



Federatīvās autentifikācijas priekšrocības un pielietojumi

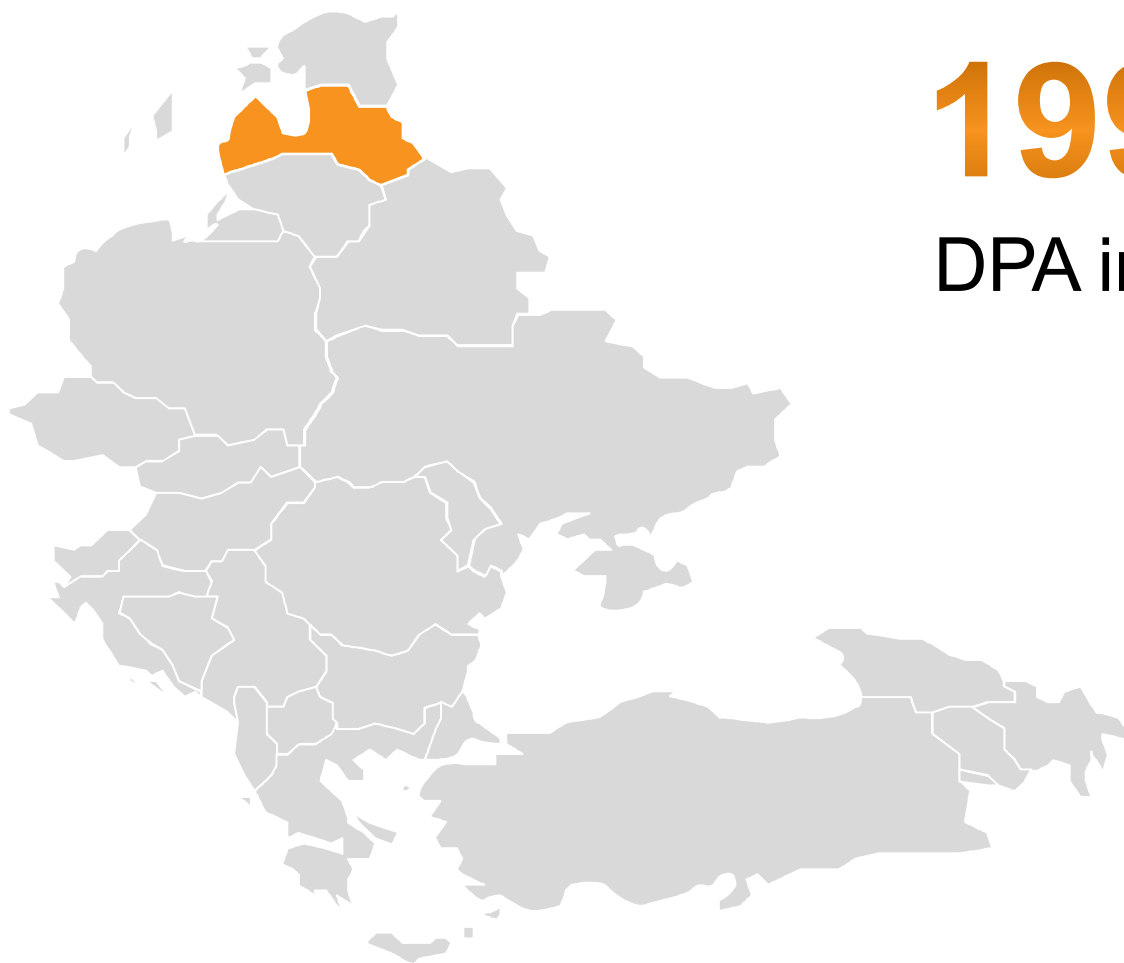
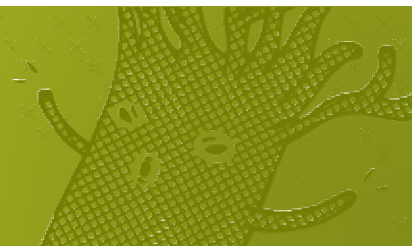
Latvijas piemēri un nākotnes vīzija.

