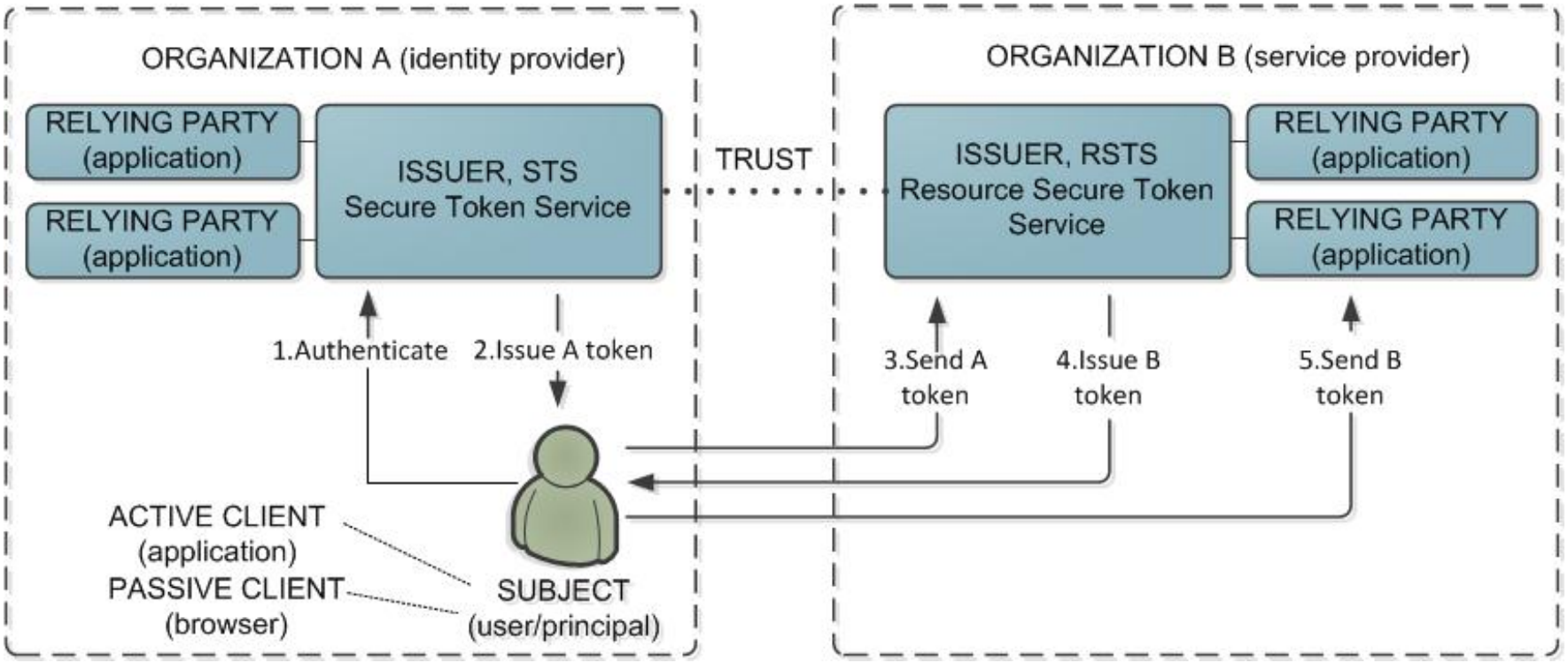
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



Federatīvās autentifikācijas pamatprincipi

Realm – 2 darbības sfēras: Divas iestādes



Izmantošanas piemērs

Projekta uzdevumi

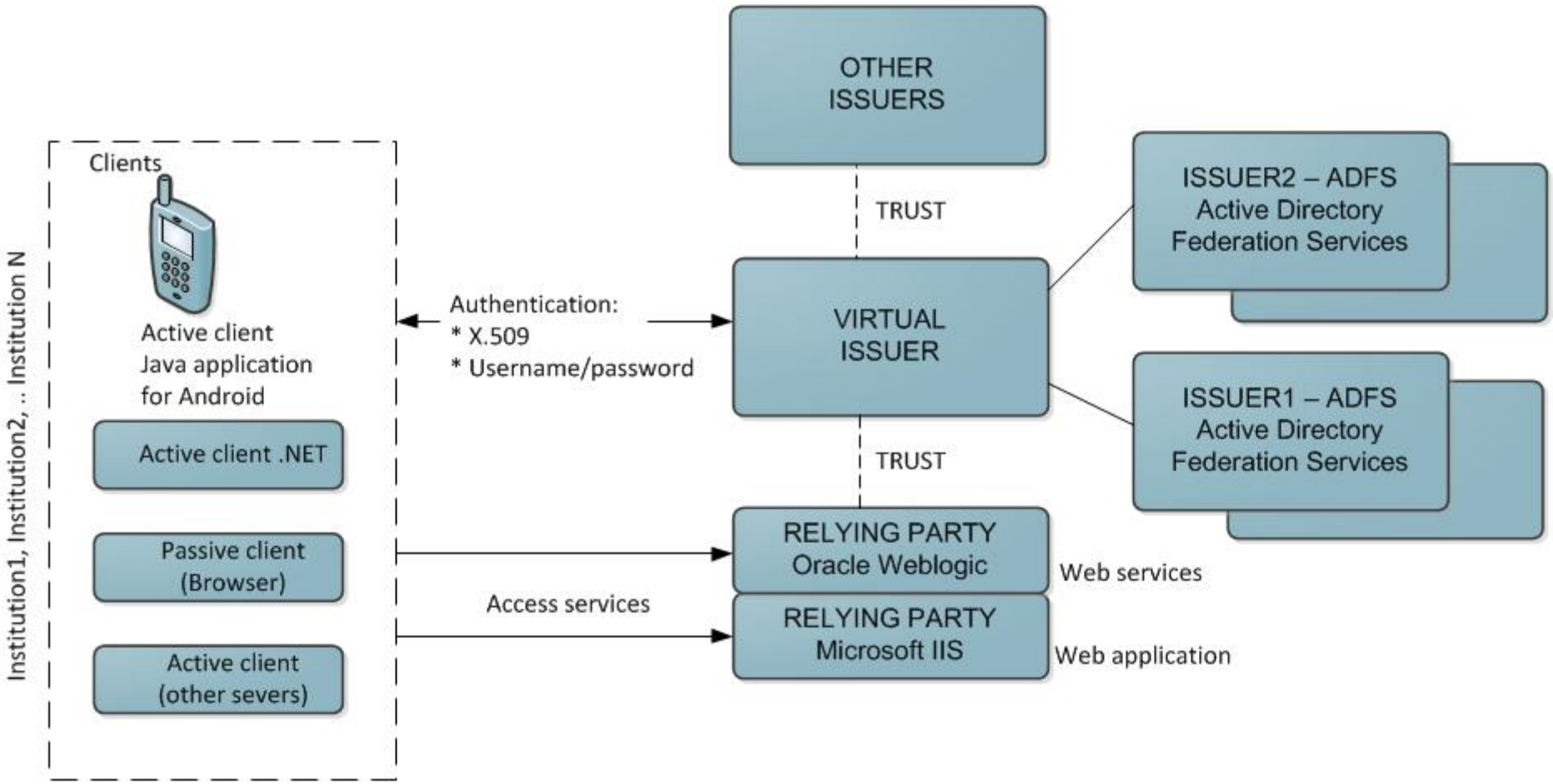
Web-service autentifikācija un autorizācija

