Demystifying Single Sign-On for Web Applications

Heesun Park, PhD
SAS Institute, Inc

SSTC 2011
May 2011, Salt Lake City, USA

Table of Contents

- Source of Authentication
- Web Application Protection Mechanism
- JAAS and SSO (Trust Relationships)
- Scopes of SSO
  - -- Web Application (Portal) based SSO
  - -- Application Server based SSO
  - -- 3rd Party Security Package based SSO
  - -- Integrated Windows Authentication (IWA)
  - -- SAML based SSO **

Source of Authentication

- Multiple “authentication points”:
  -- Windows login
  -- Web space
  -- Application server
  -- Web application
- Potentially multiple number of user registries
- Multiple web applications that share same authentication method
- Single Sign-On (SSO) means “initial” successful authentication will be honored by the rest of the authentication challenge / mechanism.

Web Application Protection Mechanism

- Authentication and Authorization
- Do it on your own or delegate authentication responsibility to other party such as application server.
- Use Deployment Descriptor (web.xml) – authentication and security role mapping
- JAAS (Java Authentication and Authorization Service) - Separation of authentication from web application functionality itself. More importantly, it makes web applications “portable”.

Deployment Descriptor (web.xml)

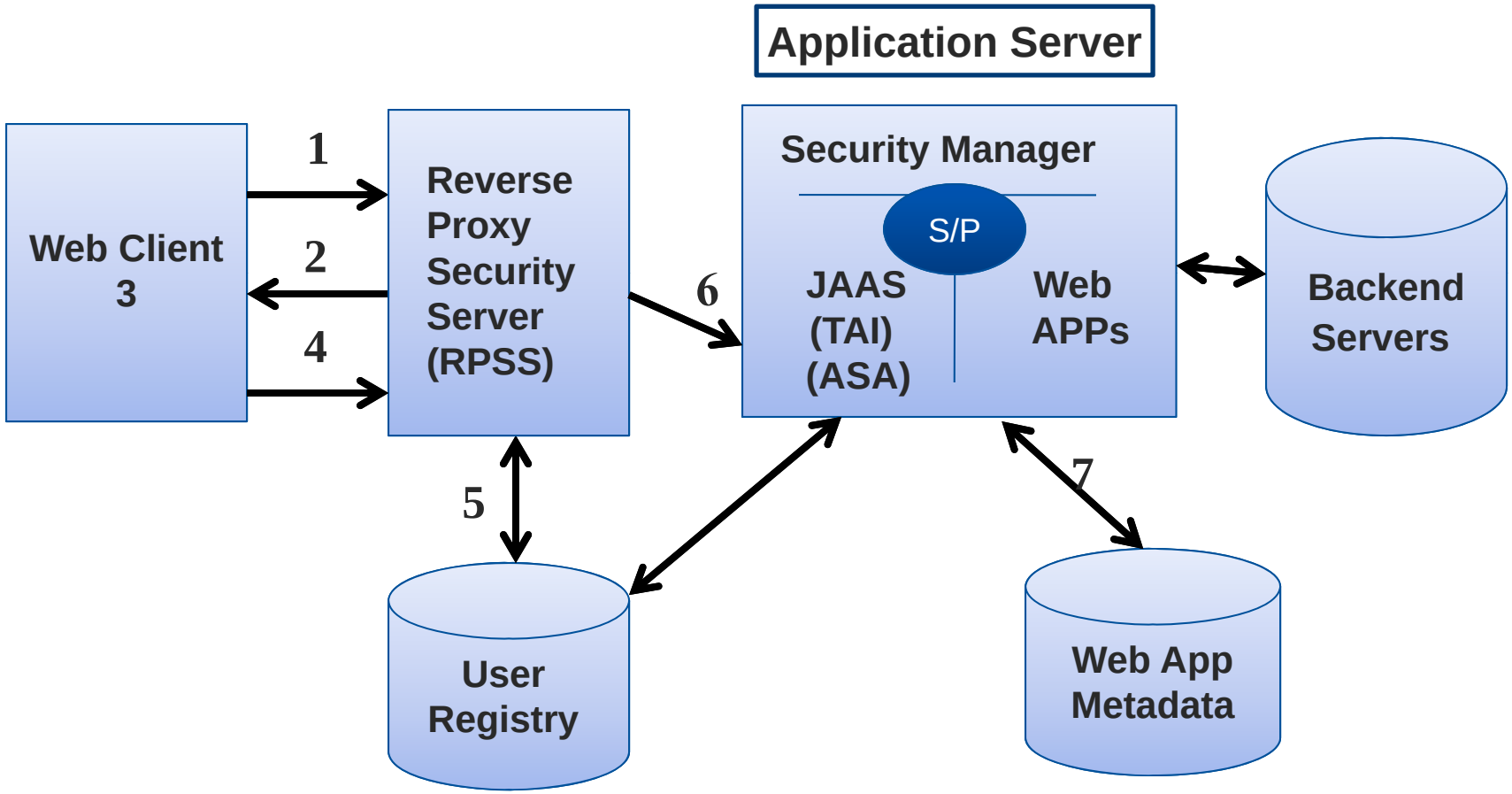
```
<security-constraint>
      <web-resource-collection>
          <web-resource-name>My Web App</web-resource-name>
          <url-pattern>/*</url-pattern>
     </web-resource-collection>
    <auth-constraint>
          <role-name>FinanceRole</role-name>
    </auth-constraint>
</security-constraint>

<login-config>
 <auth-method>CLIENT_CERT</auth-method>
 <realm-name>My Realm</realm-name>
</login-config>
```

