Single Sign-On

Vijay Kumar, CISSP

Agenda

- What is Single Sign-On (SSO)
- Advantages of SSO
- Types of SSO
- Examples
- Case Study
- Summary

What is SSO

- Single sign-on is a user/session authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

Advantages

- Reduced operational cost
- Reduced time to access data, eg. ER.
- Improved user experience, no password lists to carry
- Advanced security to systems
- Ease burden on developers
- Centralized management of users, roles.
- Fine grained auditing
- Effective compliance (SOX..)

Identity Management

- Encompasses
  - directory services
  - authentication and authorization services
  - certificate authorities
  - administration consoles
  - single sign-on
  - provisioning services.

Types of SSO

- Password Synchronization
- Legacy SSO (Employee SSO)
- Web SSO
- Cross domain (realm) SSO
- Federated SSO

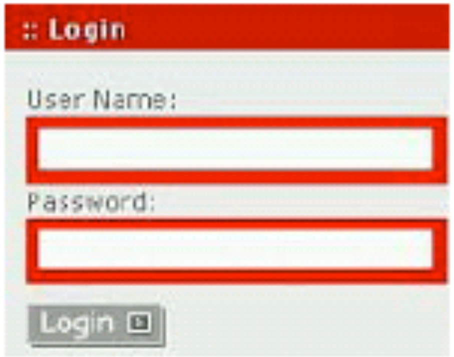
Password Synchronization

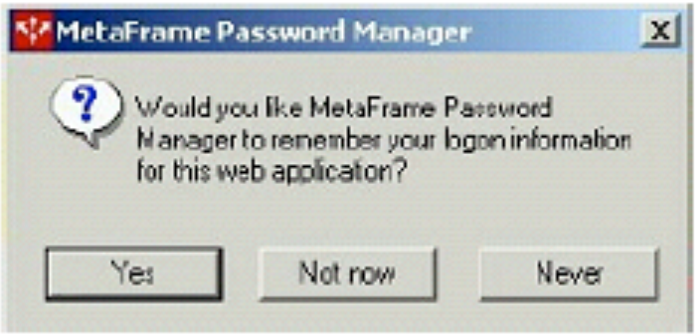
- A process that coordinates passwords across multiple computers and devices and/or applications
- Each computer, device, application still authenticates but behind the scene
- Products:
  - MTech's P-Synch
  - SecurePass
  - SAM Pass Synch

Legacy SSO

- Aka – Enterprise or Employee SSO
- After primary authentication intercepts further login prompts and fills them for you.
- Learns as you use different apps.
- Legacy apps that are unable to externalize user authentication through “screen scraping)

Citrix Password Manager





Would you like MetaFrame Password Manager to remember your logon information for this web application?

- •Installs on Citrix clients or Windows server
- •Self service password reset and account unlock
- •Hot swappable desktop (unlike Windows or Novell)
- •Integrated with User Provisioning software
- •LDAP based storage of credentials
- •Multifactor authentication support

Basic Web SSO

- Browser based application
- Cookie support is required.
- Single sign-on to applications deployed on a single web server (domain)

