



# Teamcenter Security

PLM World 2006

Troy Banitt

Teamcenter Product Management



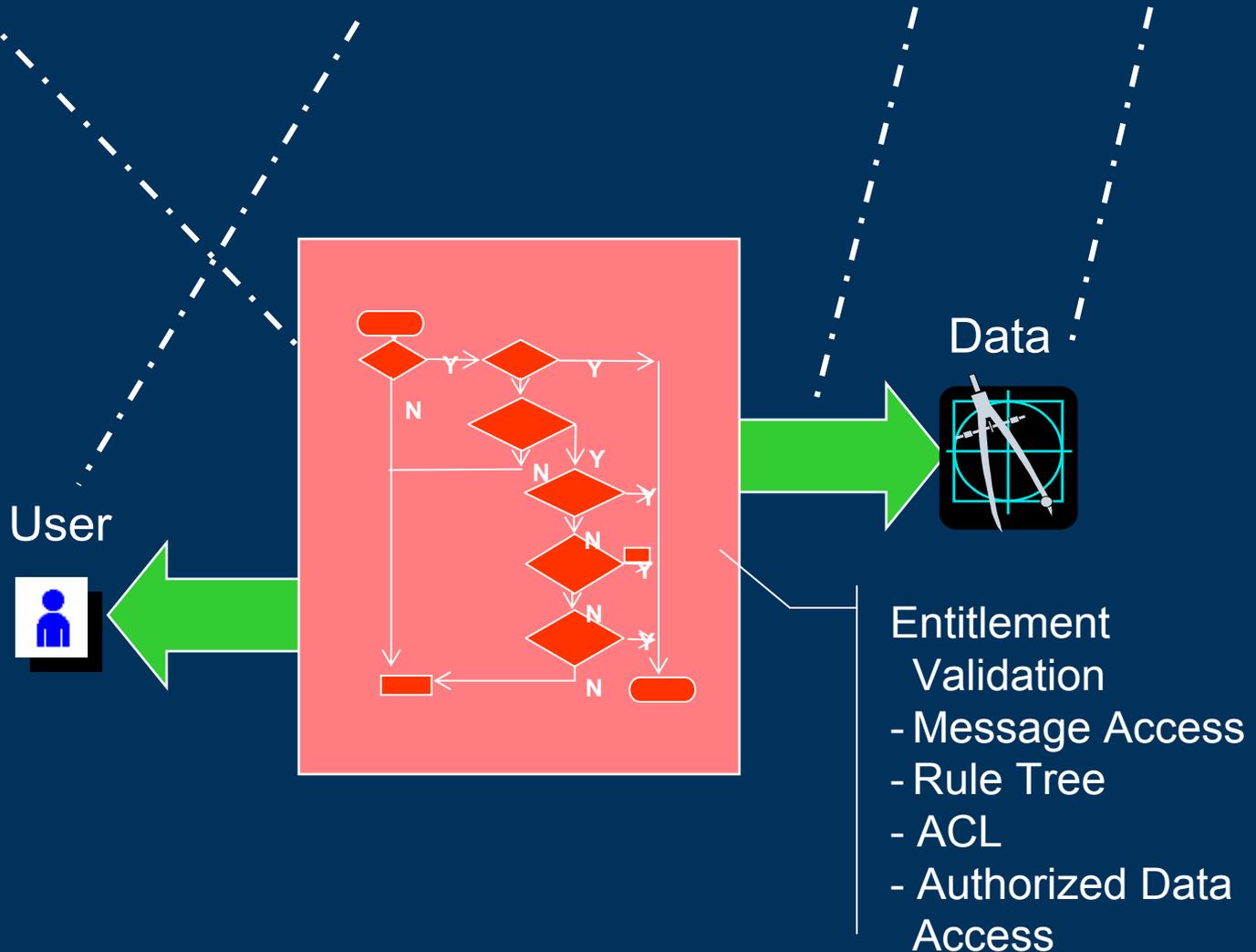
- ▶ Requirement
  - ▶ Must have a globally secure environment to share intellectual capital and collaborate with employees, suppliers and customers
- ▶ Business Value
  - ▶ Help customers lower administration costs associated with system security
  - ▶ Leverage corporate security infrastructure to help reduce cost and improve system security
  - ▶ Comply with applicable laws and regulations
  - ▶ Support industry standards and best practices



# Application of Core Security Concepts



Security applies to User, When he/she tries to Access Data





- ▶ Terminology
- ▶ Teamcenter Security Services
  - ▶ External Authentication
  - ▶ Common Directory
  - ▶ Single Sign-On
  - ▶ External Authorization
- ▶ Authorized Data Access
  - ▶ Export Control
  - ▶ ITAR Support



<b>Authentication</b>	Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. With computer systems and networks, authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.
<b>Authorization</b>	Designates user access to various system resources based on the user's identity. Authorization is typically defined through the use of categories such as groups, roles and teams.
<b>Entitlement</b>	Determining whether a participant has the rights/privileges to access specific functionality or a specific piece of information within a system at a given point in time. This is usually accomplished through the execution of business rules against the authorization defined for the entity.



# Security Terms



Directory	A place to store information about network-based entities, such as applications, files, printers, and people. It provides a consistent way to name, describe, locate, access, manage, and secure information about these individual resources.
Single Sign-On (SSO)	Single Sign-On (SSO) is a session/user authentication process that permits a user to authenticate once and then access multiple applications. SSO eliminates future authentication prompts when the user switches applications during that particular session.
LDAP	Lightweight Directory Access Protocol, or LDAP, is an open Internet standard defined by Internet Engineering Task Force (IETF) for applications to access online directory services. A LDAP service may be powered by a stand-alone LDAP server or by a backend directory server.