JAAS and SSO

- JAAS in essence is a Java based implementation of pluggable authentication module(PAM), and in its simplest form, is an abstraction over authentication module providers.
- JAAS consists of a stack of JAAS login modules that handle different types of authentication methods.
- System login module / Application login module
- Subject / Principals
- Trust relationships makes SSO possible
- Interceptor / identity Asserter / Application Server Agent (ASA) – special case of JAAS login module

Typical JAAS Authentication Process



Authentication Sequence

1) User requests for Web application access

2) RPSS issues authentication challenge **

3) Browser prompts user for credentials

4) User provides credentials

5) RPSS authenticates the user and creates user token

6) TAI/IA decodes the token and creates JAAS Subject and add Principals in the Subject

7) Optionally, web application validates the authenticated user in the Subject against its own metadata

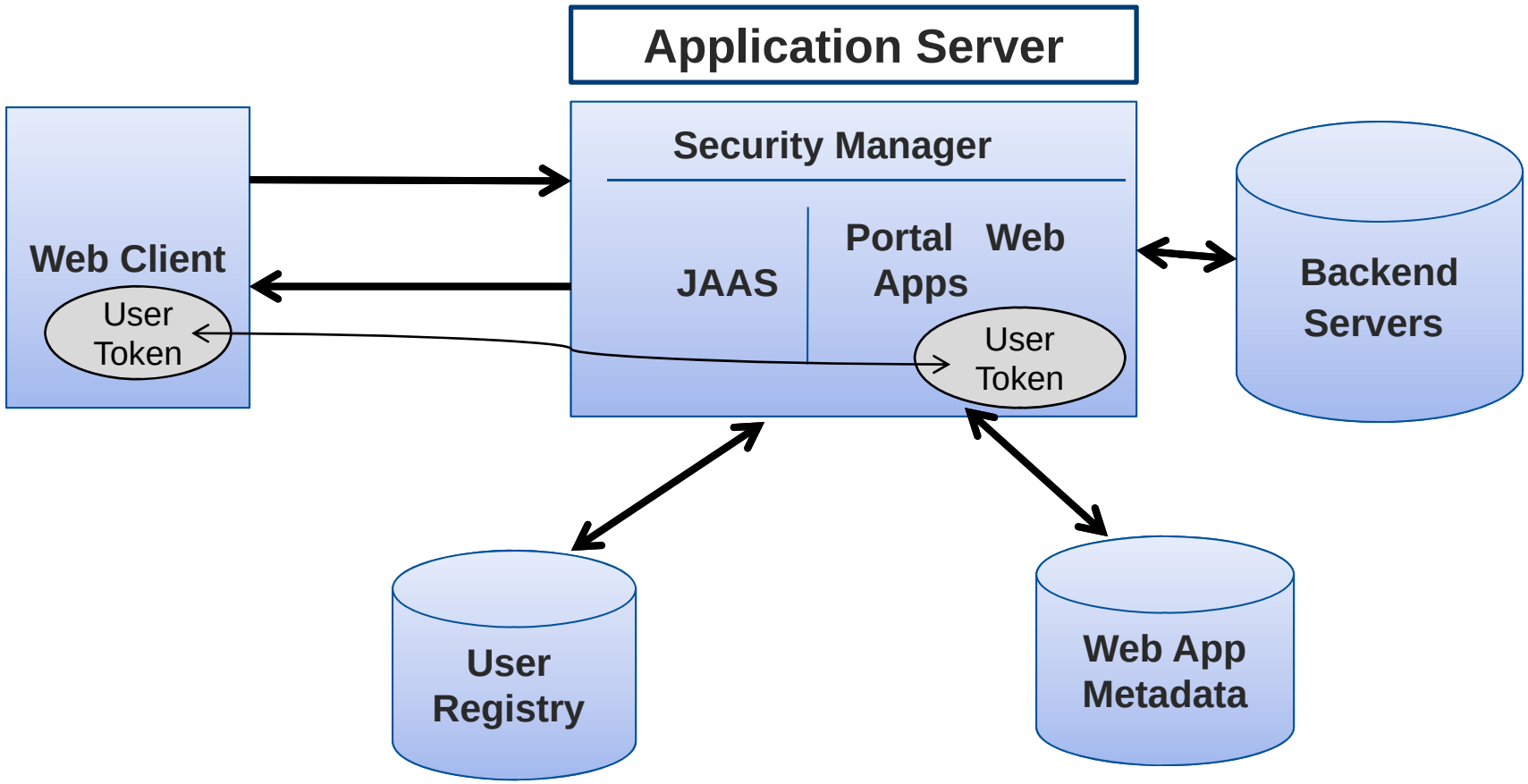
Security and Trust Relationship

- Protection of user credential – BASIC authentication is not safe
- At minimum, HTTPS (1-way SSL) is recommended. Client certificate based authentication (2-way SSL) is safer and is preferred.
- The main trust relationship is between RPSS and application server. After initial authentication, the RPSS encrypts the user credential into a security token. Only the special JAAS login module such as “interceptor” or “agent” can decode the security token and initialize JAAS Subject.
- Typically, SSO is more secure than multiple authentication.

Scopes of SSO

- (Based on initial authentication point)
- Portal Web Application based SSO
- Application Server based SSO
- 3rd Party Security Package (RPSS) based SSO
- Integrated Windows Authentication (Windows Domain login based SSO)
- SAML based SSO **