Mārtiņš Orinskis, SIA DPA projektu vadītājs

2012.gada 8. novembris



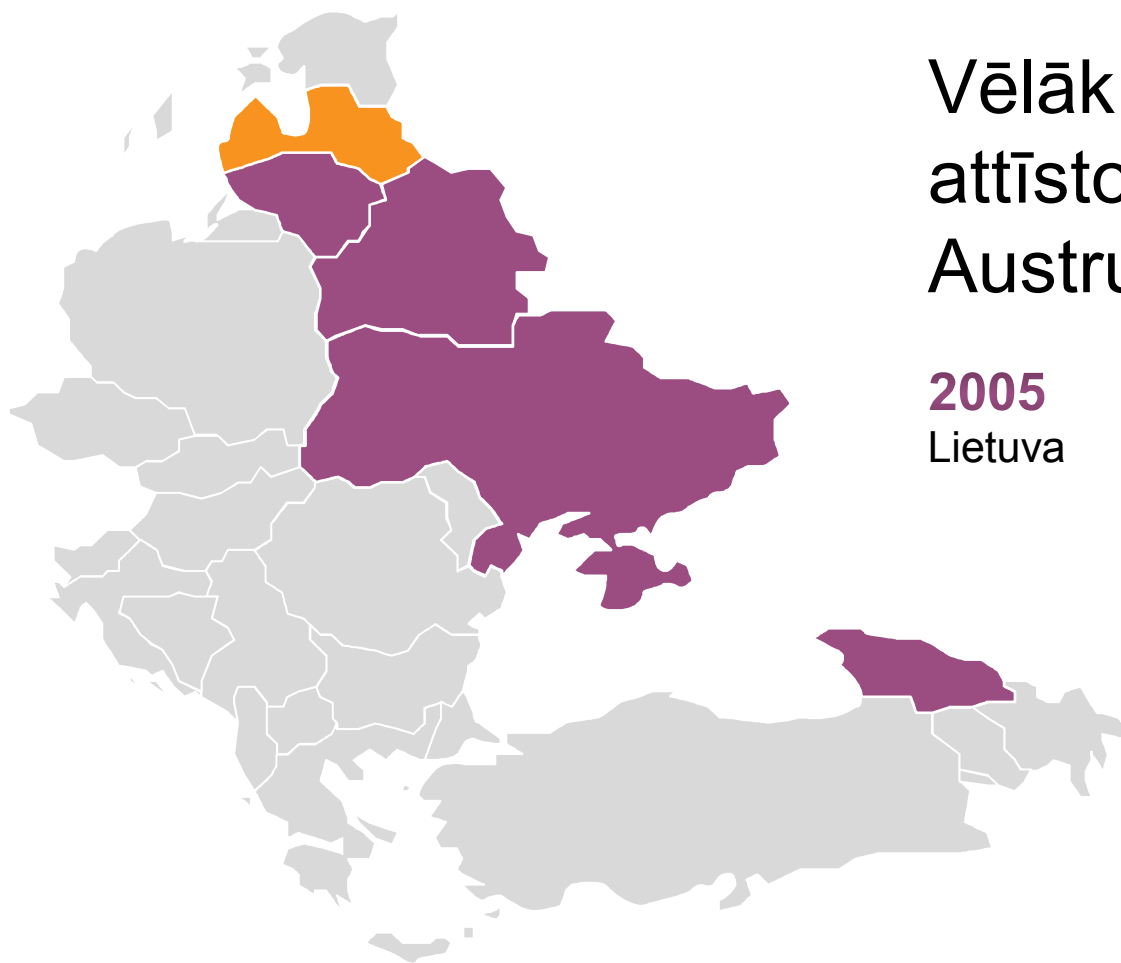
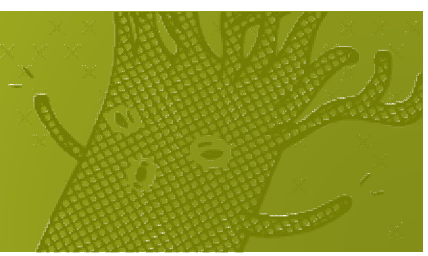
Mūsu stāsts



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

Bitte auf kurzfristigen Wechsel des Ausgangs achten
Please observe gate changes at short notice

220 230517 ECONOMY 074
etix etkt etix etkt Bordkarte/Boarding Pass

Lufthansa
A STAR ALLIANCE MEMBER
There's no better way to fly.

LUFTHANSA
ST [redacted] / IN [redacted] MRS
MUC LH 2140 T 10NOV
FMO
7B
LH 2140 /074

M

Name of passenger
ST [redacted] / IN [redacted] MRS
ETKT 220 230517
MUC
FMO
LUFTHANSA

Carrier Flight No./Class Date
LH 2140 T 10NOV

Gate Boarding time Seat
G31 2050 **7B**
NONSMOKER

OPERATED BY LUFTHANSA CITYLINE
MAX 1 HANDGEPÄCK/HANDBLUGGAGE

MUC 18403

Pcs Ck. Wt. Unck. Wt. Pcs. Ck. Wt. Unck. Wt.