Platformu neatkarīgs autentifikācijas serviss

Autentifikācija dažādu iestāžu darbiniekiem

Autentifikācija iekārtām un sistēmām

WebServices, Active/Passive Clients + HA + MS ADFS + Weblogic + .NET + JAVA



WebServices, Active/Passive Clients + HA + MS ADFS + Weblogic + .NET + JAVA

1: Add Logic to Your Applications to Support Claims

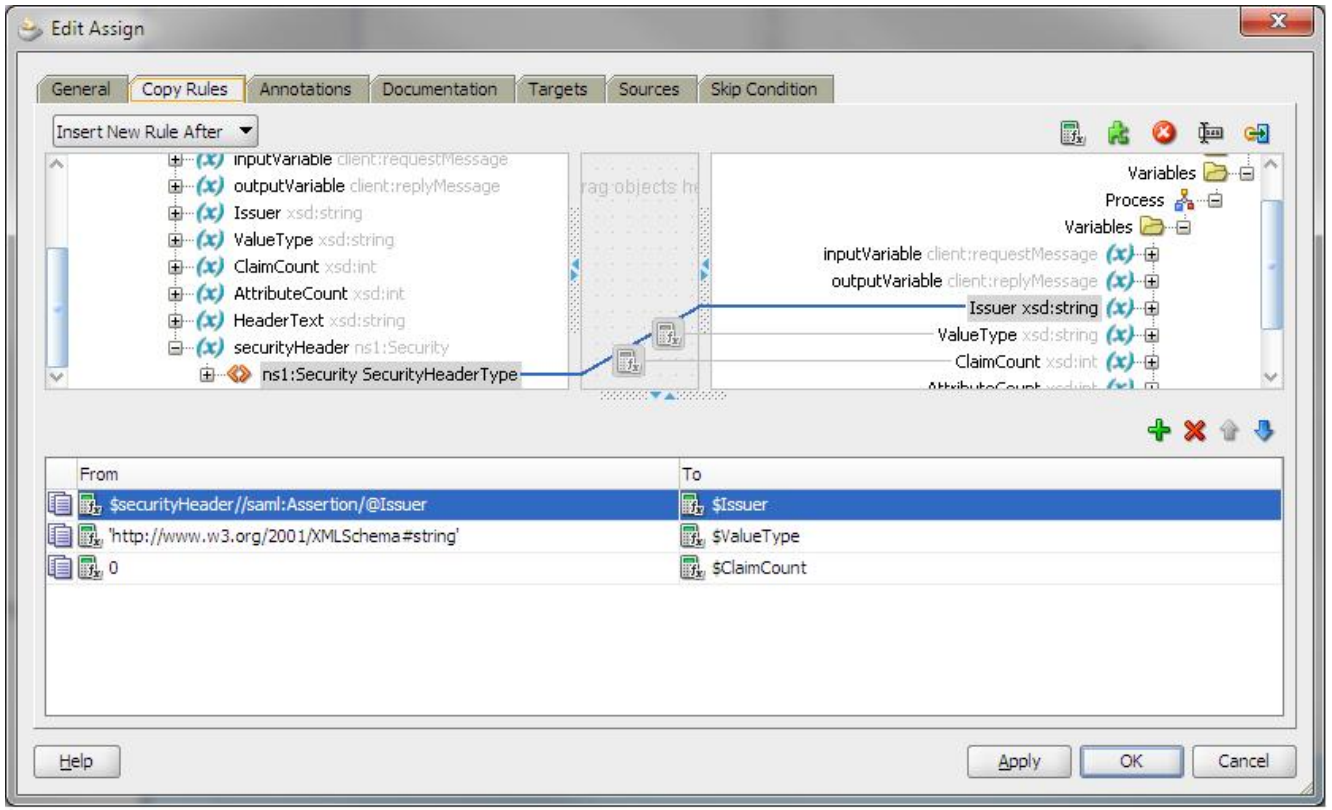
2: Acquire or Build an Issuer

3: Configure Your Application to Trust the Issuer

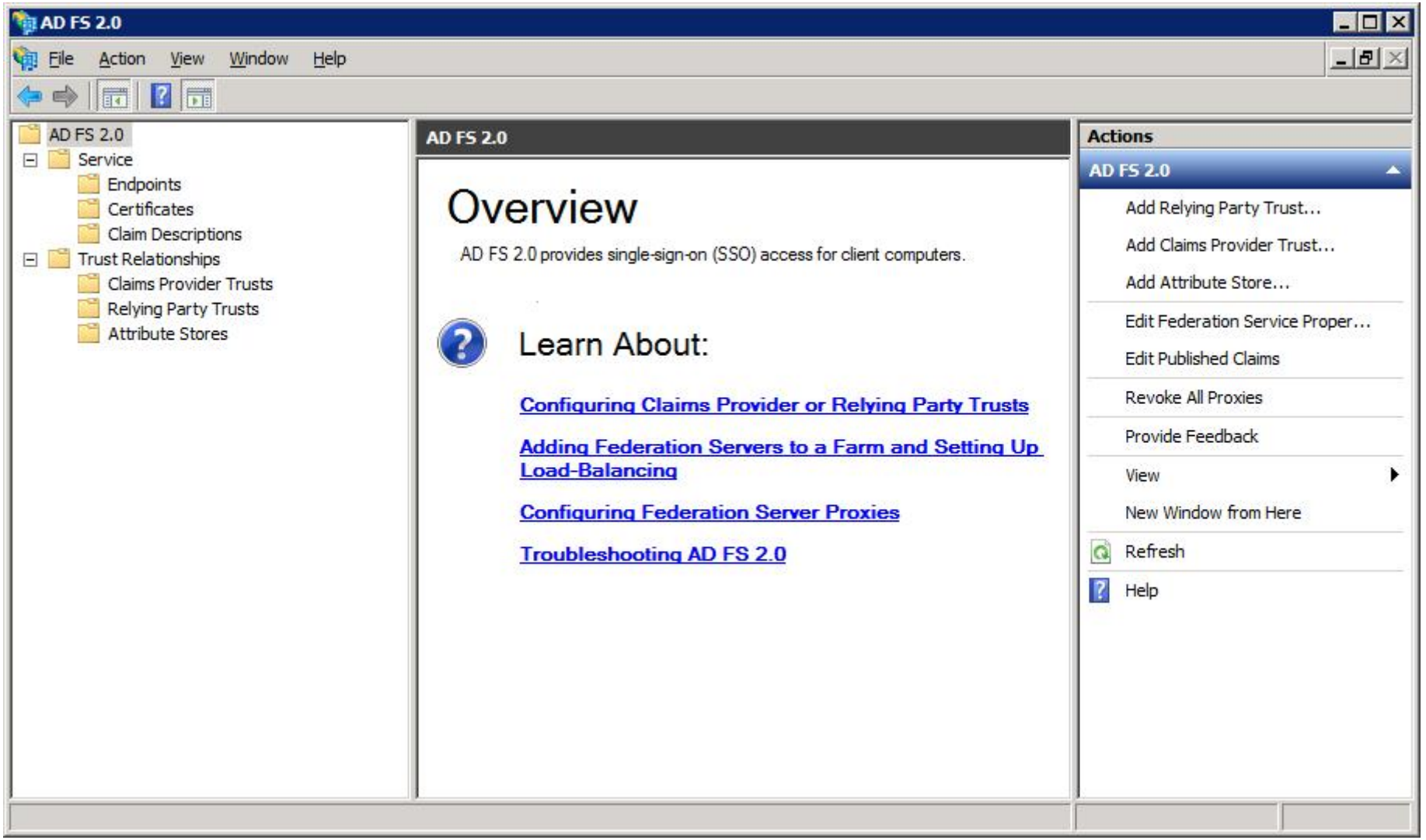
4: Configure the Issuer to Know about the Application