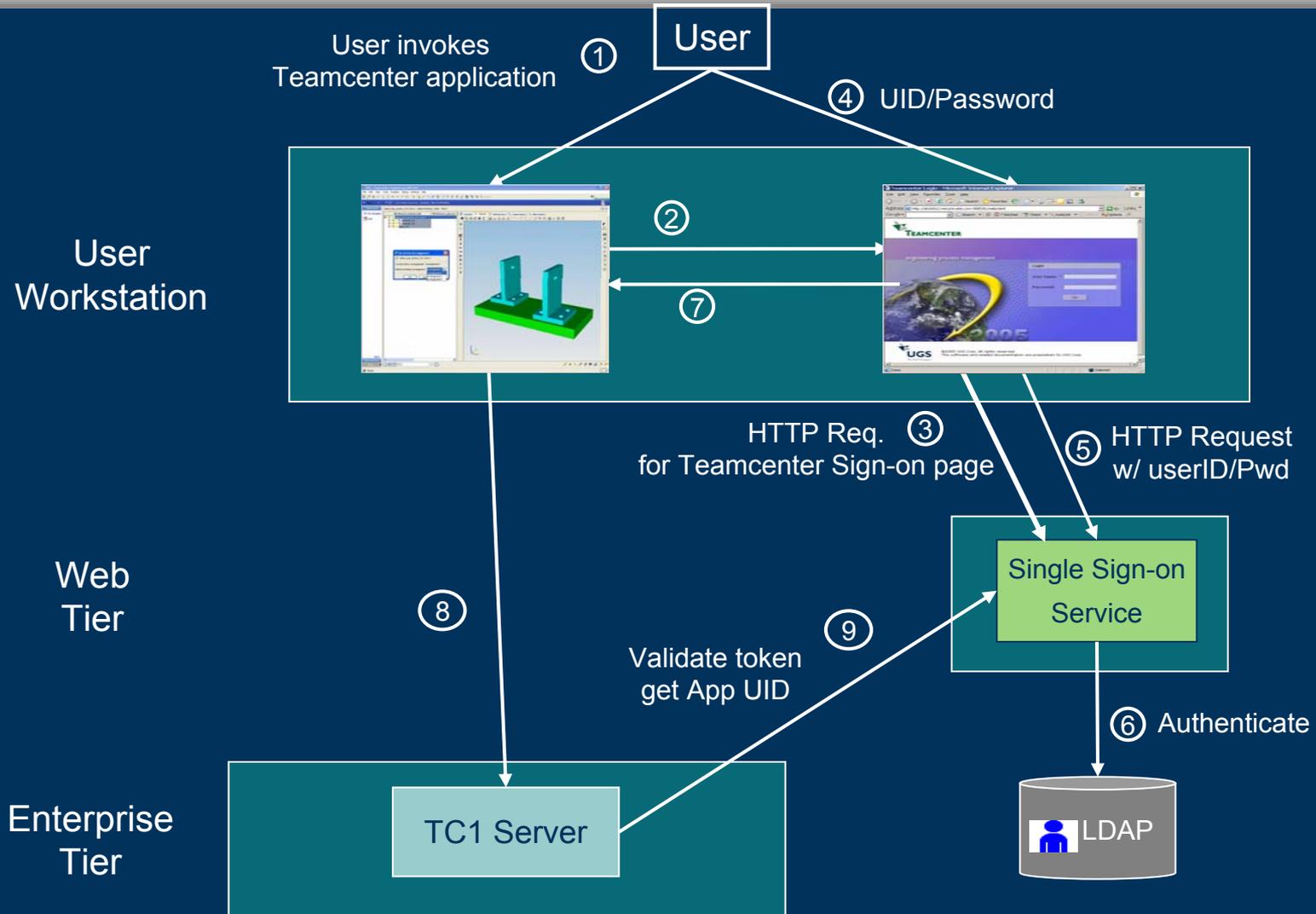
- ▶ Teamcenter Security Services provides a common framework to use 3<sup>rd</sup> party authentication and single sign-on solutions
  - ▶ User authentication (both directory integration and client single challenge / SSO)
  - ▶ Optional coordination with commercial single sign-on application
  - ▶ External Authorization with Teamcenter Engineering 2005 SR1



- ▶ External Authentication
  - ▶ Leverage corporate directory servers
  - ▶ Lower administration costs
  - ▶ Common authentication mechanism across Teamcenter applications
- ▶ Single Sign-On
  - ▶ Eliminate the need for repetitive manual login processes so that logging in is seamless to the user
  - ▶ Provide a common and shared mechanism for user's credentials calling trusted applications
  - ▶ Support corporate security policies