Federatīvās autentifikācijas ieguvumi



Autentifikācijas nodalīšana no
autorizācijas

Vispārpieņemtņu standartu
izmantošana

Ārējo lietotāju pārvaldība

Anonimitātes nodrošināšana

Netiek mainīti eksistējošie
lietotāju autentifikācijas veidi



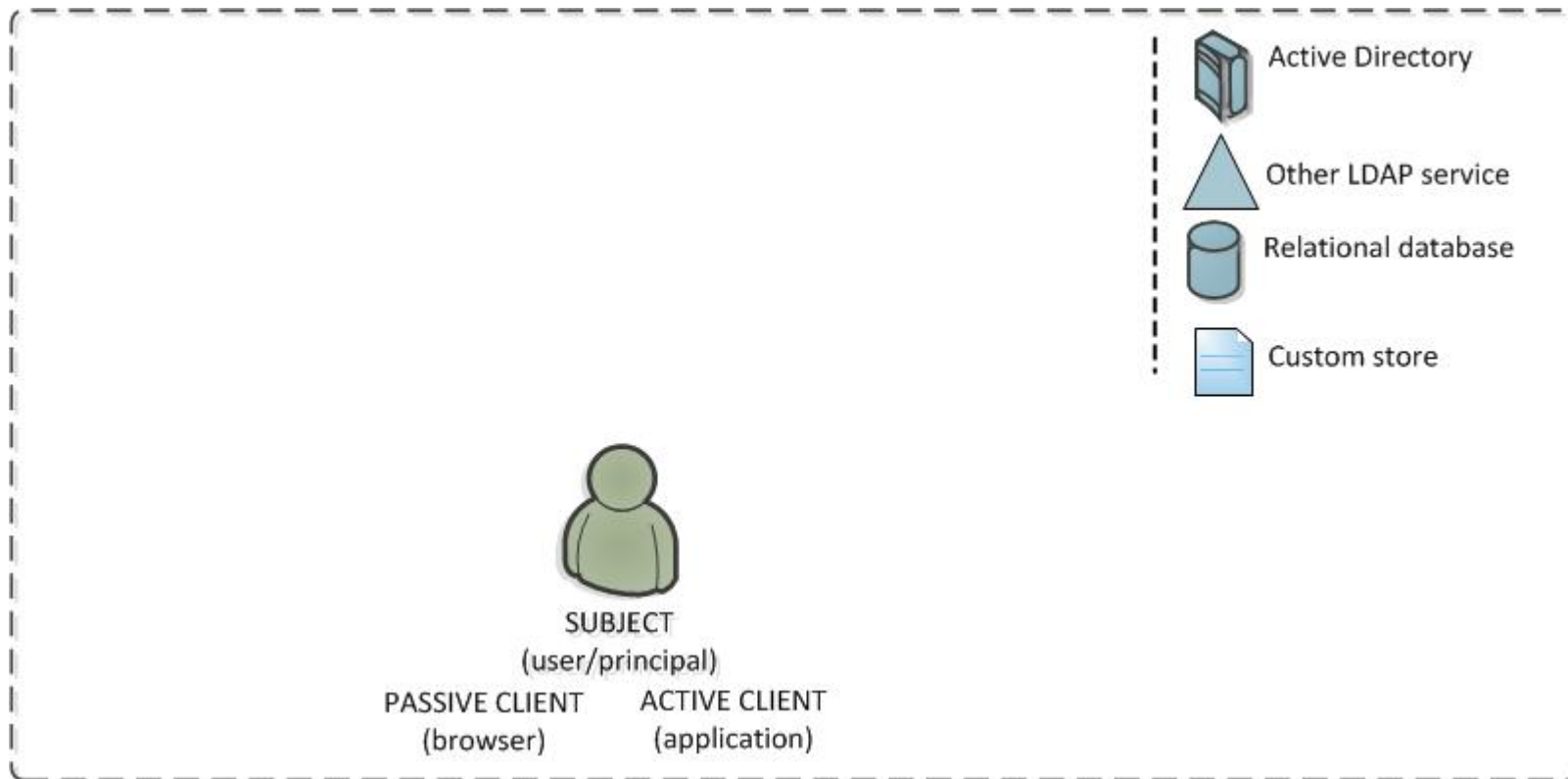
Pamatprincipi: OASIS standarti - WS*

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



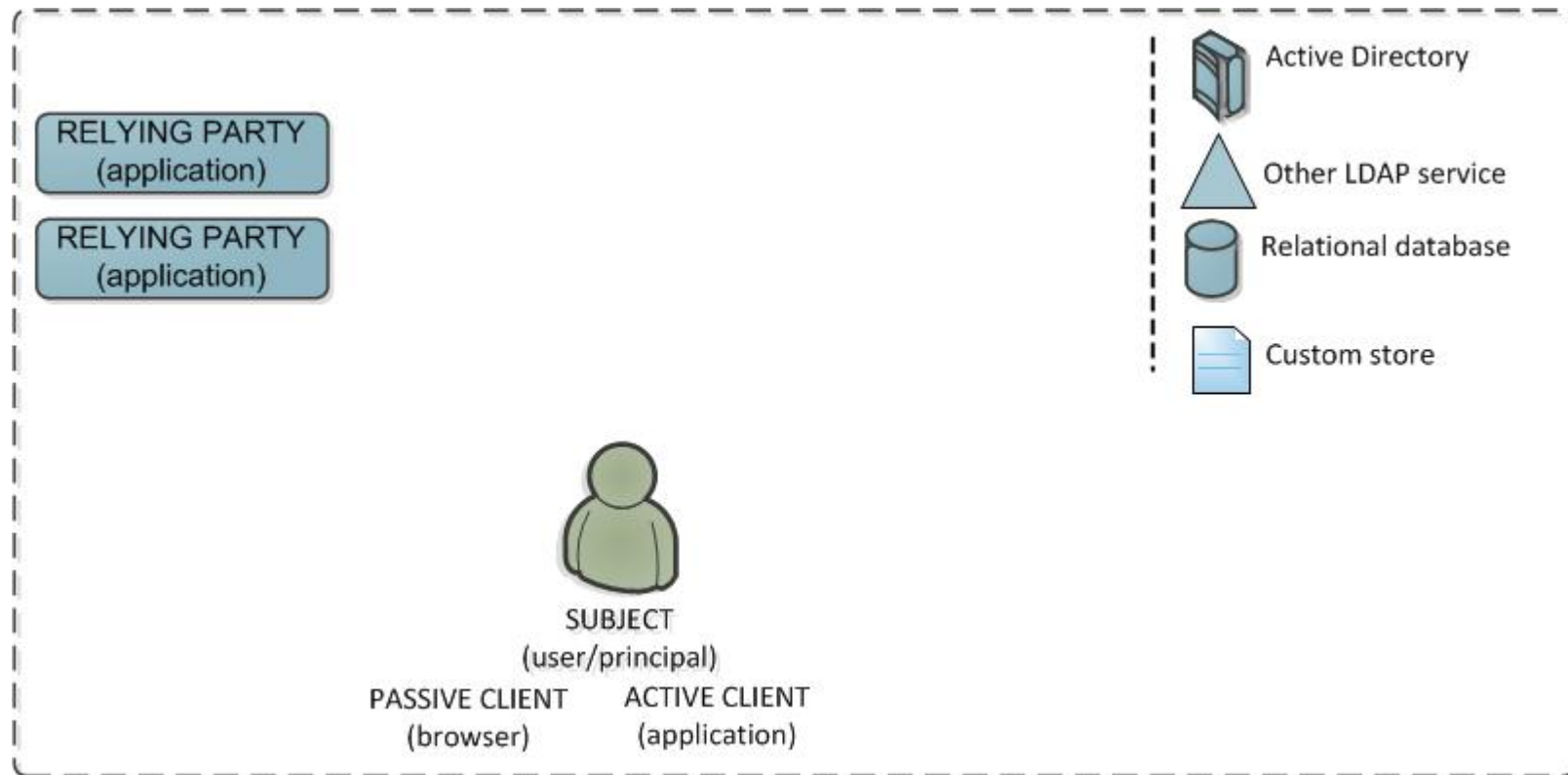
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