1: Add Logic to Your Applications to Support Claims .NET, Java and workflows

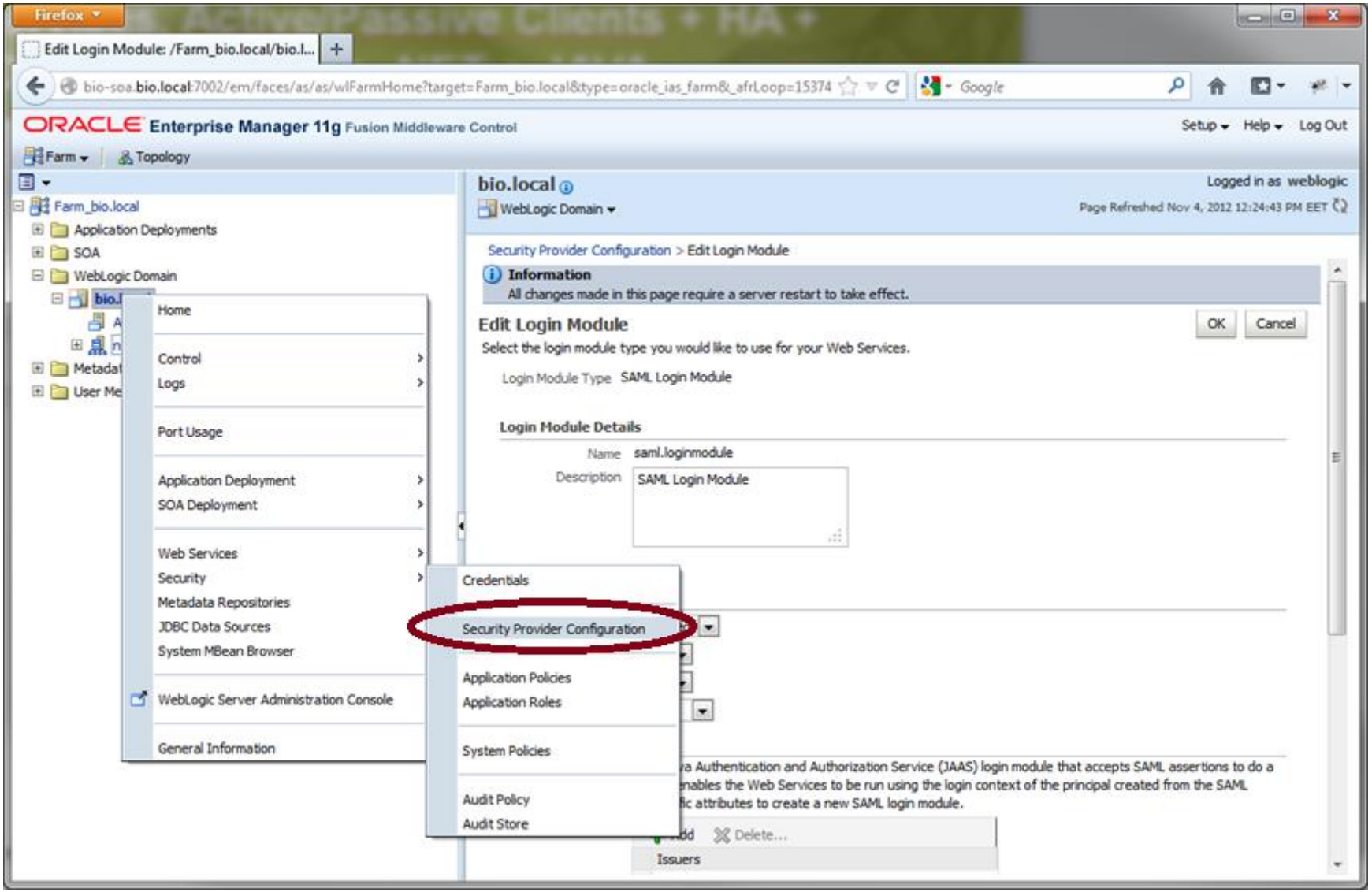
Loģikas implementēšana