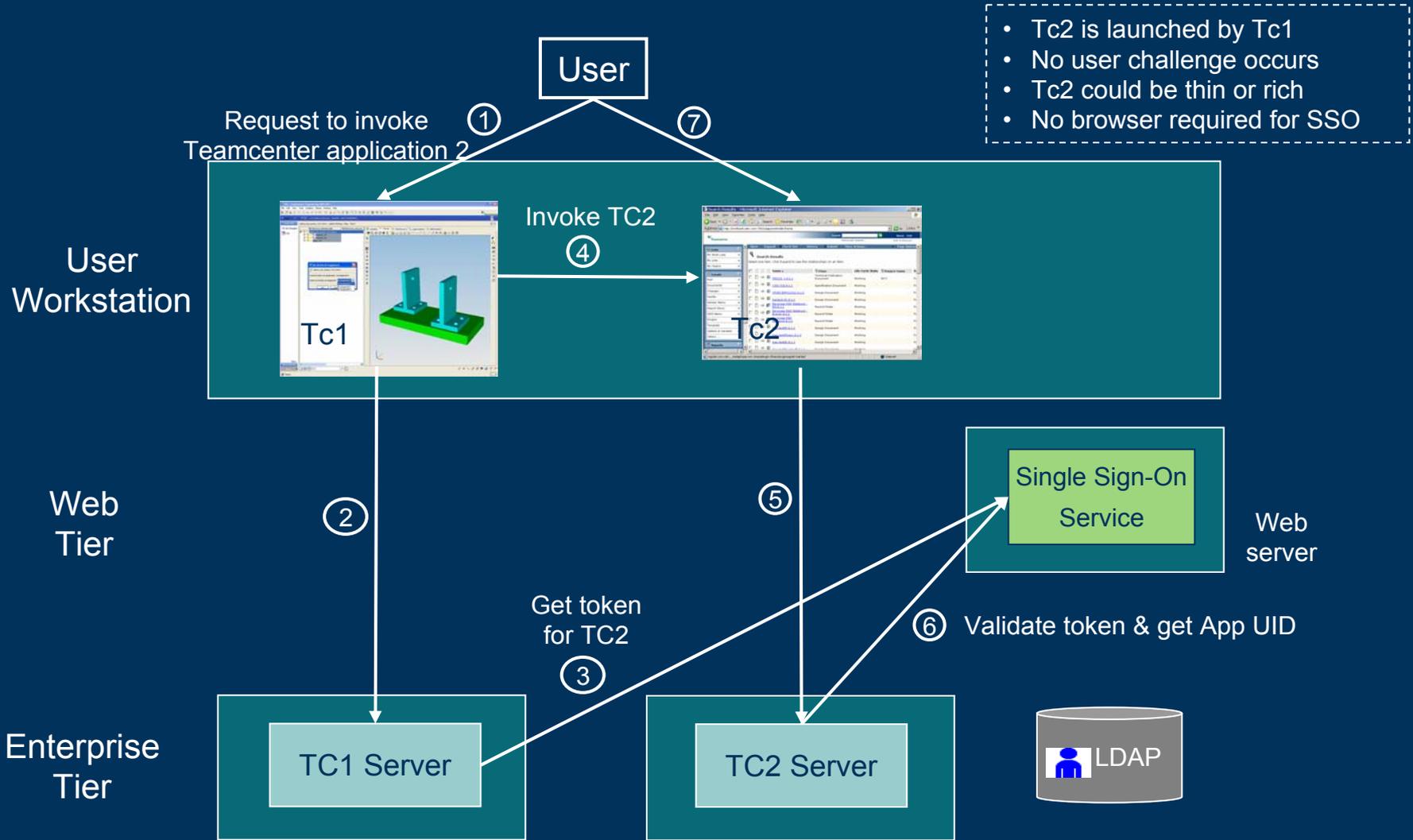
# Teamcenter Client Login





# Launching Teamcenter Application 2 from Teamcenter Application 1

Post login



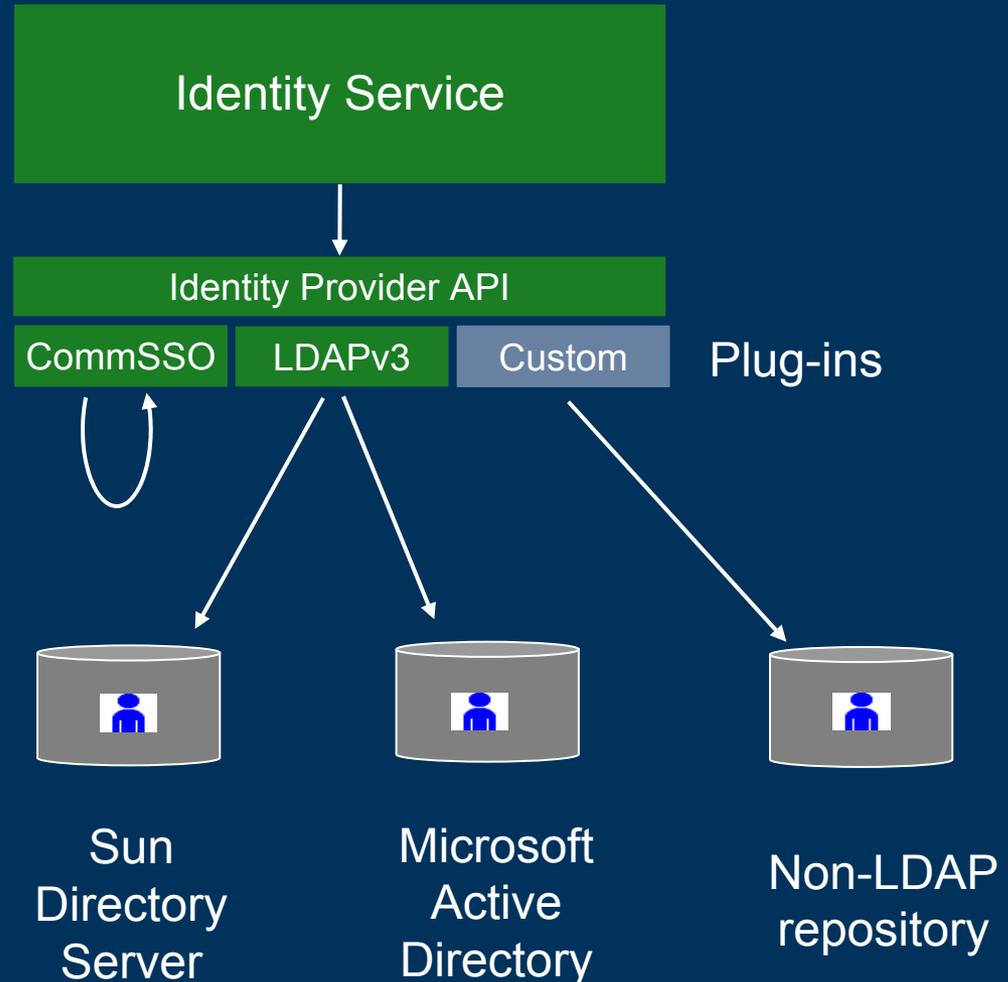


# Identity Provider Plug-ins



Plug-ins certified for LDAP v3 directories:

- ▶ Active Directory
- ▶ SunONE Directory Sever
- ▶ Oracle Internet Directory





# Teamcenter Security Service Features



- ▶ Single login page for access to all Teamcenter clients
  - ▶ 'Single challenge' provides secure access across clients, processes, hosts and sites
- ▶ Requires no user workstation installation or administration
- ▶ Uses HTTP(S) protocols
- ▶ Can be configured to work with
  - ▶ LDAP servers, such as Microsoft Active Directory and the SunONE Directory Server
  - ▶ Commercial single sign-on products (such Netegrity Siteminder, IBM Tivoli AM/WebSEAL)



- ▶ Login Service
  - ▶ A Web application that serves login page and welcome page for Teamcenter Clients
  - ▶ Web browser clients interact with the Login Service through a web redirection protocol, while rich clients interact with the Login Service through applets
- ▶ Identity Service
  - ▶ The Login Service interacts with Identity Service to authenticate users and to generate Single Sign On tokens



# Support for LDAP Referrals



- ▶ Teamcenter Security Services supports a distributed LDAP environment through support of “referrals”
  - ▶ Referrals are an LDAP v3 construct where 1 LDAP server can have a subtree that exists in another LDAP server
  - ▶ When searching for a user, traverse referral links if and only if the user was not found in the current server (no unnecessary server hops)
  - ▶ When authenticating a user, connect to the server where that user is located, then authenticate that user
- ▶ Like the root LDAP server, the referred-to LDAP servers may allow anonymous searches or may require query DN credentials. Three authentication options are supported:
  - ▶ Anonymous (for all servers or for specific LDAP servers)
  - ▶ Common query DN – use the root query DN credentials for all servers
  - ▶ Per-server query DN credentials – define these in the Referral Credentials table