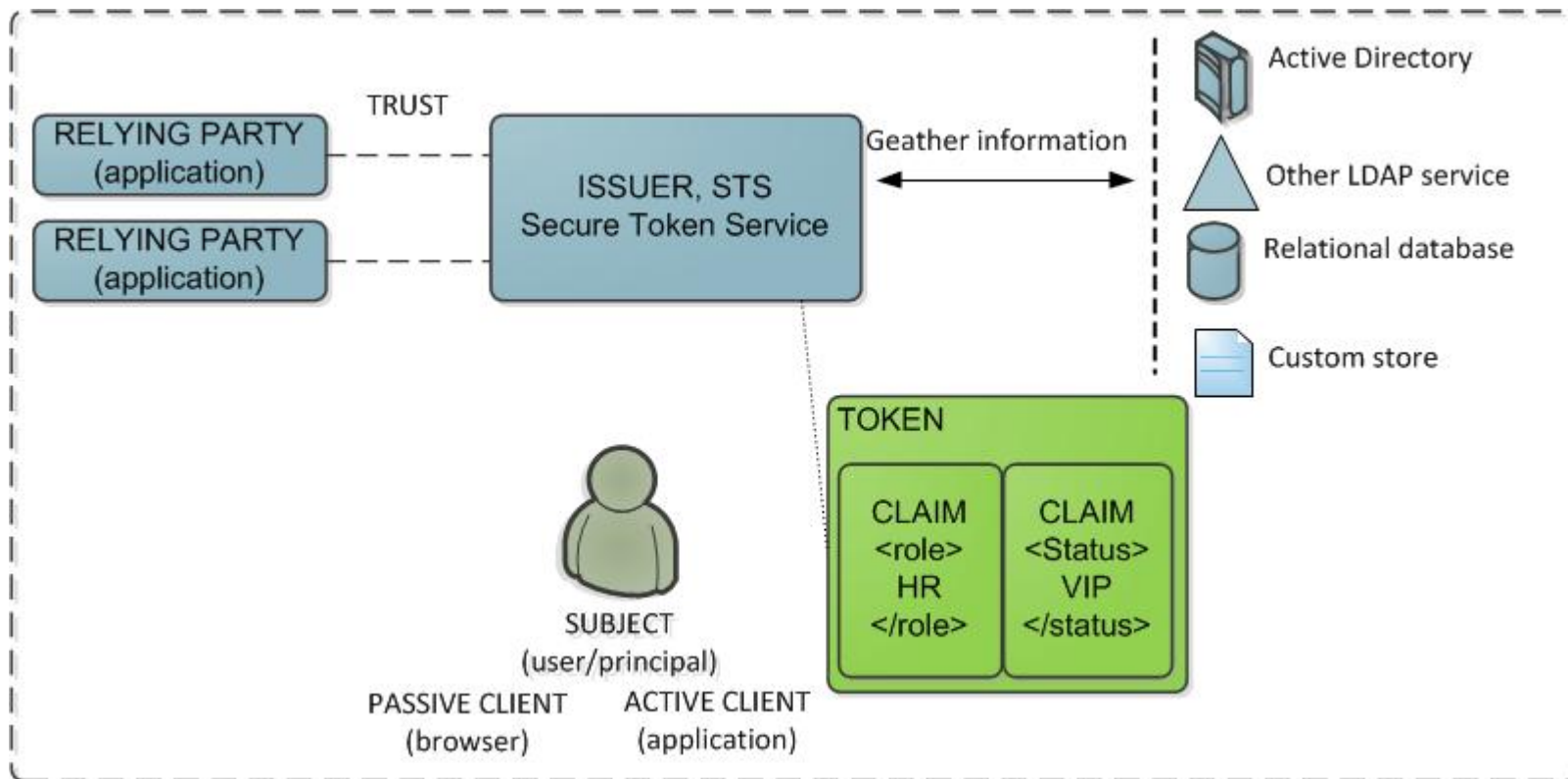
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



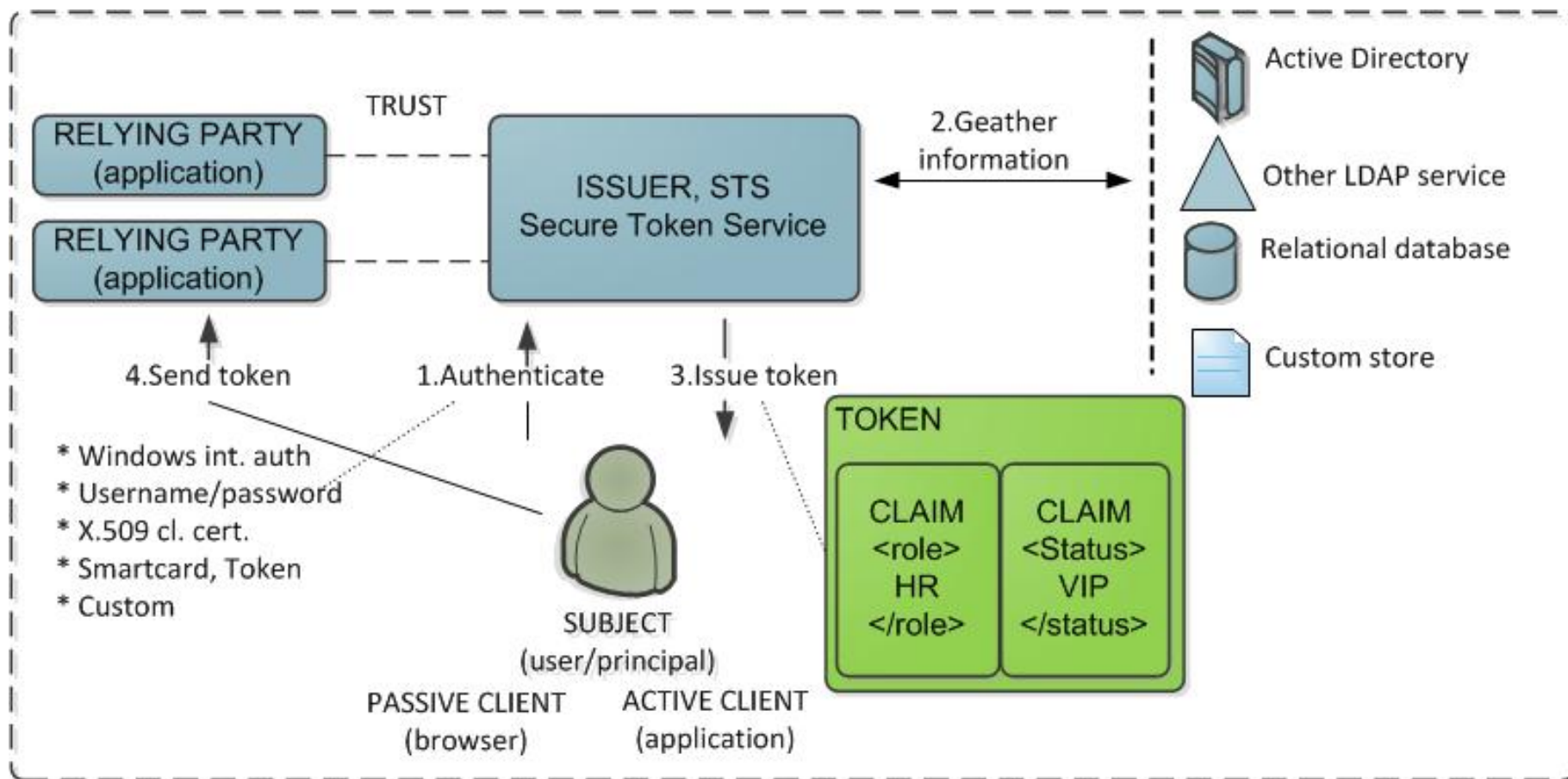
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