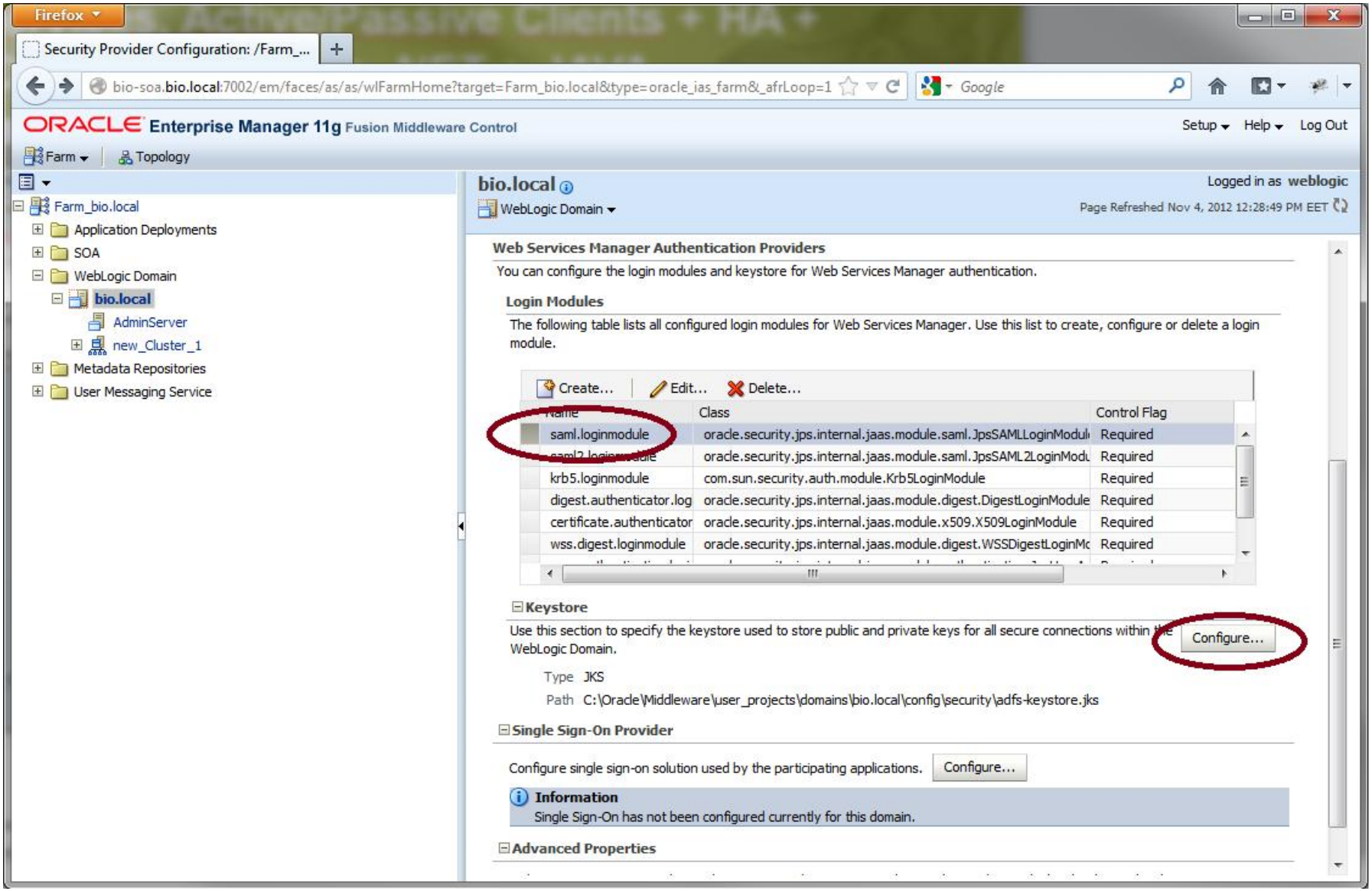
2: Acquire or Build an Issuer



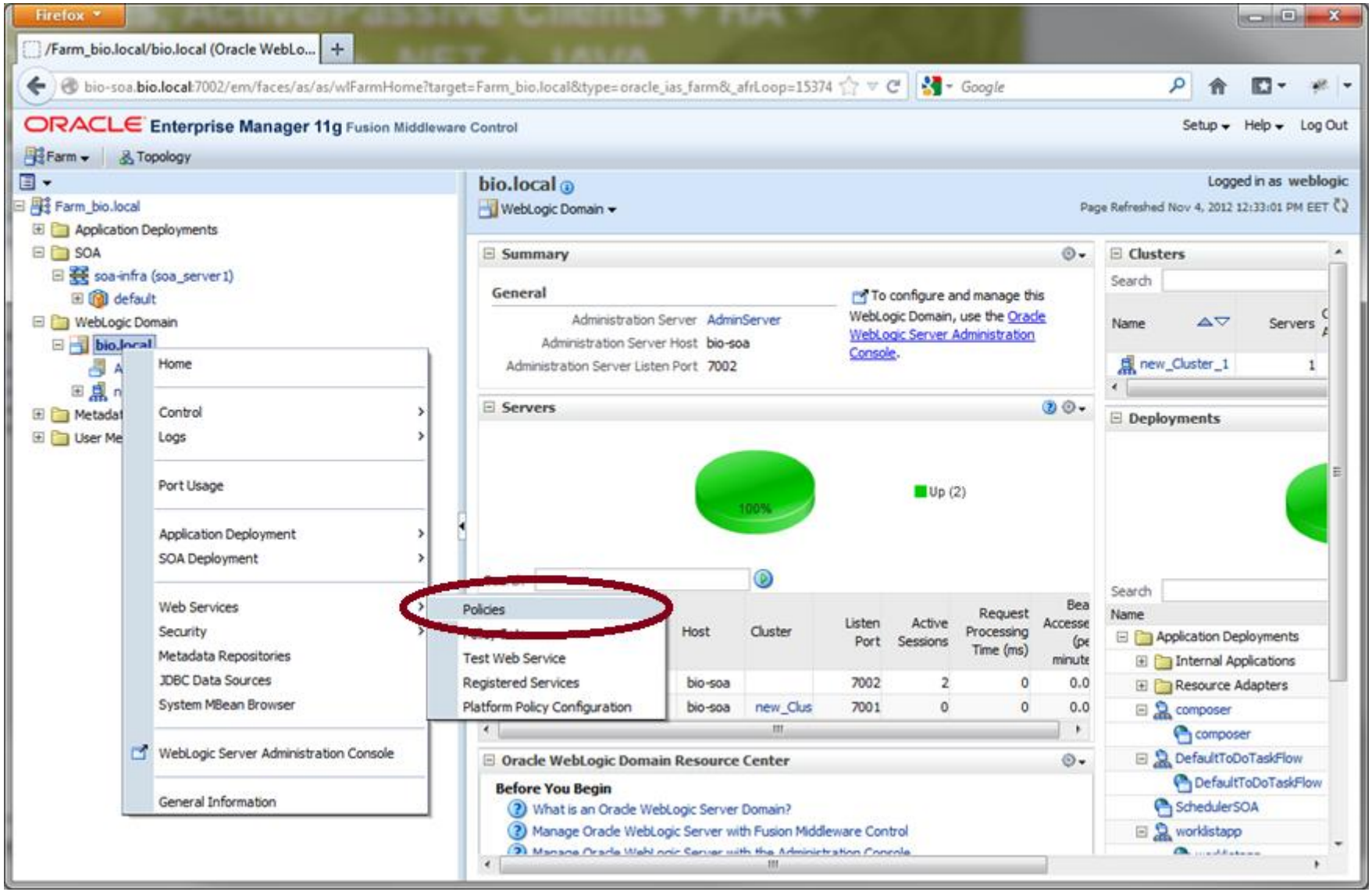