# Using Secure Sockets Layer (SSL)



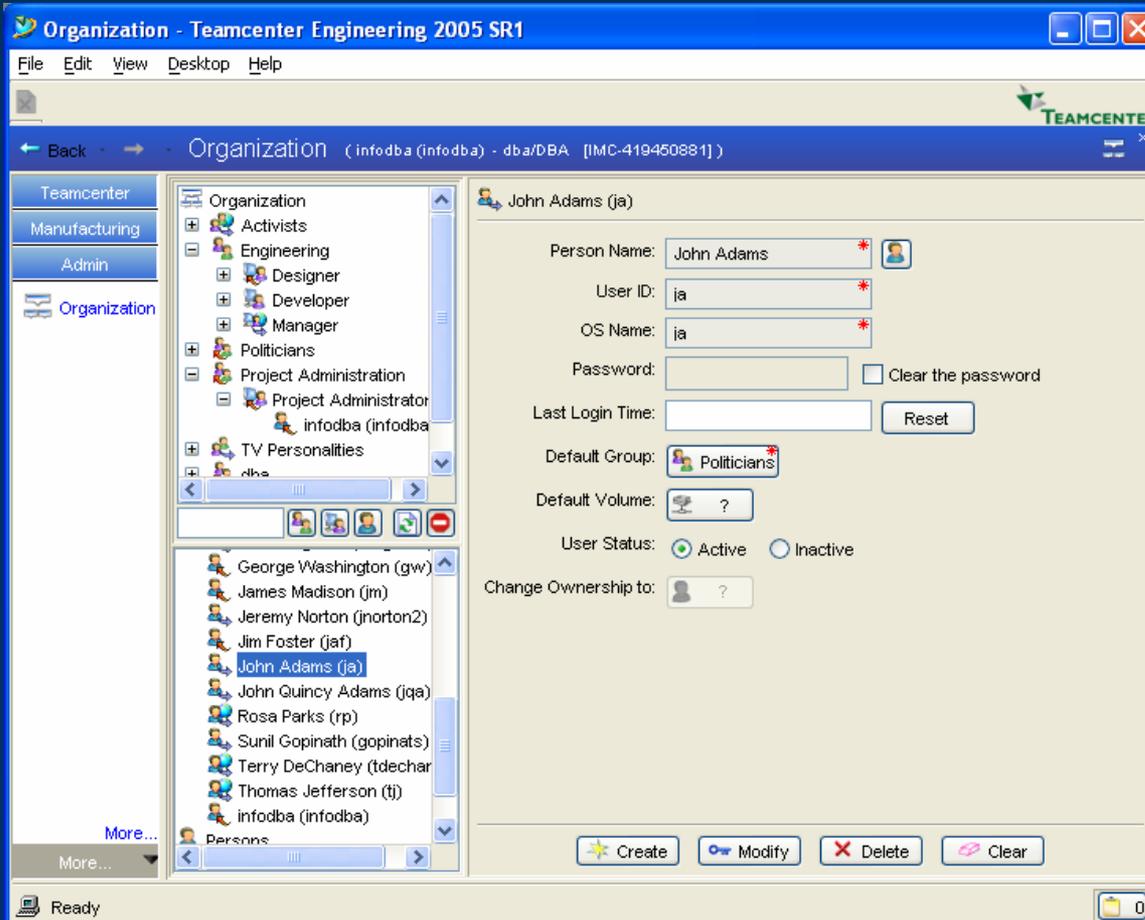
- ▶ All Teamcenter Security Services communication may be encrypted via SSL
  - ▶ Achieved by configuration
- ▶ Configuration involves
  - ▶ Using SSL URLs – specify “https” protocol and SSL port
  - ▶ Using LDAPS – specify the LDAP server’s SSL port



- ▶ Install of Login Service and Identity Service on Web Tier
  - ▶ WAR files created using INSWEB installation utility
  - ▶ Runs on supported Teamcenter Application Servers
- ▶ All versions of Security Services are cross-compatible with Teamcenter applications
  - ▶ Both forward and backward
  - ▶ Any version of Security Services components can interoperate with any version of a Security Services-enabled Teamcenter application



# External Authorization with Teamcenter Engineering 2005 SR1



- ▶ Deliver extended command line sync tool for synchronizing groups and default roles into Teamcenter Engineering 2005 SR1
- ▶ Batch synchronization and “On-Demand” by running sync tool
- ▶ Includes mechanism to prevent administrators from changing user attributes that are coming from external repository



# Engineering 2005 SR1 External Authorization

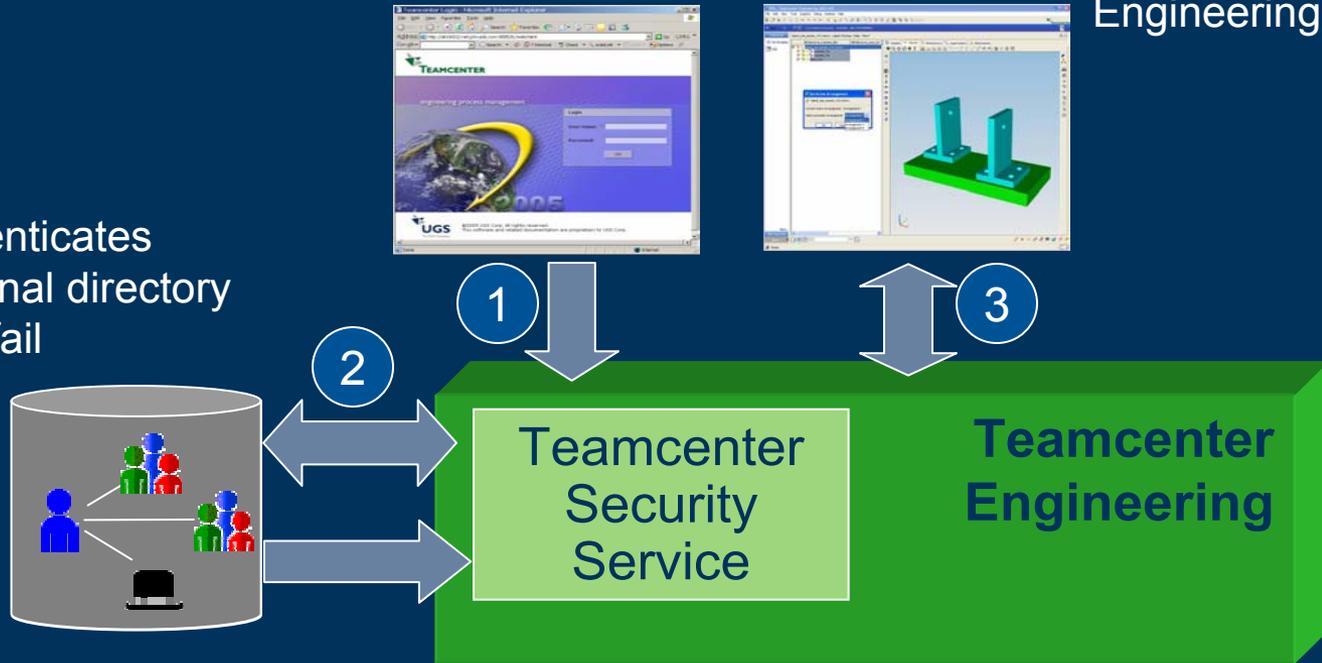


User supplies login / password through Teamcenter client which is passed to authentication service

On pass Teamcenter application launches and authorization is provided by groups, roles and projects persisted in Teamcenter Engineering

Teamcenter authenticates user against external directory and returns pass/fail

External Directory  
e.g. LDAP



Uni-direction synchronization tool provided to sync role and group definitions in Teamcenter from external repository



## Commercial Single Sign-On (SSO)



# Commercial SSO



- ▶ Authenticates access to web applications
  - ▶ Typically they do not support rich clients
- ▶ Performs user authentication
  - ▶ Typically tied to an LDAP directory
- ▶ Monitors all HTTP traffic
- ▶ SSO session is tied to the browser session
- ▶ Products
  - ▶ CA (Netegrity) Siteminder
  - ▶ IBM Tivoli Access Manager (WebSEAL)
  - ▶ Sun Identity Server
  - ▶ Oracle Oblix NetPoint