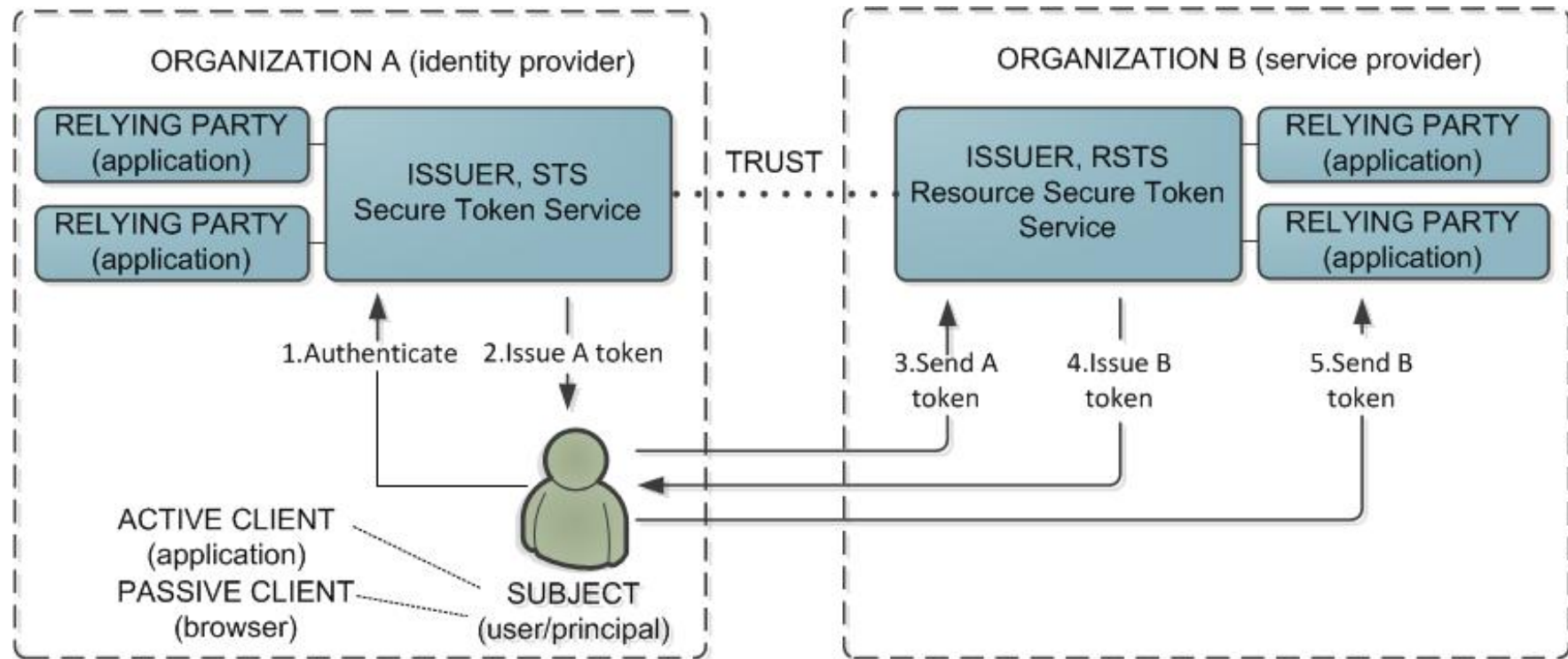
Federatīvās autentifikācijas pamatprincipi