3: Configure Your Application to Trust the Issuer



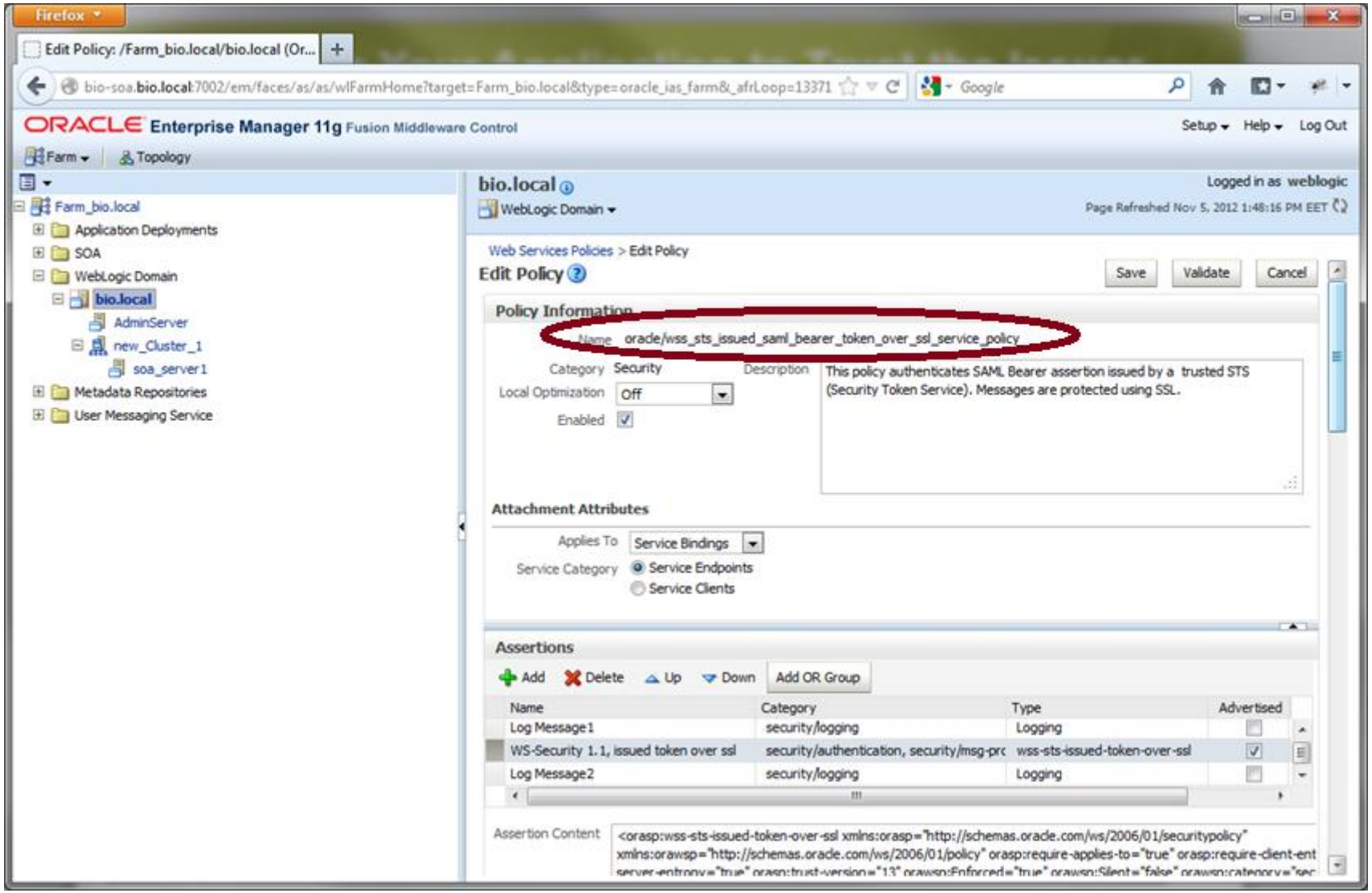
3: Configure Your Application to Trust the Issuer