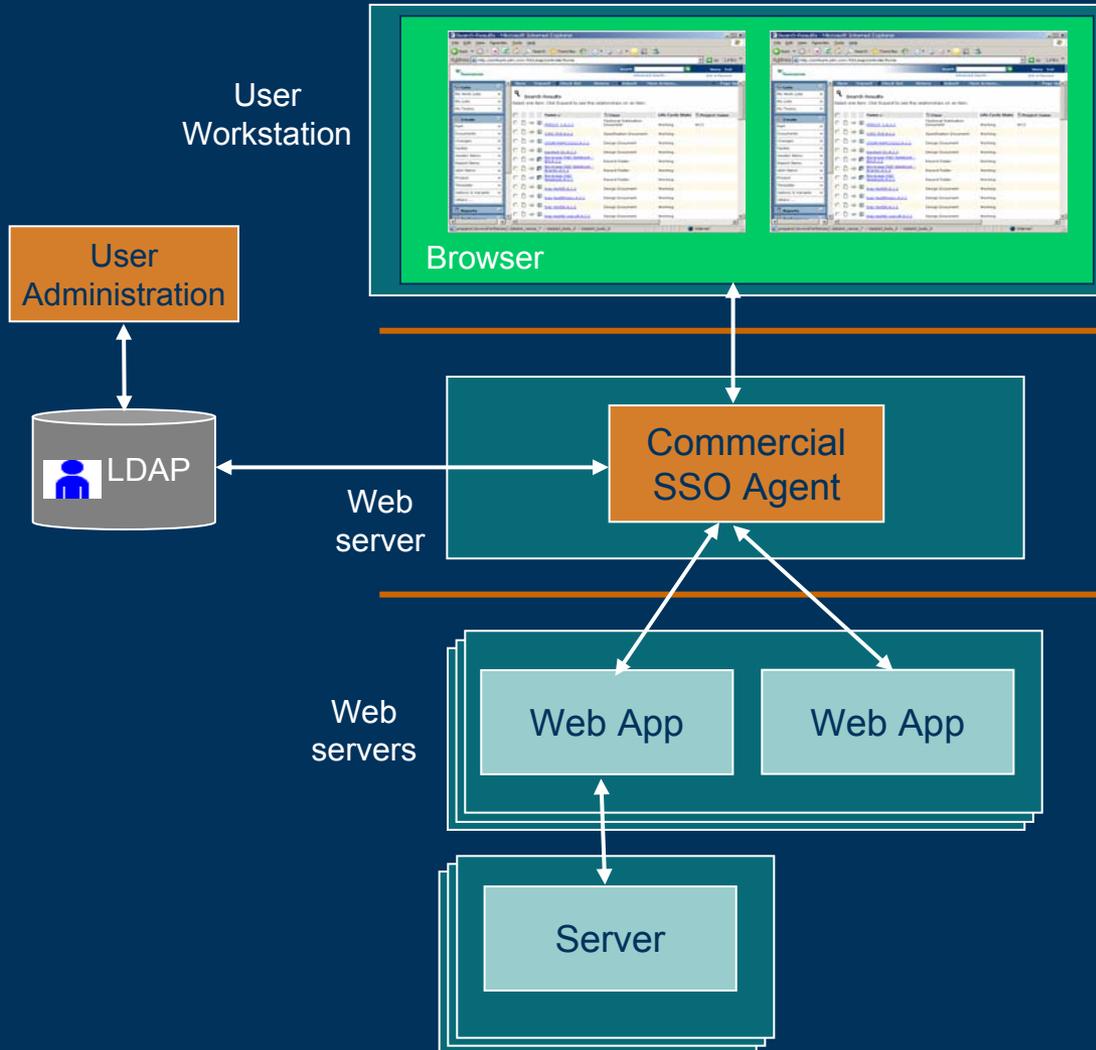
# Integration Approach



- ▶ Teamcenter Security Services is designed to co-exist and interoperate with commercial Single Sign-On (SSO)
- ▶ When configured to support commercial SSO
  - ▶ Login Service is configured as a protected web app
  - ▶ Teamcenter Identity Service does *not* perform authentication
  - ▶ Can do application-level authorization, if desired
  - ▶ Integrates Teamcenter rich clients “under” the commercial SSO session – rich client login occurs via commercial SSO
  - ▶ Insulates individual Teamcenter applications from direct integration with the commercial SSO product
  - ▶ The Teamcenter SSO session
    - ▶ Is established after login on first Teamcenter application startup
    - ▶ Persists until all participating Teamcenter applications are terminated