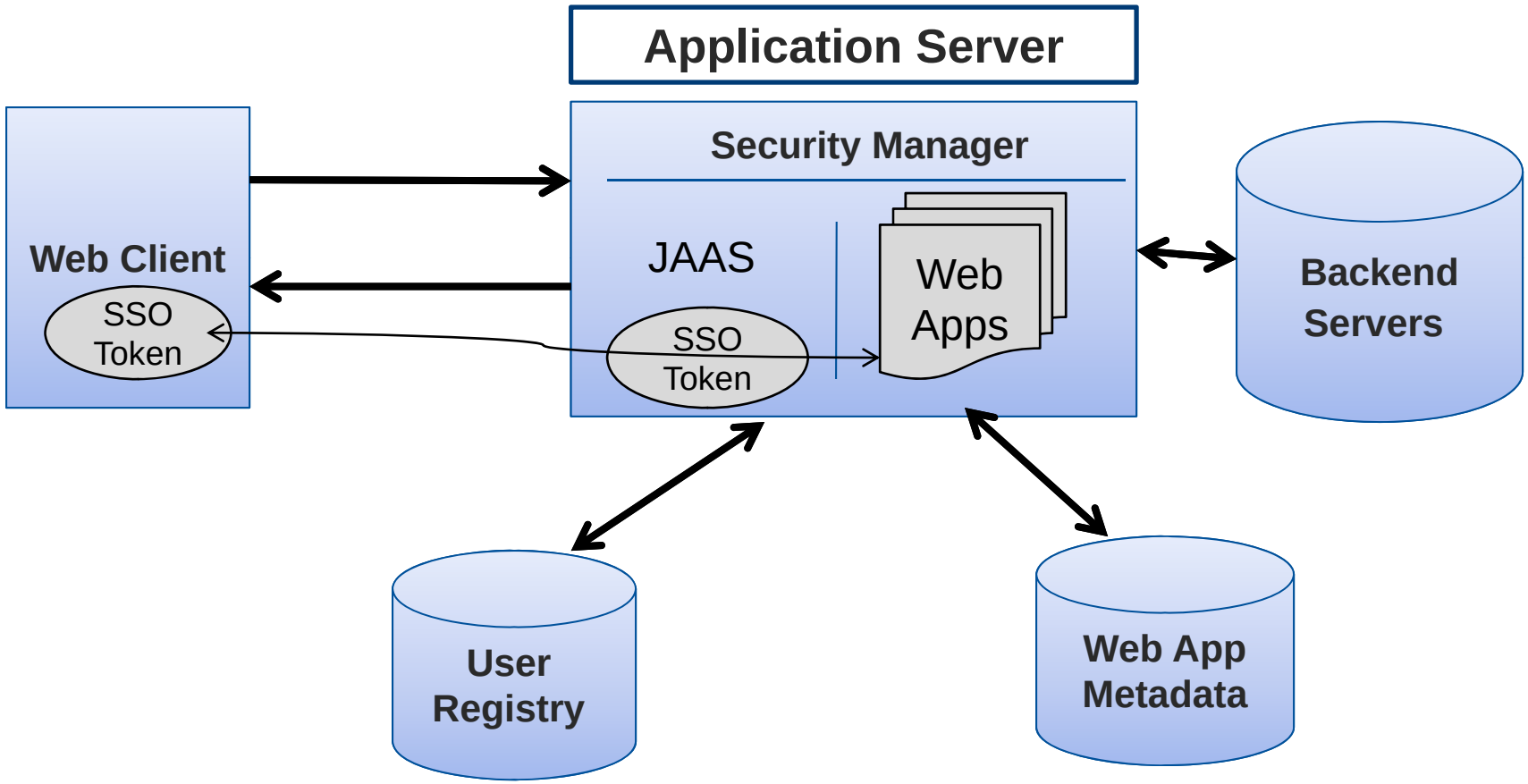
Portal Web Application based SSO



Portal Web Application based SSO

- It is a very narrowly defined SSO for the family of web applications accessible through Portal web application . Portal web application initiates authentication (typically through FORM authentication) and creates the session token for itself and passes the token when it invokes web applications under its control.
- The session information created by the Portal web application is valid only for the Portal web application. Independent access to other web applications will trigger separate authentication challenge.
- It is a simple SSO solution for the small and homogeneous environment.