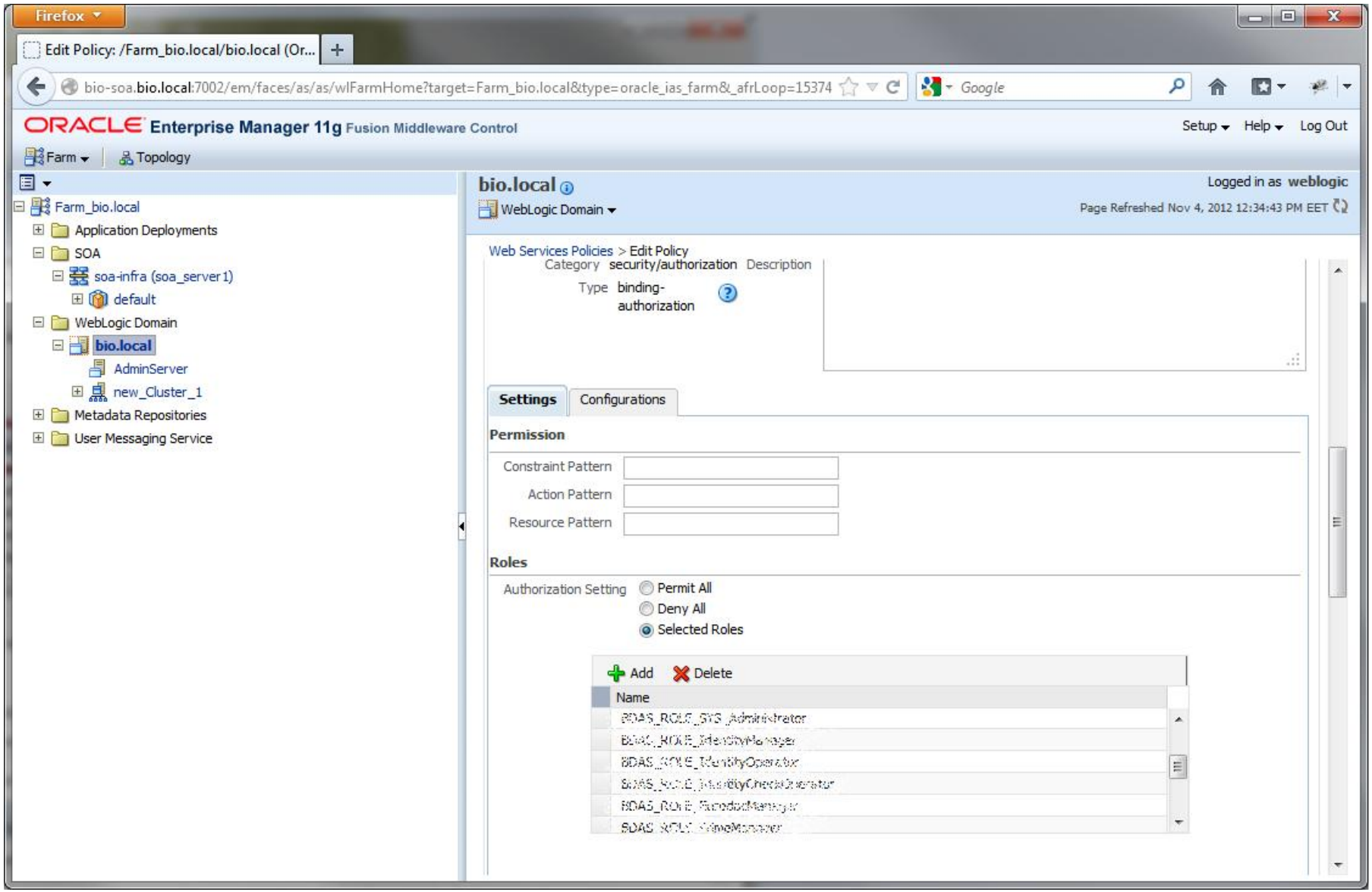
3: Configure Your Application to Trust the Issuer