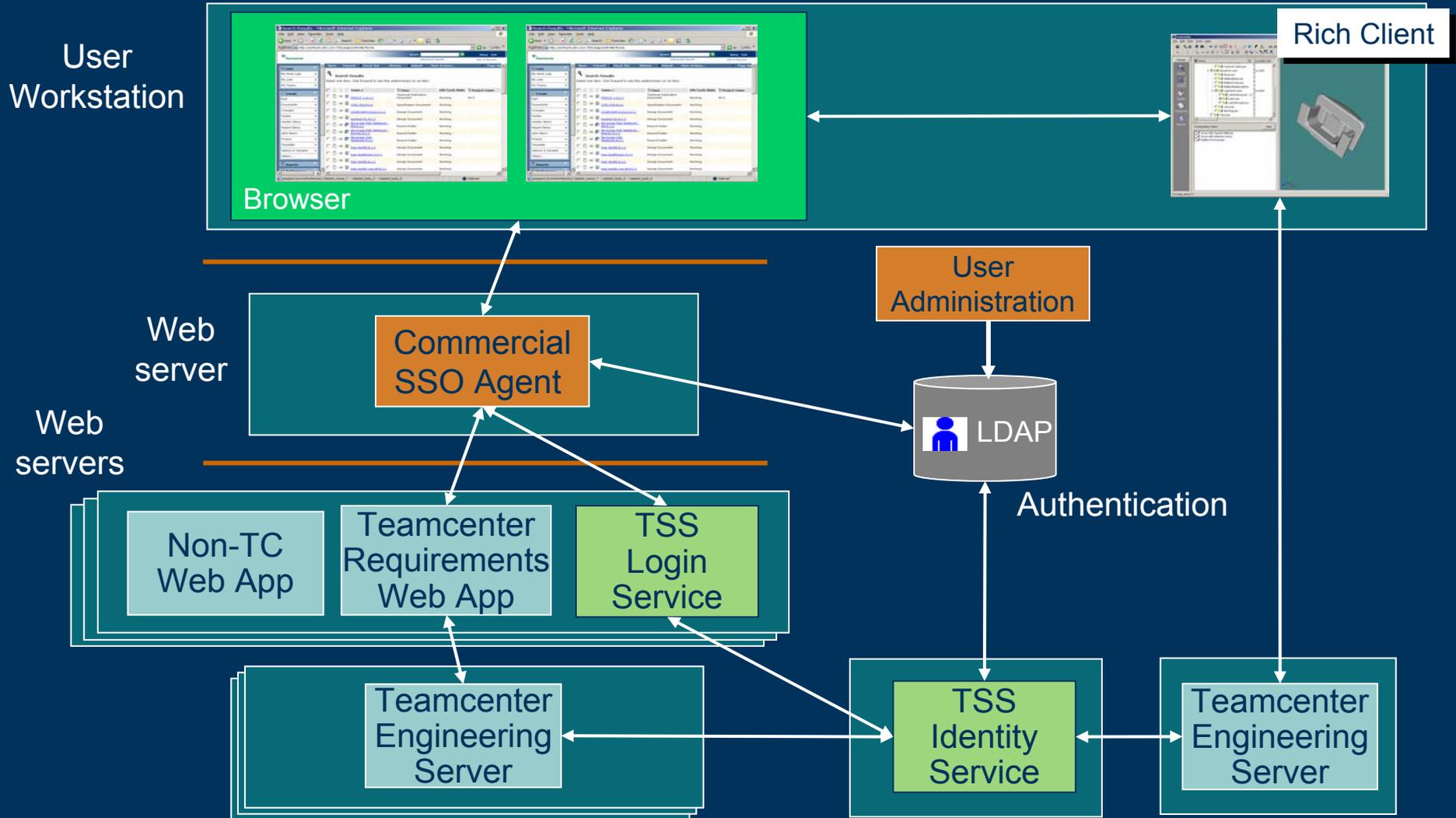


# Commercial SSO Architecture





# Teamcenter and Commercial SSO





# Commercial SSO Configuration



- ▶ Teamcenter 2005 and later support integration via configuration
  - ▶ Login Service context parameters
  - ▶ Identity Service context parameters
- ▶ Customization is required in some cases
  - ▶ Login Service customization – PreLoginPage.jsp
  - ▶ Identity Provider plug-in customization



# Authorized Data Access



# Authorized Data Access – Concepts Teamcenter Enterprise 2005



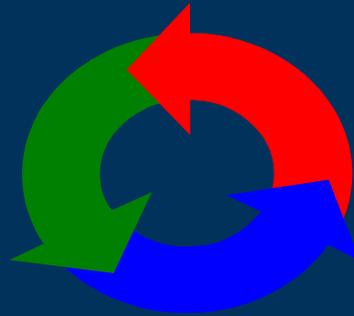
- ▶ Authorized Data Access is an umbrella term that covers;
  - ▶ Export Control e.g. ITAR
  - ▶ Non-Disclosure Agreements
  - ▶ Supplier contracts
- ▶ Facilitating Data Access Control via
  - ▶ Identification of users as restricted
  - ▶ Identification of data as restricted
  - ▶ Authorization of access to restricted data by restricted users using “Authorizing Documents”
    - ▶ Licenses
    - ▶ Technical Assistance Agreement (TAA)
    - ▶ Non-Disclosure Agreements
    - ▶ Contracts
  - ▶ ADA access validation during any access attempt by restricted user



# Teamcenter Supports the 3 steps to Authorized Data Access

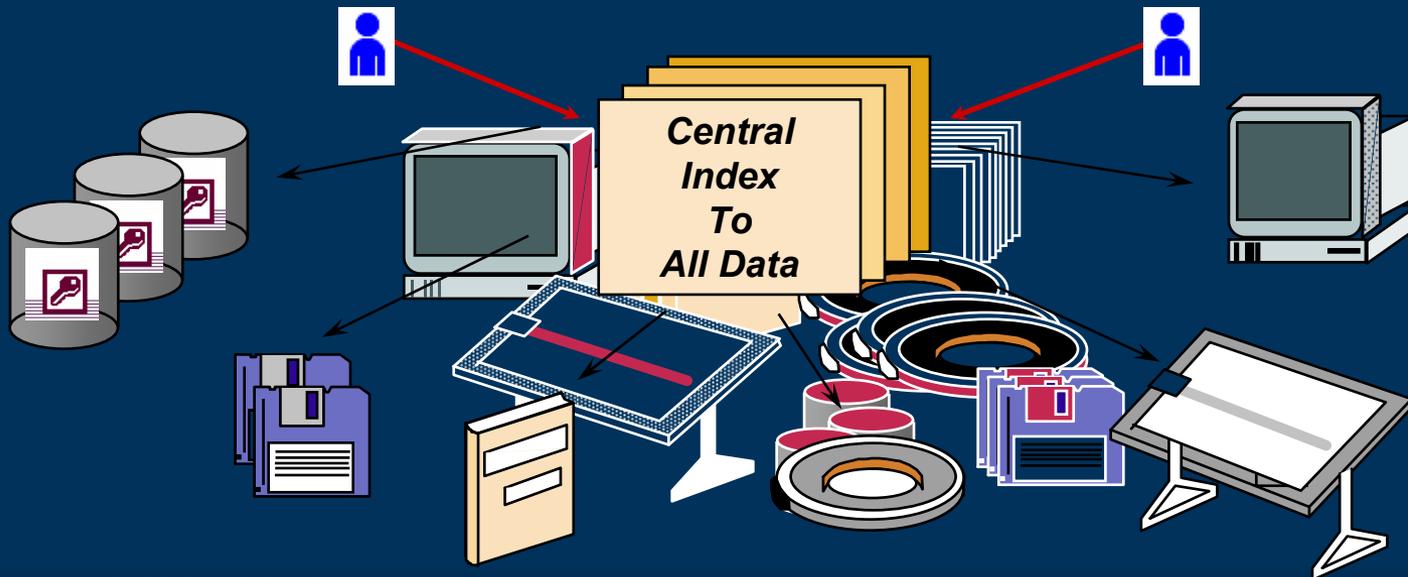


1) Consolidate and Control Your Data



2) Ensure All Users Have Appropriate Security Registration

3) Manage The Electronic Processes that Distribute Your Product Information





# Authorized Data Access - Functional Areas



- ▶ User extensions
  - ▶ Access level (restricted/full), nationality, company, training designated on user object
- ▶ Data extensions
  - ▶ Export control attributes
- ▶ Authorizing Documents (License/TAA)
  - ▶ Identify authorized restricted users, groups
- ▶ Data Access Validation
  - ▶ Leverage existing entitlement engine
- ▶ Configurability
  - ▶ Conditional control of items, and propagation during revision



# Functional Area – Users



- ▶ Access Level
  - ▶ Restricted / Full Access
- ▶ Location
  - ▶ Nationality, Company
- ▶ Training Completion Date
  - ▶ Warning if training completion date is expiring
  - ▶ Automatic deactivation upon expiration