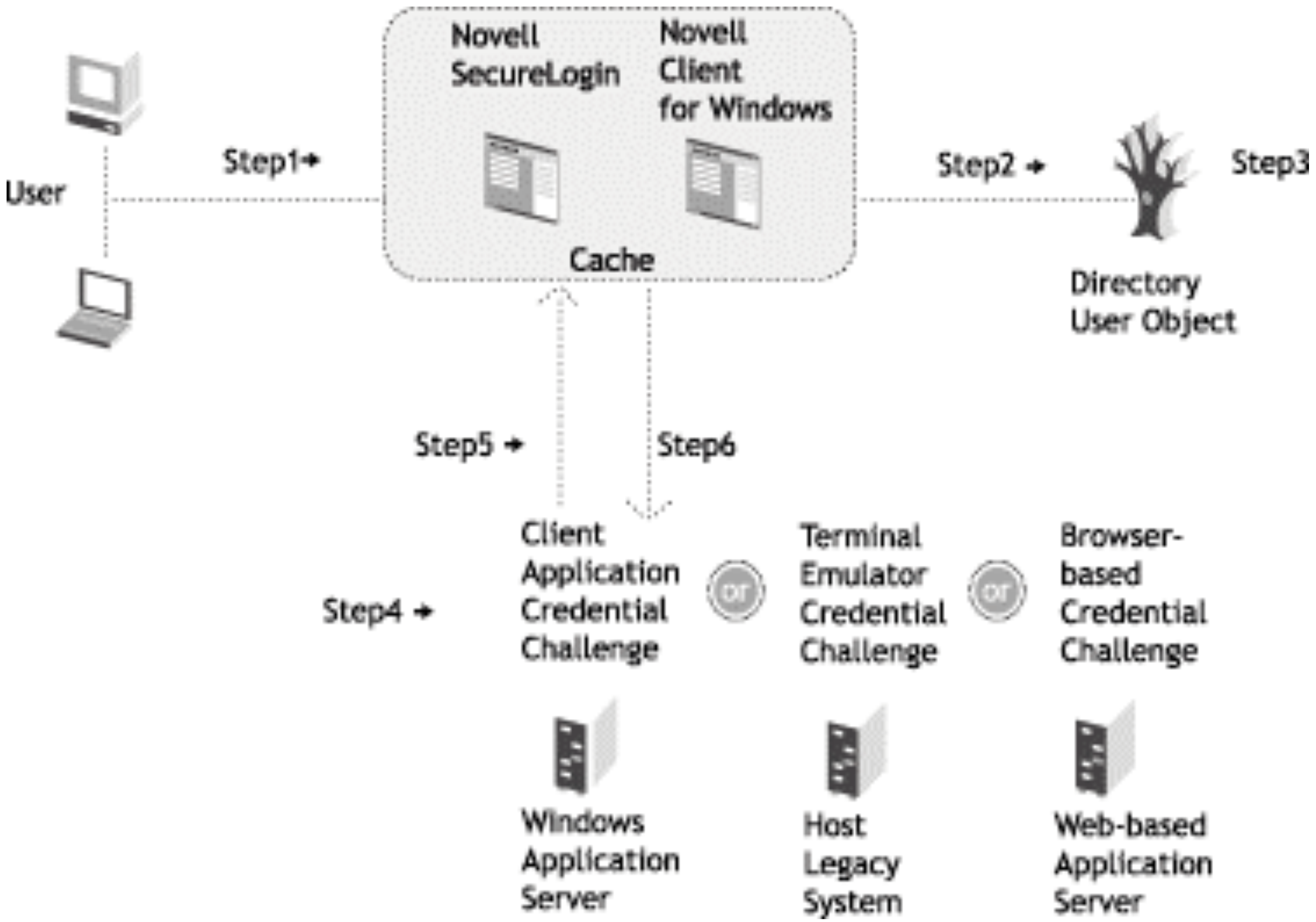
Cross Domain SSO

- Multiple realms that manage user credentials.
- A user authenticated in one realm gets signed-on to an application using another realm typically with in the same enterprise