Application Server based SSO



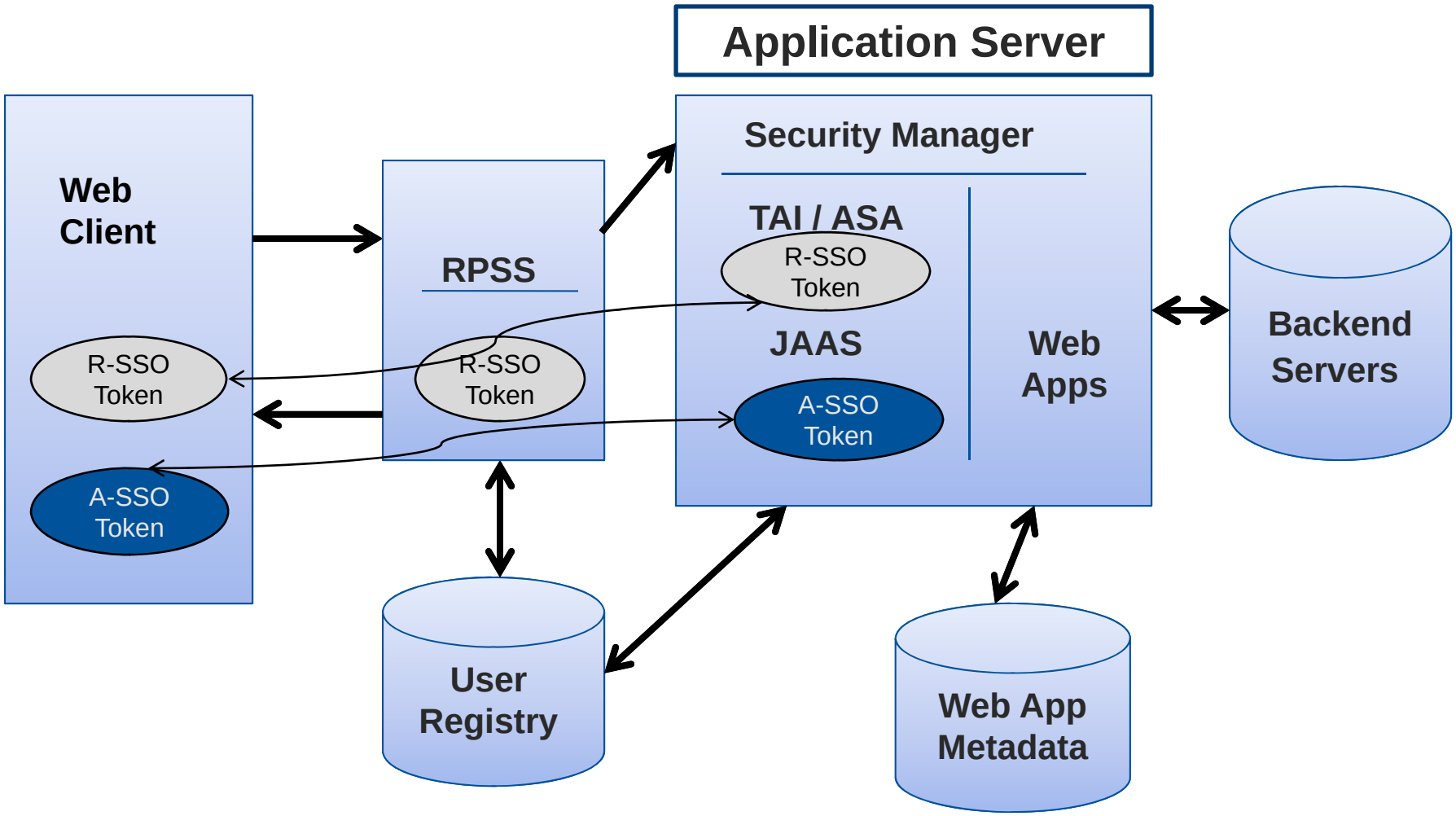
Application Server based SSO (I)

- Use of authentication service provided by the application server.
- Web application uses web.xml file to designate auth-method and security role.
- Application server creates SSO token. The SSO token gets passed to the browser as a part of HTTP header. The access to the multiple Web applications deployed in the same application server, that share the same authentication mechanism will not trigger any additional authentication challenge as the request carries the SSO token from the browser.

Application Server based SSO (II)

- Does this mean that everyone authenticated by the application server can access all web applications deployed under the same application server?
- Answer is NO. Access to each web application can be controlled by its security role mapping capability. In the web.xml, you define the role name and deliver/map the physical users to it from the application server. Only the mapped users can access the web application.
- Security role mapping implementation differs by the application server.