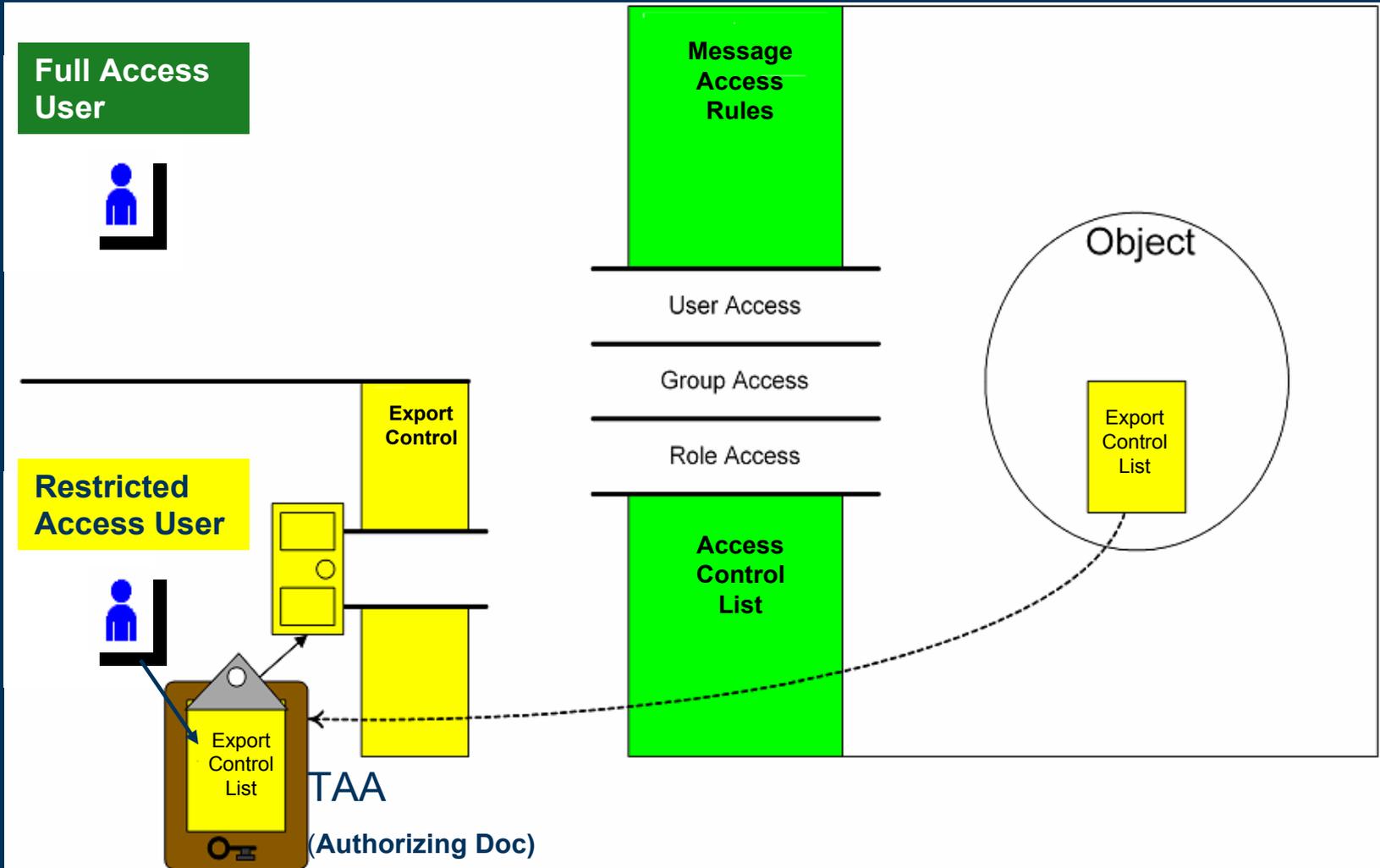
# Functional Area - Authorizing Document



- ▶ Attaches legal (e.g. Licensed) content
- ▶ Holds list of authorized / restricted access groups and individual users
- ▶ Has expiration date
- ▶ Has activate / deactivate capability
  - ▶ Automatic deactivation upon expiration
- ▶ Controlled by ADA Admin
  - ▶ Create, Update, Activate/Deactivate