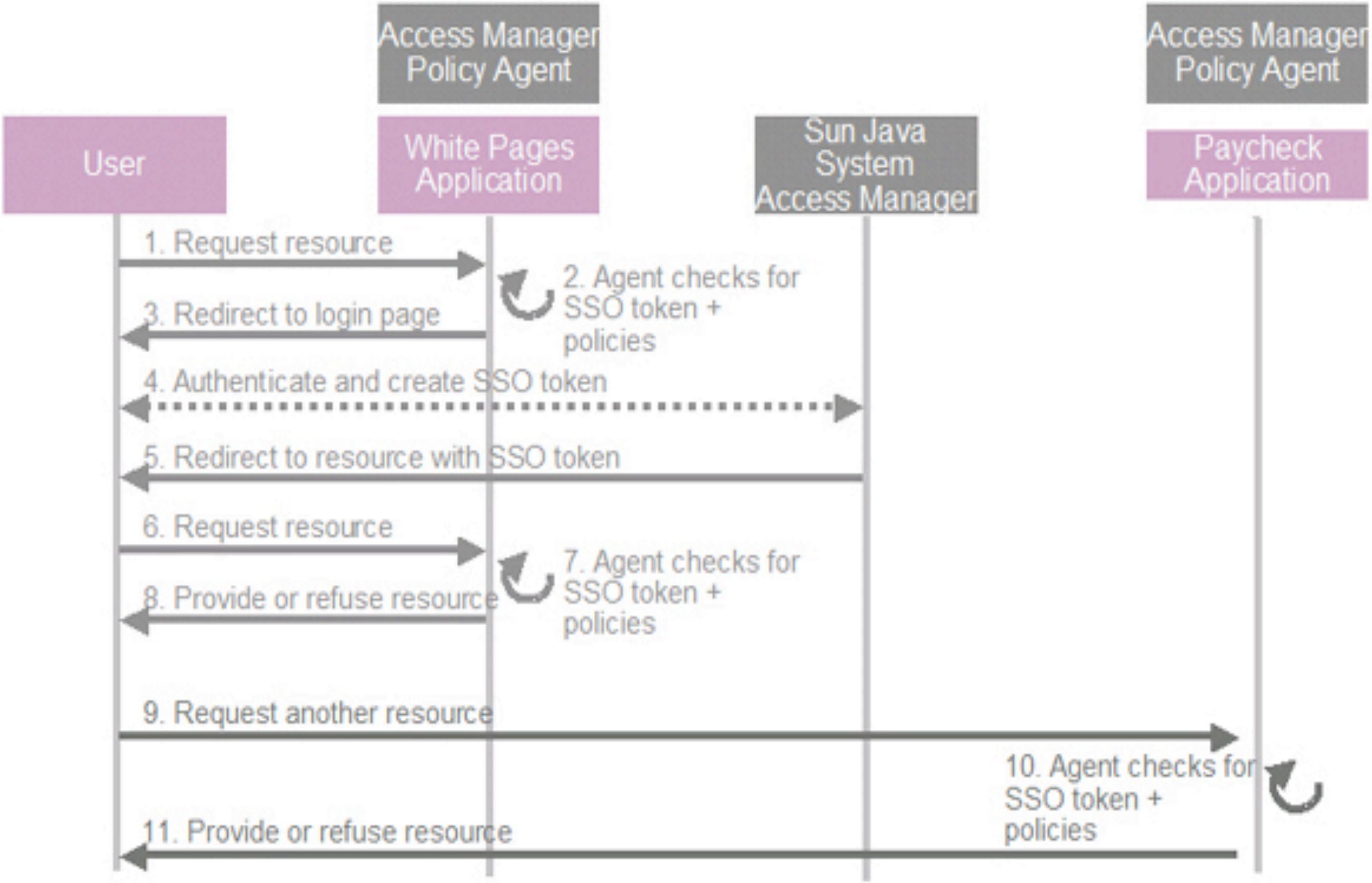
Novell SecureLogin

- True SSO for
  - Web applications
  - Windows host (Windows Application Server)
  - Legacy (Client Server) applications
- Mutiple identities and password policies stored in eDir in encrypted form
- Novell client is installed on each workstation,
- User can access apps from any workstation
- Optionally cache credentials on workstation
- Transparent pw expirations and resets