3rd Party Security Package based SSO



3rd Party Security Package based SSO

- Authentication is provided by the RPSS (Reverse Proxy Security Server)
- Application server trusts users authenticated by RPSS through interceptor or agent.
- RPSS creates its own session token for SSO (R-SSO), which is heavily encrypted.
- Optionally, application server can create its own SSO token (A-SSO), which is heavily encrypted.
- Security role mapping for each web application can be applied.
- Typical configuration for large organization.

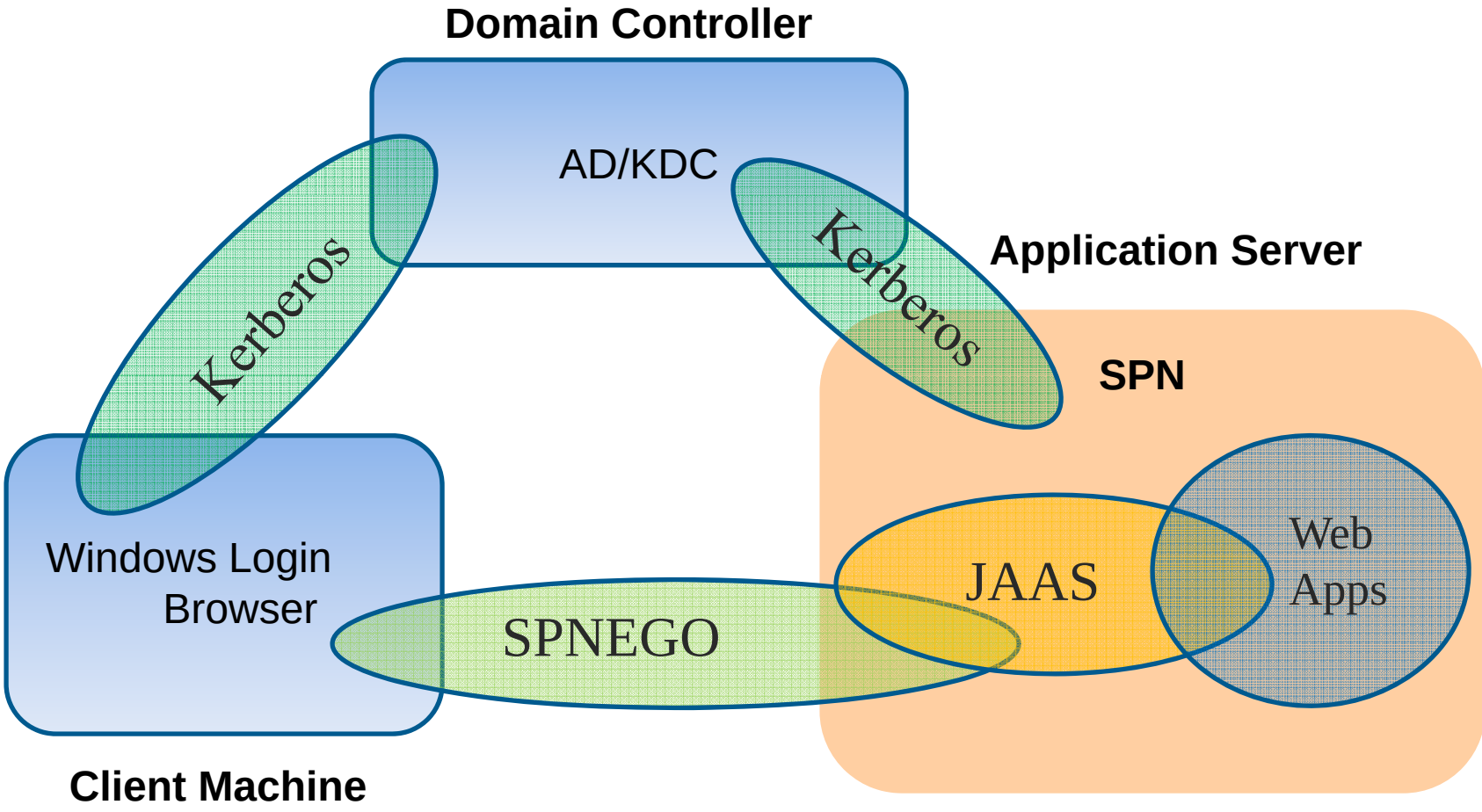
Integrated Windows Authentication (I)