Realm – darbības sfēra: Viena iestāde



Federatīvās autentifikācijas pamatprincipi

Realm – 2 darbības sfēras: Divas iestādes





Izmantošanas piemērs



Projekta uzdevumi



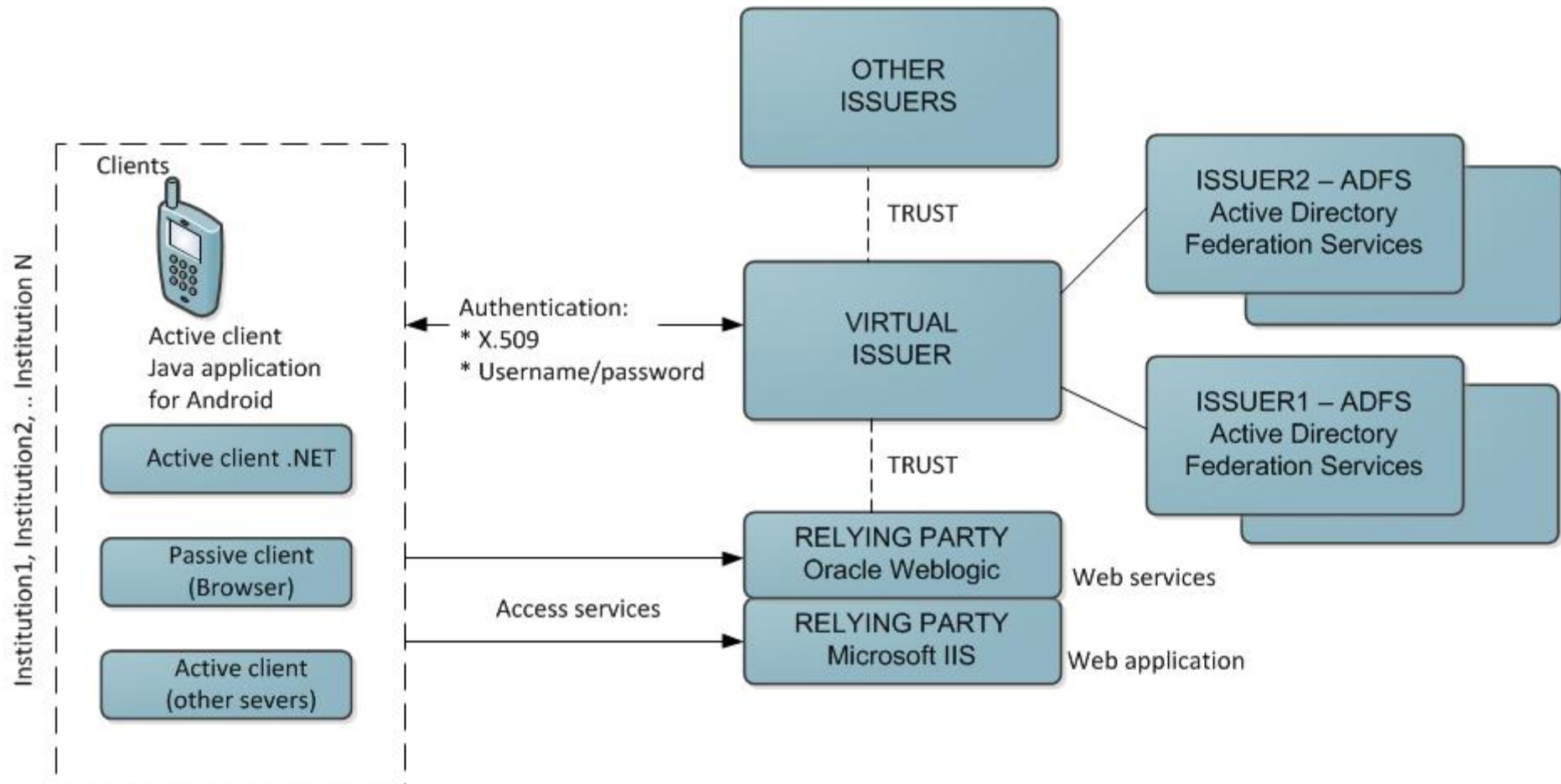
Web-service autentifikācija un
autorizācija

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

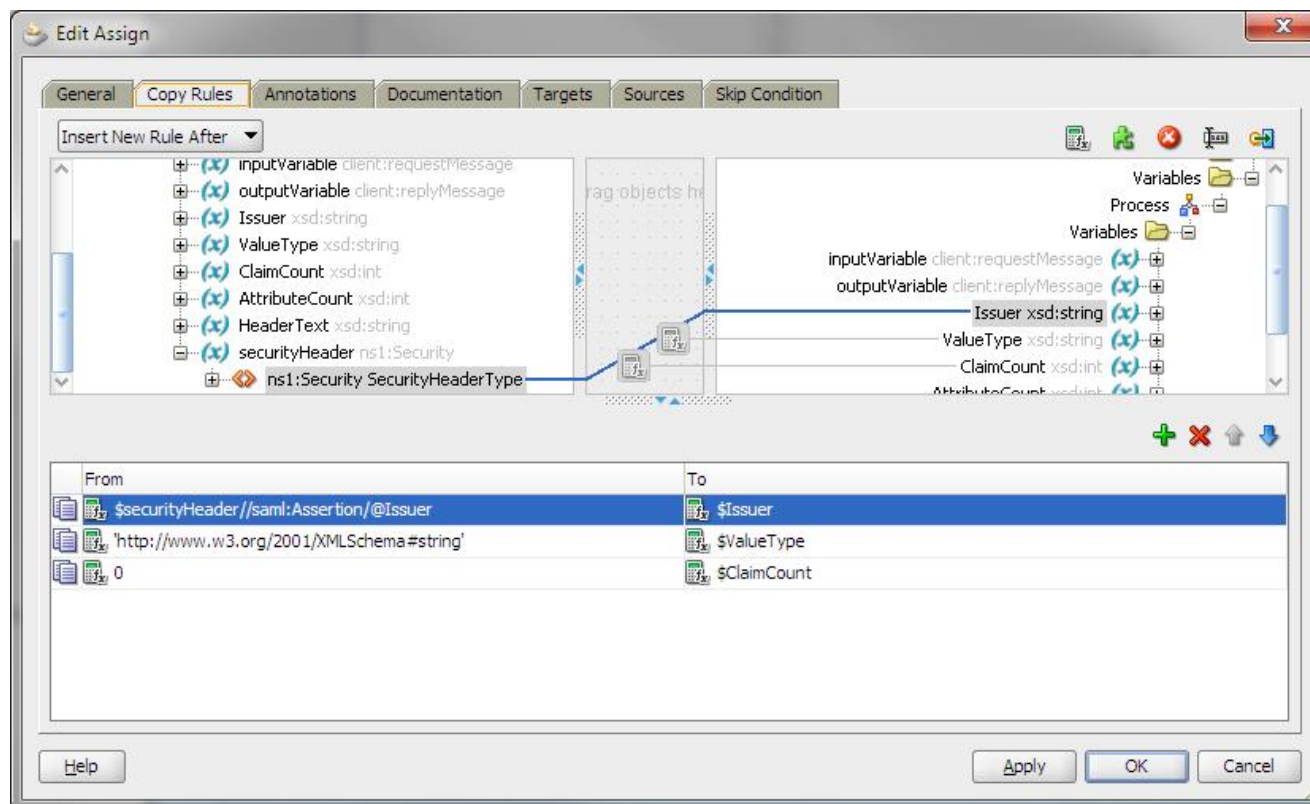
2: Acquire or Build an Issuer

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

The screenshot displays the AD FS 2.0 management console. The window title is "AD FS 2.0". The menu bar includes "File", "Action", "View", "Window", and "Help". The left-hand navigation pane shows a tree structure under "AD FS 2.0":

- AD FS 2.0
 - Service
 - Endpoints
 - Certificates
 - Claim Descriptions
 - Trust Relationships
 - Claims Provider Trusts
 - Relying Party Trusts
 - Attribute Stores

The main content area is titled "AD FS 2.0" and "Overview". It contains the following text:

AD FS 2.0 provides single-sign-on (SSO) access for client computers.