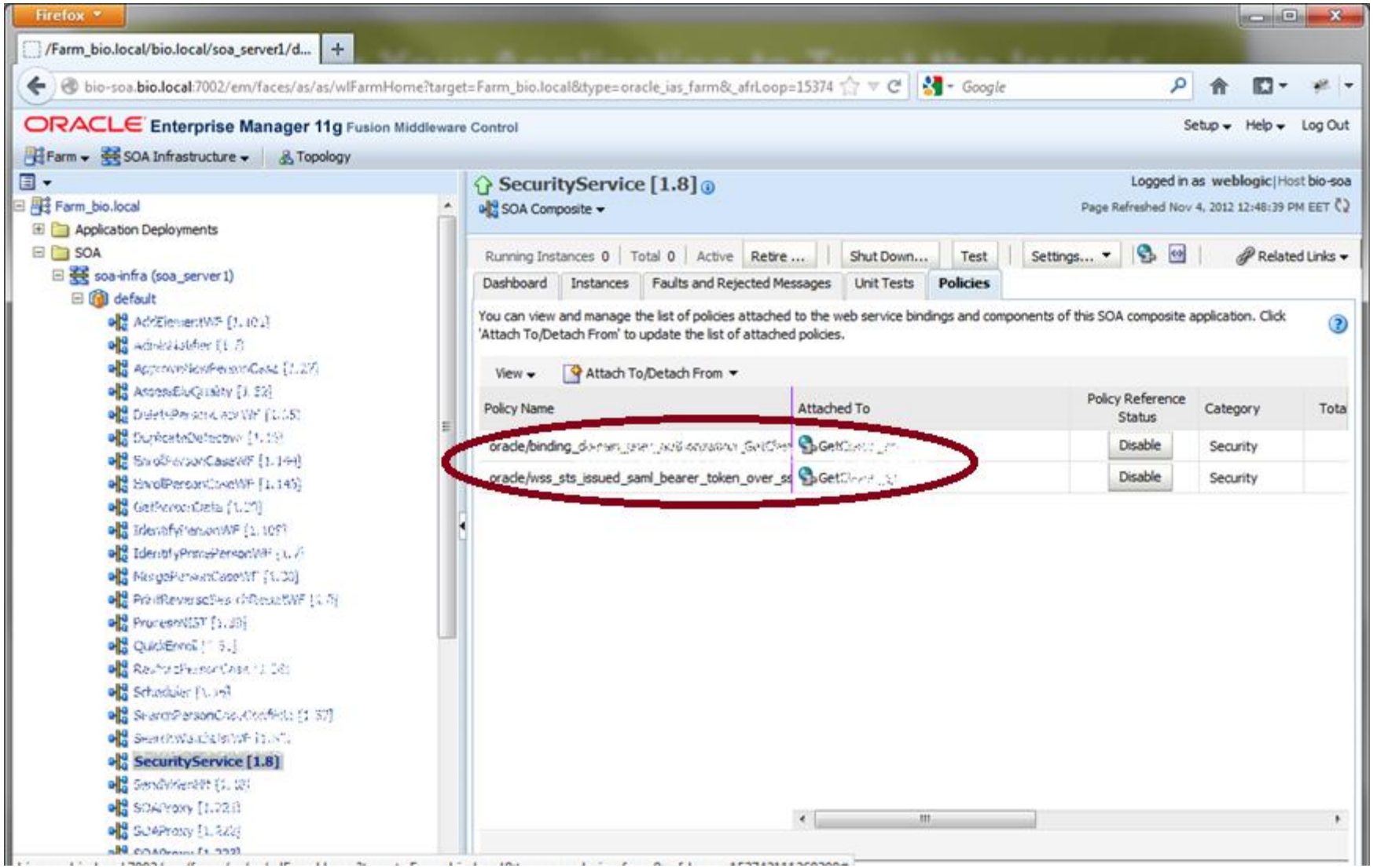
3: Configure Your Application to Trust the Issuer Authentication policy



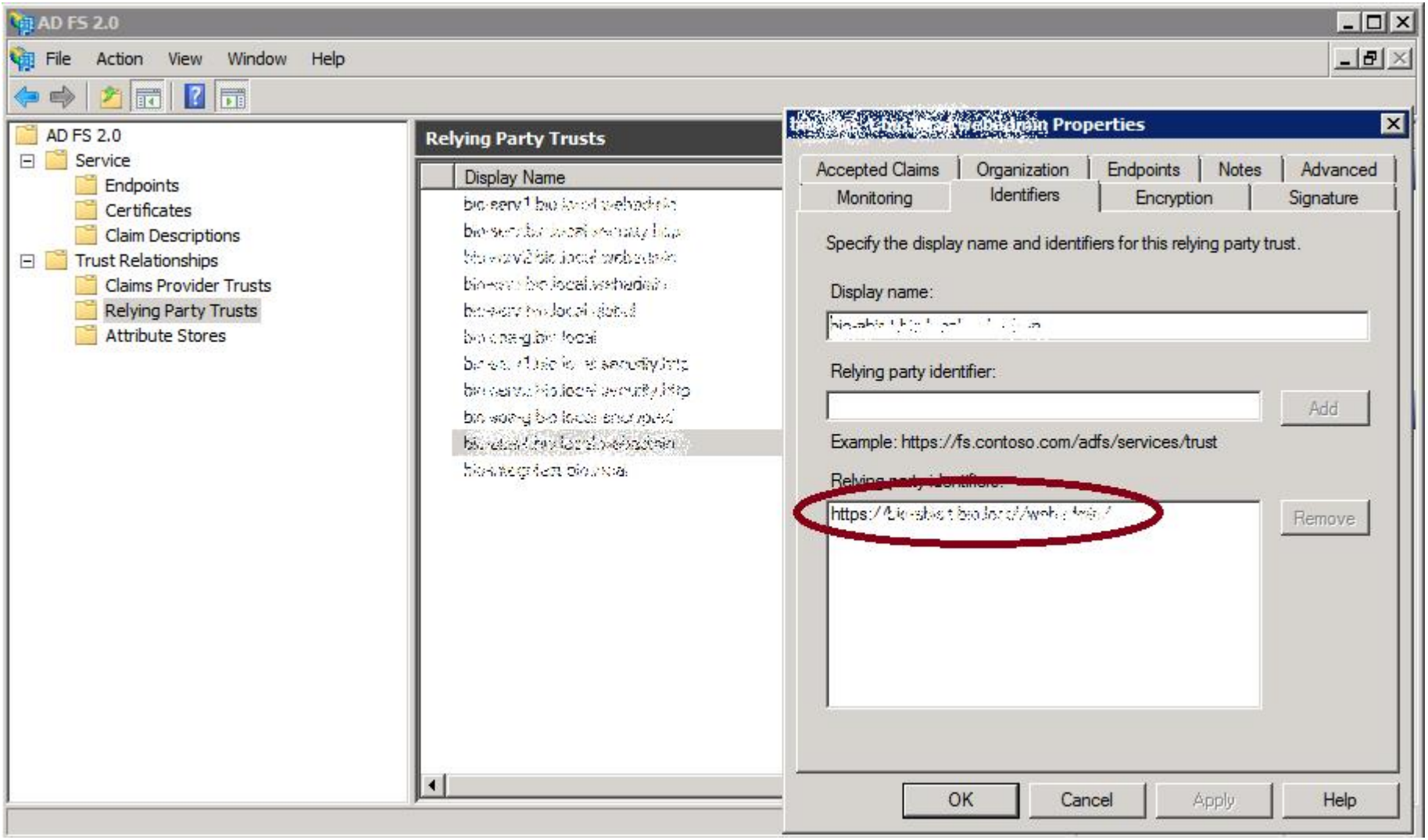
3: Configure Your Application to Trust the Issuer Authorization policy