# Export Control - Concepts

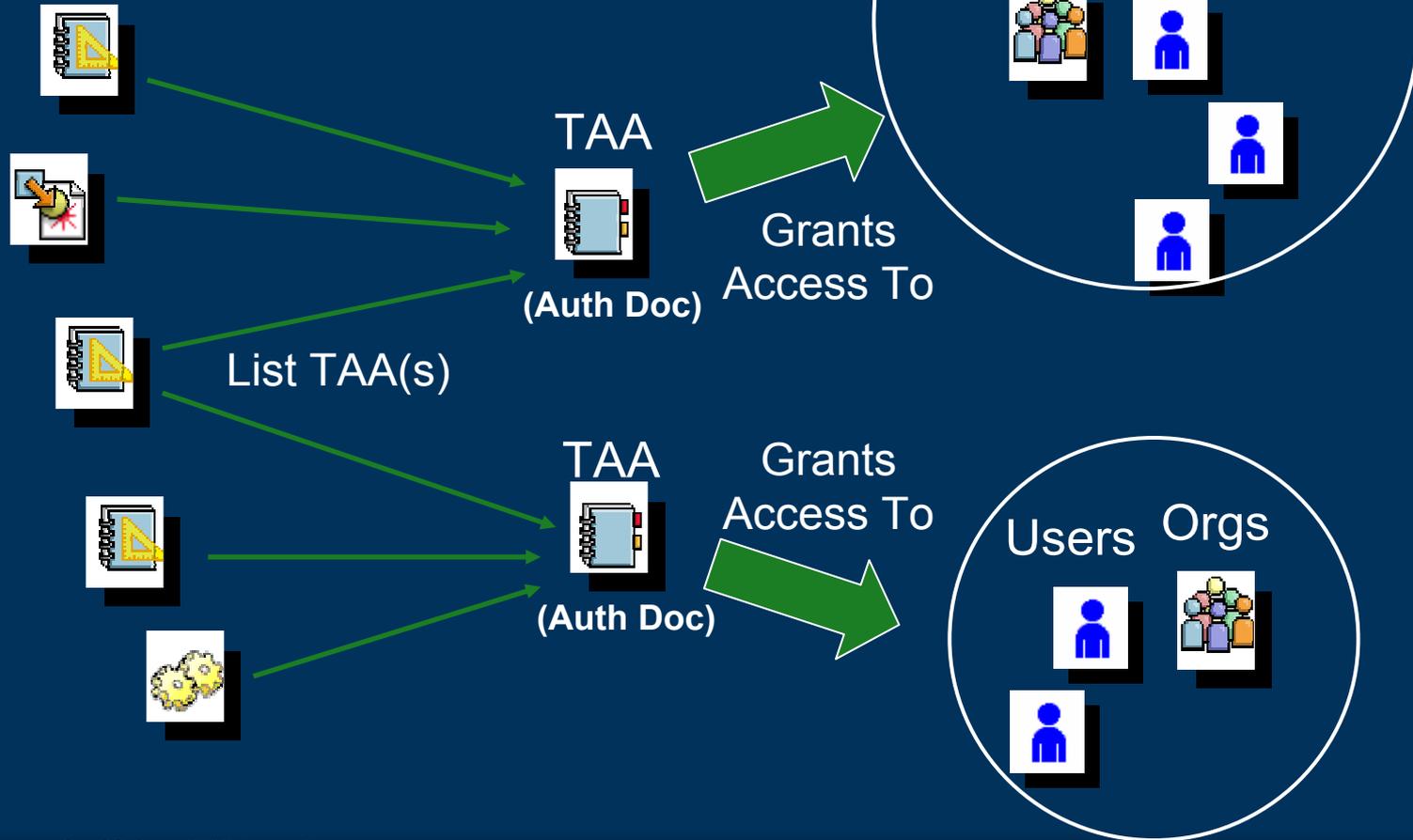




# ADA Control Model



Restricted  
Data





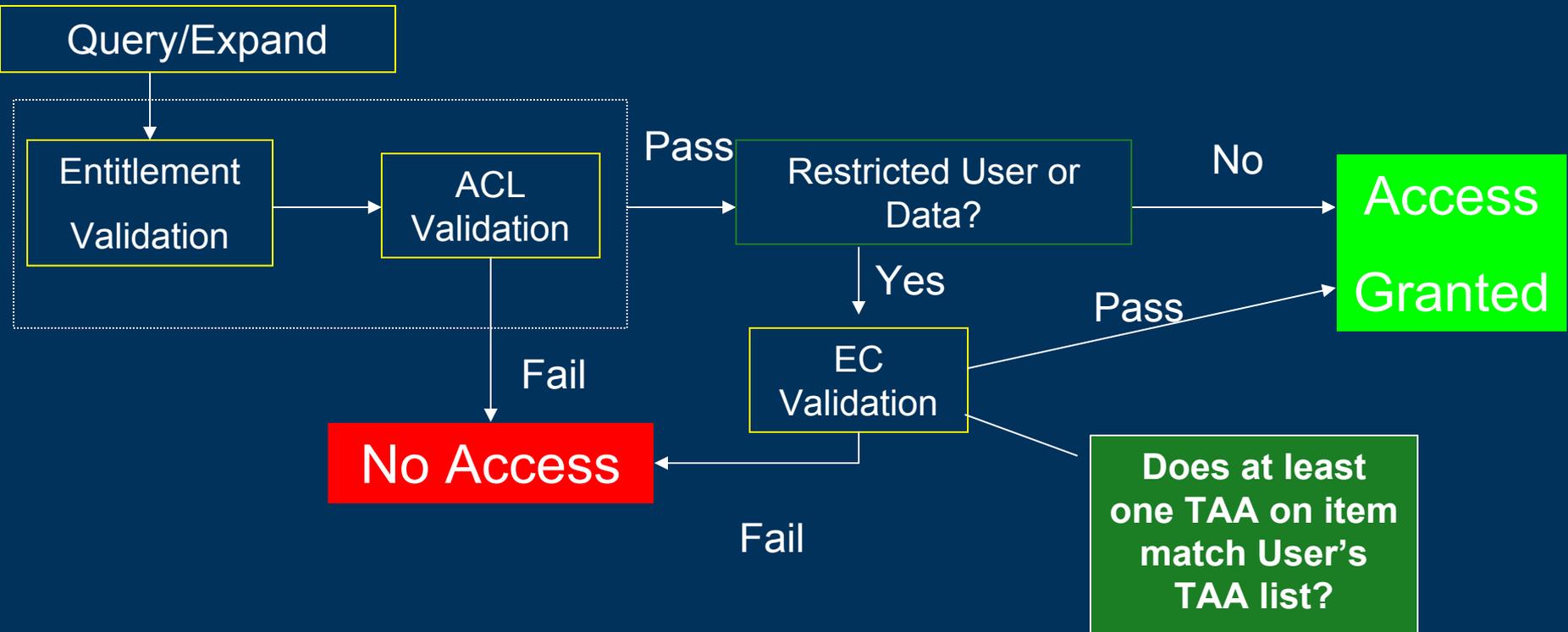
# Functional Area – Data Access



Per user session

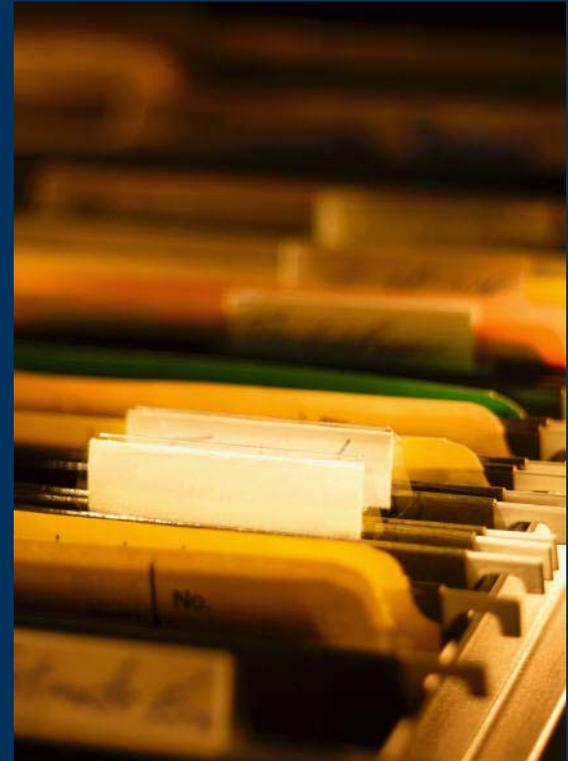


Per Query / Expand





- ▶ Teamcenter Enterprise 2005 User Activity Logging
  - ▶ Configurable Activity Log
    - ▶ What Events
    - ▶ What Users / Participants
    - ▶ What Objects
    - ▶ Log Content
  - ▶ XML Log File
    - ▶ Event / Event Filter
    - ▶ User
    - ▶ Date / Time
    - ▶ Defined Object Content
  - ▶ Log File Rotation controlled by
    - ▶ maximum permissible log file size
    - ▶ log rotation period
    - ▶ “expired log” condition during period of inactivity
    - ▶ forced rotation





# Authorized Data Access Availability



- ▶ Included in Teamcenter Enterprise ADS 4.0
- ▶ Field Implementation of Teamcenter Engineering in 8.1 leveraging AM rule tree exits
- ▶ Included in Teamcenter Enterprise 2005 core
- ▶ Continued in Teamcenter PLM 2007



# Summary



- ▶ Teamcenter provides a secure environment to share intellectual capital and collaborate with employees, suppliers, and customers
- ▶ Supports industry standards and best practices
- ▶ Lower administration costs associated with security
- ▶ Leverage corporate security infrastructure to help reduce cost and improve system security
- ▶ Comply with applicable laws and regulations



# Teamcenter Security Contact



Troy Banitt

Teamcenter Product Management

[Troy.banitt@ugs.com](mailto:Troy.banitt@ugs.com)



[ugs.com](http://ugs.com)