Learn About:

- [Configuring Claims Provider or Relying Party Trusts](#)
- [Adding Federation Servers to a Farm and Setting Up Load-Balancing](#)
- [Configuring Federation Server Proxies](#)
- [Troubleshooting AD FS 2.0](#)

The right-hand pane is titled "Actions" and lists the following options:

- AD FS 2.0
 - Add Relying Party Trust...
 - Add Claims Provider Trust...
 - Add Attribute Store...
 - Edit Federation Service Proper...
 - Edit Published Claims
 - Revoke All Proxies
 - Provide Feedback
 - View
 - New Window from Here
 - Refresh
 - Help

3: Configure Your Application to Trust the Issuer

The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The browser address bar shows the URL: `bio-soa.bio.local:7002/em/faces/as/es/wlFarmHome?target=Farm_bio.local&type=oracle_ias_farm&_afLoop=15374`. The page title is "ORACLE Enterprise Manager 11g Fusion Middleware Control". The user is logged in as "weblogic".

The main content area is titled "Edit Login Module" and includes an information banner: "All changes made in this page require a server restart to take effect." Below this, the "Login Module Type" is set to "SAML Login Module".

The "Login Module Details" section shows the following information:

Name	saml.loginmodule
Description	SAML Login Module

A context menu is open over the "Security Provider Configuration" link, with this option circled in red. The menu items include: Home, Control, Logs, Port Usage, Application Deployment, SOA Deployment, Web Services, Security, Metadata Repositories, JDBC Data Sources, System MBean Browser, WebLogic Server Administration Console, General Information, Credentials, Security Provider Configuration, Application Policies, Application Roles, System Policies, Audit Policy, and Audit Store.

3: Configure Your Application to Trust the Issuer

The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The browser address bar shows the URL: `bio-soa.bio.local:7002/em/faces/as/as/wlFarmHome?target=Farm_bio.local&type=oracle_ias_farm&_afLoop=1`. The page title is "ORACLE Enterprise Manager 11g Fusion Middleware Control".

The left-hand navigation pane shows the tree structure for the "Farm_bio.local" domain, including "Application Deployments", "SOA", "WebLogic Domain", "bio.local" (selected), "AdminServer", "new_Cluster_1", "Metadata Repositories", and "User Messaging Service".

The main content area is titled "bio.local" and "WebLogic Domain". It is logged in as "weblogic". The page was refreshed on Nov 4, 2012 12:28:49 PM EET.

The "Web Services Manager Authentication Providers" section is active. It contains the following sections:

- Login Modules:** A table listing configured login modules. The "saml.loginmodule" row is highlighted with a red circle.
- Keystore:** A section for specifying the keystore. The "Configure..." button is highlighted with a red circle.
- Single Sign-On Provider:** A section for configuring single sign-on solutions.
- Information:** A message stating "Single Sign-On has not been configured currently for this domain."
- Advanced Properties:** A section for advanced configuration options.

Name	Class	Control Flag
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	Required
saml2.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAML2LoginModule	Required
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	Required
digest.authenticator.log	oracle.security.jps.internal.jaas.module.digest.DigestLoginModule	Required
certificate.authenticator	oracle.security.jps.internal.jaas.module.x509.X509LoginModule	Required
wss.digest.loginmodule	oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginModule	Required

3: Configure Your Application to Trust the Issuer

The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The browser address bar shows the URL: `bio-soa.bio.local:7002/em/faces/as/as/wlFarmHome?target=Farm_bio.local&type=oracle_ias_farm&_afLoop=15374`. The page title is "ORACLE Enterprise Manager 11g Fusion Middleware Control". The user is logged in as "weblogic".

The main content area shows the configuration for the "bio.local" WebLogic Domain. The "Summary" section includes the following information:

- Administration Server: AdminServer
- Administration Server Host: bio-soa
- Administration Server Listen Port: 7002

The "Servers" section shows a 100% availability status with "Up (2)" servers. A table below lists the servers:

Host	Cluster	Listen Port	Active Sessions	Request Processing Time (ms)	Bea Accesses (per minute)
bio-soa		7002	2	0	0.0
bio-soa	new_Clus	7001	0	0	0.0

The "Policies" menu item is circled in red. The "Oracle WebLogic Domain Resource Center" section includes a "Before You Begin" section with links to help topics.

3: Configure Your Application to Trust the Issuer Authentication policy

The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The left-hand navigation pane shows a tree structure with 'Farm_bio.local' selected, containing sub-items like 'Application Deployments', 'SOA', 'WebLogic Domain', and 'bio.local'. The main content area is titled 'Edit Policy' and shows the configuration for a policy named 'orade/wss_sts_issued_saml_bearer_token_over_ssl_service_policy'. This name is circled in red. The policy is categorized under 'Security' and is currently enabled. The description states: 'This policy authenticates SAML Bearer assertion issued by a trusted STS (Security Token Service). Messages are protected using SSL.' Below the policy information, the 'Attachment Attributes' section shows 'Applies To' set to 'Service Bindings' and 'Service Category' set to 'Service Endpoints'. The 'Assertions' section contains a table with the following data:

Name	Category	Type	Advised
Log Message1	security/logging	Logging	<input type="checkbox"/>
WS-Security 1.1, issued token over ssl	security/authentication, security/msg-prot	wss-sts-issued-token-over-ssl	<input checked="" type="checkbox"/>
Log Message2	security/logging	Logging	<input type="checkbox"/>

At the bottom, the 'Assertion Content' field shows the following XML snippet:

```
<orasp:wss-sts-issued-token-over-ssl xmlns:orasp="http://schemas.oracle.com/ws/2006/01/securitypolicy"
xmlns:orawsp="http://schemas.oracle.com/ws/2006/01/policy" orasp:require-uses-to="true" orasp:require-client-end
server-entrancy="true" orasp:trust-version="1.3" orasp:Enforced="true" orasp:Silent="false" orasp:category="sec
```


3: Configure Your Application to Trust the Issuer Authorization policy

The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The browser address bar shows the URL: `bio-soa.bio.local:7002/em/faces/as/as/wlFarmHome?target=Farm_bio.local&type=oracle_ias_farm&afrLoop=15374`. The page title is "ORACLE Enterprise Manager 11g Fusion Middleware Control". The user is logged in as "weblogic".