- Windows domain login uses Kerberos protocol.
- Kerberos is ticket based mutual authentication protocol developed by MIT. It is the most widely used authentication protocol today.
- Kerberos is the main authentication protocol for Windows since 2000 (Windows 2000 server).
- Application server on Unix or other platform can be a Kerberos entity (SPN – Service Principal Name) and works with IWA.
- Browser supports IWA through SPNEGO protocol that wraps Kerberos ticket.

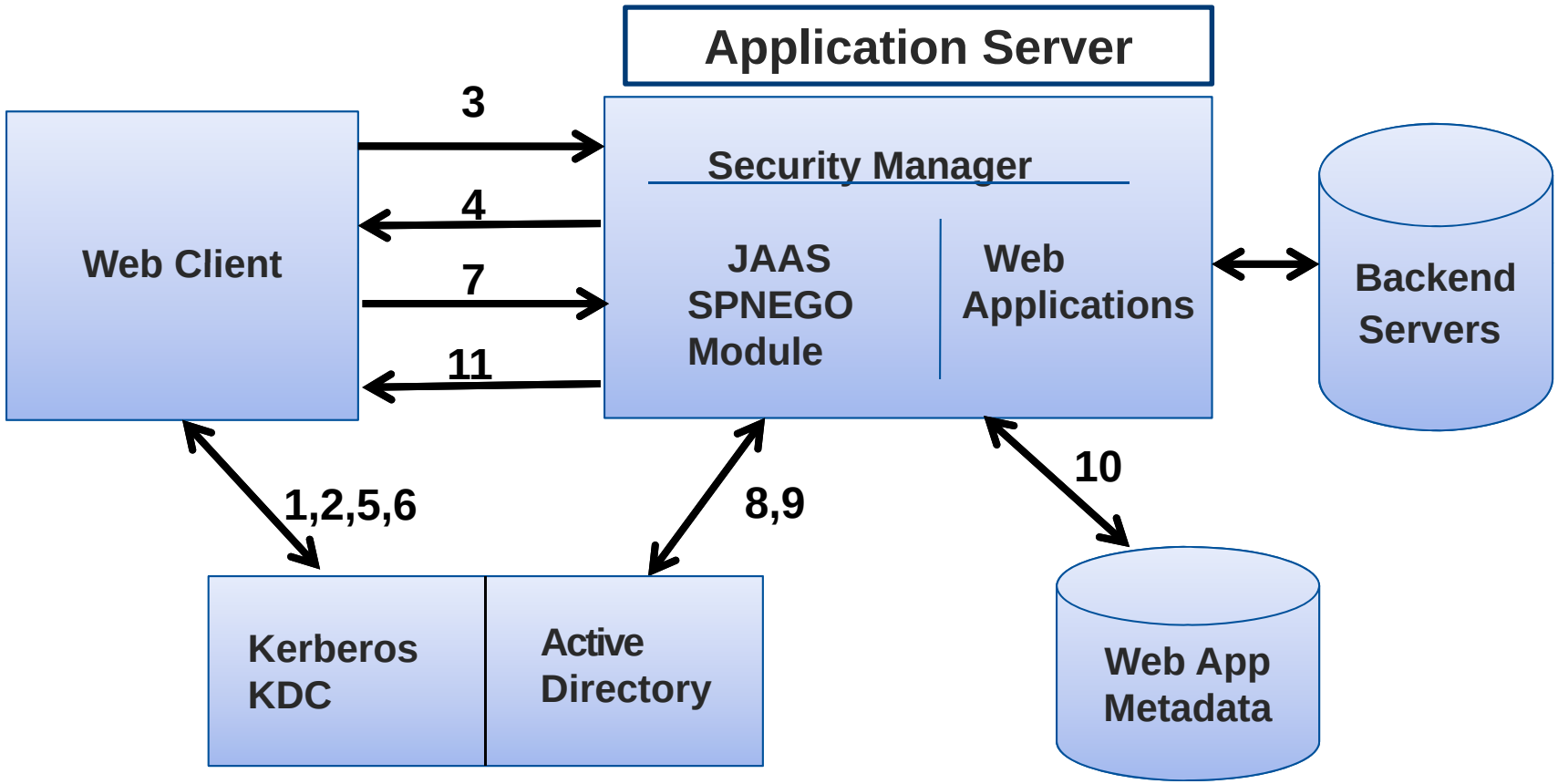
Integrated Windows Authentication (II)