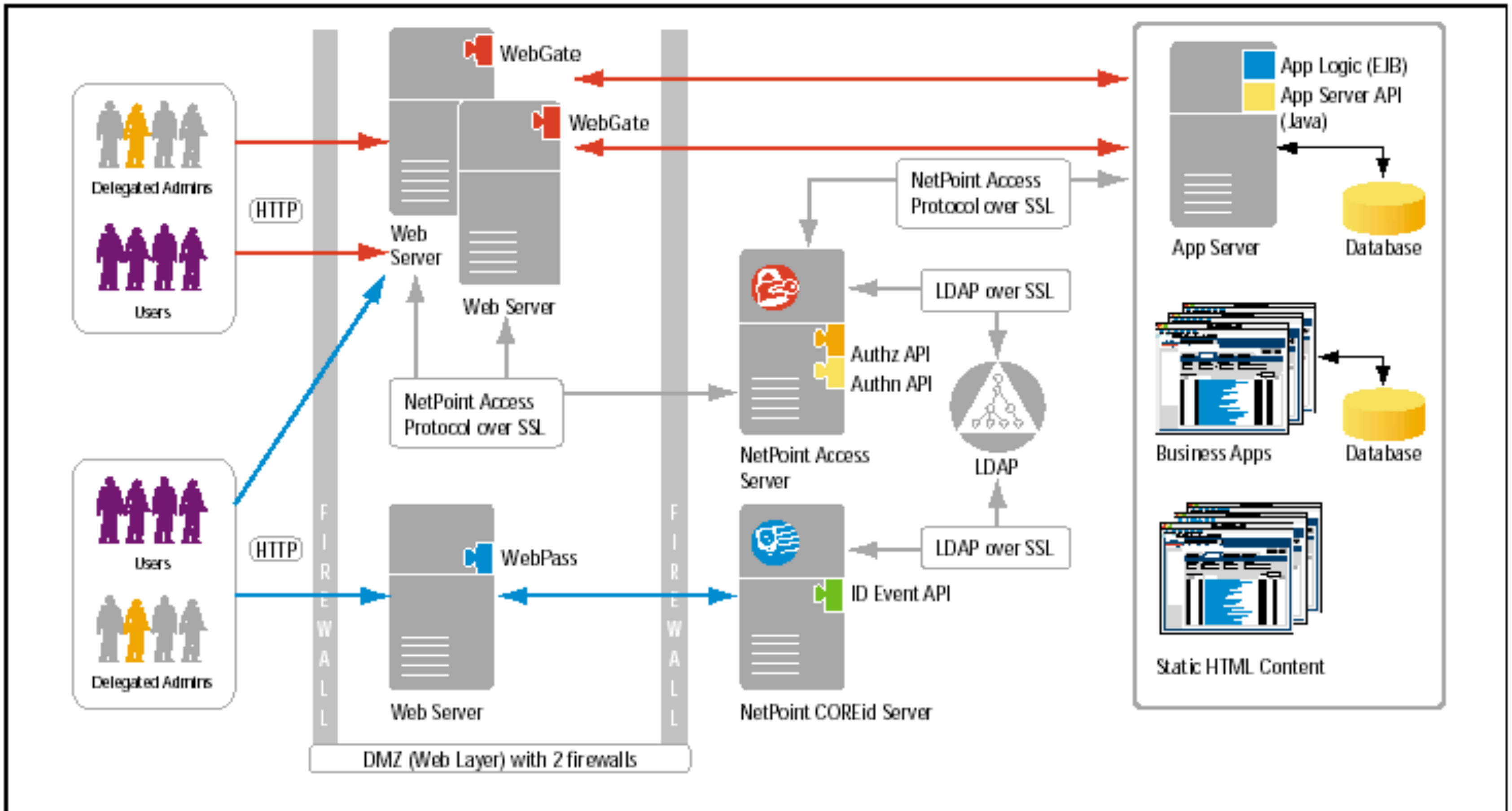
Novell SecureLogin



Sun Java Access Manager


Access Manager Policy Agent
Access Manager Policy Agent
User
White Pages Application
Sun Java System Access Manager
Paycheck Application
1. Request resource
2. Agent checks for SSO token + policies
3. Redirect to login page
4. Authenticate and create SSO token
5. Redirect to resource with SSO token
6. Request resource
7. Agent checks for SSO token + policies
8. Provide or refuse resource
9. Request another resource
10. Agent checks for SSO token + policies
11. Provide or refuse resource

Oblix (Oracle)