The left-hand navigation pane shows a tree view of the environment:

- Farm_bio.local
 - Application Deployments
 - SOA
 - soa-infra (soa_server1)
 - default
 - WebLogic Domain
 - bio.local**
 - AdminServer
 - new_Cluster_1
 - Metadata Repositories
 - User Messaging Service

The main content area is titled "bio.local" and "WebLogic Domain". It shows the configuration for a policy:

Web Services Policies > Edit Policy
Category security/authorization Description
Type binding-authorization

There are two tabs: "Settings" (selected) and "Configurations".

Permission

Constraint Pattern:
Action Pattern:
Resource Pattern:

Roles

Authorization Setting: Permit All, Deny All, Selected Roles

Below the roles section, there are "Add" and "Delete" buttons, followed by a table of roles:

Name
BDAS_ROLE_SVS_Administrator
BDAS_ROLE_IntegrityManager
BDAS_ROLE_IntegrityOperator
BDAS_ROLE_IntegrityCheckOperator
BDAS_ROLE_MetadataManager
BDAS_ROLE_SlaveManager

3: Configure Your Application to Trust the Issuer

Attach policies

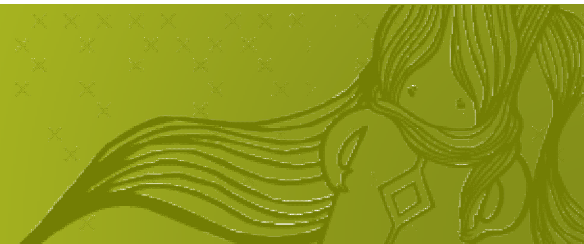
Running Instances 0 | Total 0 | Active | Retire ... | Shut Down... | Test | Settings... | Related Links

Dashboard | Instances | Faults and Rejected Messages | Unit Tests | **Policies**

You can view and manage the list of policies attached to the web service bindings and components of this SOA composite application. Click 'Attach To/Detach From' to update the list of attached policies.

Policy Name	Attached To	Policy Reference Status	Category	Total
oracle/binding_domen...	GetClient...	Disable	Security	
oracle/wss_sts_issued_saml_bearer_token_over...	GetClient...	Disable	Security	

Secinājumi



Ātra un paralēli veicama
izstrāde

Augsts (konfigurējams)
drošības līmenis

Izdēvējam (STS) ir jābūt
augstas pieejamības

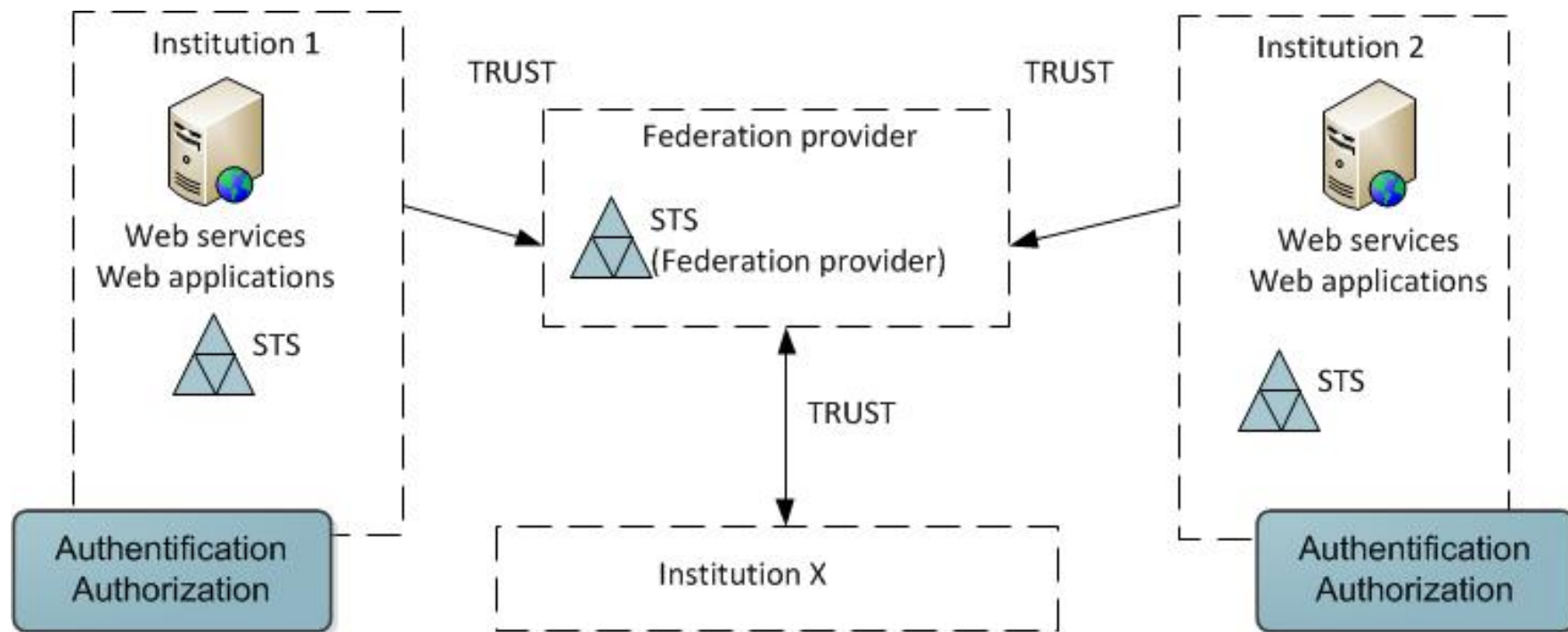
Platformu neatkarīgs risinājums



Federatīvās autentifikācija lielākā mērogā



Vīzija



Kopsavilkums

Autentifikācijas nodalīšana no
autorizācijas

Vispārpieņemtus standartus
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/>