3: Configure Your Application to Trust the Issuer
Attach policies



4: Configure the Issuer to Know about the Application



Secinājumi

Ātra un paralēli veicama izstrāde

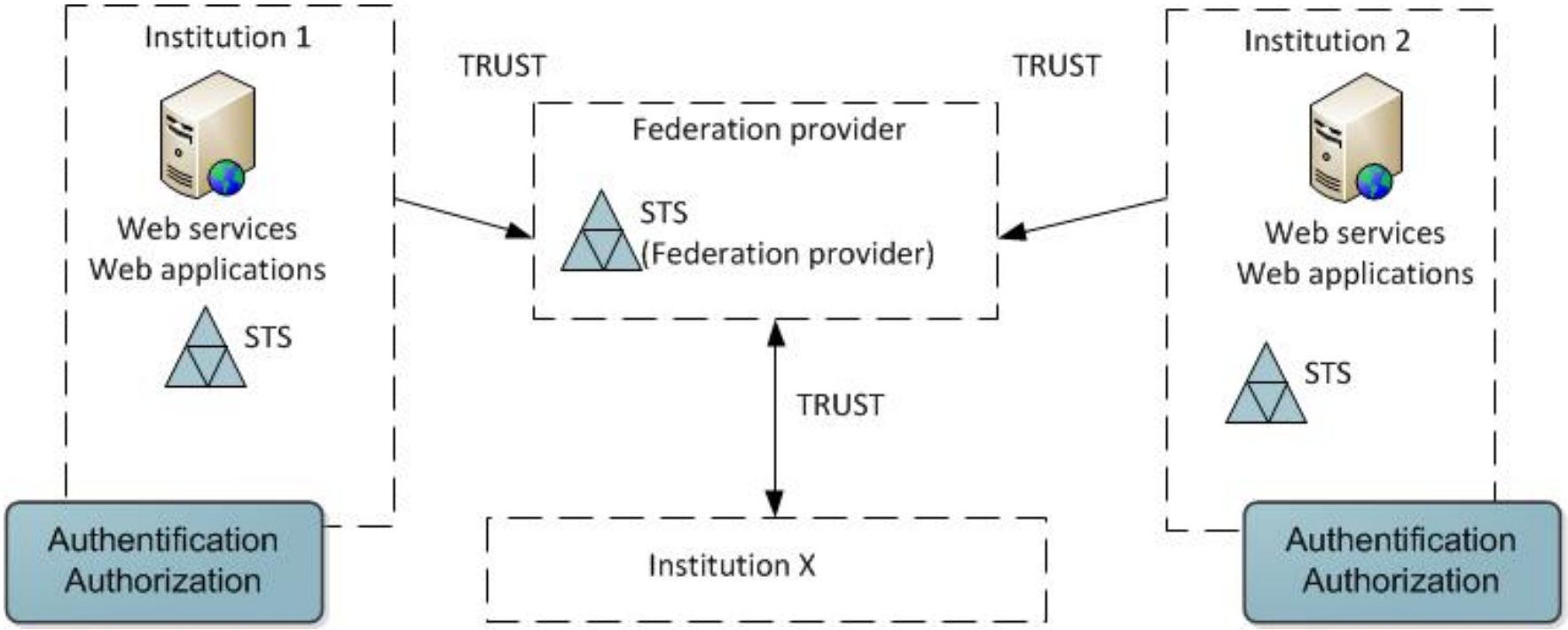
Augsts (konfigurējams) drošības līmenis

Izdēvējam (STS) ir jābūt augstas pieejamības

Platformu neatkarīgs risinājums

Federatīvās autentifikācija lielākā mērogā

Vīzija


Institution 1
Web services
Web applications
STS
Authentification
Authorization
TRUST
Federation provider
STS
(Federation provider)
TRUST
TRUST
Institution X
Institution 2
Web services
Web applications
STS
Authentification
Authorization

Kopsavilkums

Autentifikācijas nodalīšana no autorizācijas

Vispārpieņemtu standartu izmantošana

Ārējo lietotāju pārvaldība

Anonimitātes nodrošināšana

Netiek mainīti eksistējošie lietotāju autentifikācijas veidi

Paldies!

Twitter: https://twitter.com/dpa_latvia
Facebook: https://www.facebook.com/DPALatvia
Blog: http://blogs.dpa.lv/