- Application server supports SPNEGO though its JAAS login module.
- The Active Directory that Windows domain is based, needs to be configured as user repository for the application server.
- From SSO perspective, you login to the Windows and use that username to access web application deployed in the application server without any authentication challenge.

Conceptual IWA Authentication Path



Integrated Windows Authentication (IWA)



IWA Authentication Sequence

1) Request Ticket Granting Ticket (AS_REQ)
2) Get Ticket Granting Ticket (AS_REP)
3) HTTP Request
4) HTTP 401 Authenticate/Negotiate
5) Request Service Ticket (TGS_REQ)
6) Get Service Ticket (TGS_REP)
7) HTTP + Authorization SPNEGO Token
8) Get Username from SPNEGO Token
9) Validate User with User Registry and initialize JAAS Subject
10) Web application consumes JAAS Subject and processes the request
11) HTTP Response

Security Assertion Markup Language (SAML) based SSO **

- SSO scheme for trading partners or affiliates.
- Identity provider and Service provider agree on “Attribute Contract”.
- Federated Identity provider validates the user and creates SAML assertion and sends the assertion to the Service provider.
- JAAS login module for SAML assertion in the application server processes the SAML and initializes the JAAS Subject.
- Web application trusts the authenticated user in the JAAS Subject.

Conclusion

- Single Sign-On (SSO) means different things to different people.
- Single Sign-On process differs by the configuration.
- Understanding JAAS framework in the application server and the trust relationship among the web components are the essential pieces for successful SSO implementation.

Acronyms

SSO: Single Sign-On
JAAS: Java Authentication and Authorization Service
IWA: Integrated Windows Authentication
SSL: Secure Socket Layer
RPSS: Reverse Proxy Security Server
TAI: Trust Association Interceptor
IA: Identity Asserter
ASA: Application Server Agent
SPNEGO: Simple and Protected Negotiation Mechanism
KDC: Key Distribution Center
AD: Active Directory
AS: Authentication Service
TGS: Ticket Granting Service
SPN: Service Principal Name
SAML: Security Assertion Markup Language

Related Papers

1. "Single Sign-On Configuration and Troubleshooting for SAS 9.2 BI Web Applications", Heesun Park and Stuart Rogers, SAS Global Forum 2011, Las Vegas, USA, April, 2011

2. "Integrated Windows Authentication Support for SAS 9.2 Enterprise BI Web Applications", Heesun Park, SAS Global Forum 2010, Seattle, USA, April, 2010

3. "Security Role Based Data Encryption for J2EE Web Applications, Heesun Park, System and Software Technical Conference (SSTC) 2009, Salt Lake City, USA, May, 2009

4. "SAS Business Intelligence Web Application Security Configuration Primer" Heesun Park and Brian English, SAS Global Forum 2009, Washington DC, USA, March, 2009

5. "Client Certificate and IP Address based Multi-Factor Authentication for J2EE Web Applications", Heesun Park, Centers for Advanced Studies Conference (CASCON) - IBM, 2007, Toronto, Canada, October, 2007

Contact Information

- Name: Heesun Park
- Email: sashsp@sas.com
- Phone: (919) 531-7769