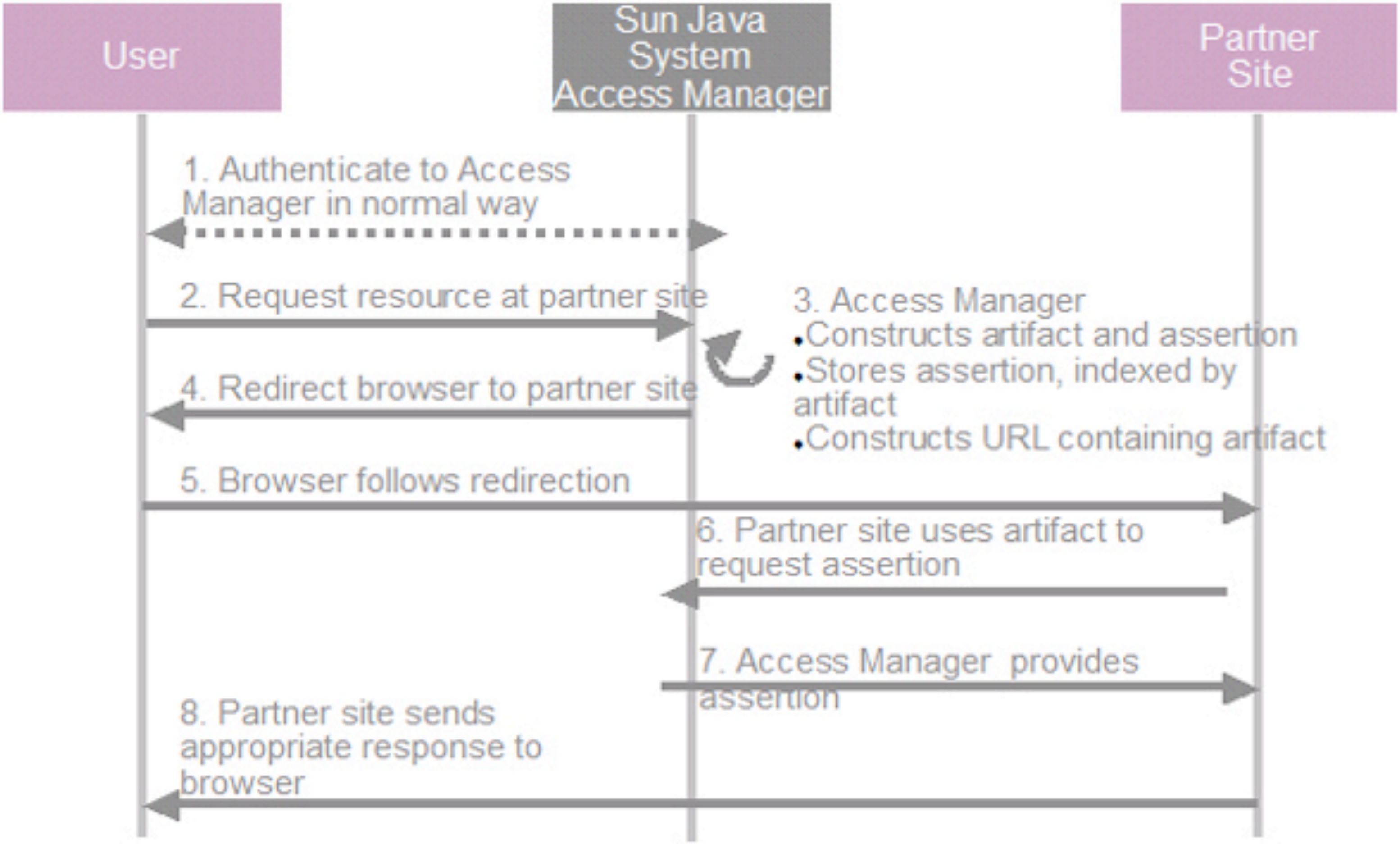


The Oblix NetPoint Three-Tier Architecture

Federated SSO

- Extend SSO across enterprises
- One of the goals of the Liberty Alliance
- Advantages
  - Establishment of trusted partnerships
  - New revenue opportunities
  - New, efficient, and production biz models
- Why is this hard to implement?
  - SAML (OASIS)
  - Liberty Alliance builds fed ident on top of SAML

Liberty model for federated SSO



User

Sun Java System Access Manager

Partner Site

1. Authenticate to Access Manager in normal way

2. Request resource at partner site

3. Access Manager
- Constructs artifact and assertion
- Stores assertion, indexed by artifact
- Constructs URL containing artifact

4. Redirect browser to partner site

5. Browser follows redirection

6. Partner site uses artifact to request assertion

7. Access Manager provides assertion

8. Partner site sends appropriate response to browser

Microsoft

- Windows Server 2003 R2 adds
  - Active Directory Federation Service
  - Web Services based SSO
  - Use Active Directory in non-Windows env
- Microsoft Identity Integration Server 2003
  - SSO and account management features
  - “agents" that handle protocol translation between Active Directory
  - ADFS provides federated SSO based on WS-*

Summary

- SSO is saves money and enhances security

- But….there are risks.

  – Malicious user gets hold of unattended desktop
  – Malicious processes/services sign on as you to services that they are not supposed to.

References

- Sun Java System Access Manager
- eTrust Secure Sign-On
- Oracle IDM
- IBM Tivoli Access Manager
- Novell SecureLogin
- Citrix Password Manager
- Liberty Alliance
- Yale CAS (Central Authentication Service)
  - Integrates well with Spring based Acegi