UGS CONNECTION

AMERICAS 2008

PLM WORLD®
The Voice of Siemens PLM Software Users Worldwide

Siemens PLM Software

SIEMENS

Product Data Security and Access Management

Dilip Agrawal
Security PLM Lead
Ford Motor Company
dagrawal@ford.com

Objective

Design a PLM security model that strengthen the enforcement of policies while providing a collaborative environment for vehicle development.

Must satisfy

- Corporate policy
- Government Regulation
- Business Requirement i.e. protect intellectual property

Key is to balance benefits of collaboration vs. administration of protecting data.

Applications of Core Security Concepts

UGS CONNECTION AMERICAS 2008

User Type

Ford users working on advance technology

Ford users working on Vehicle programs

Suppliers users

Joint Venture users

Ford Admin Users

Teamcenter and Enterprise Security

Data Type

- Joint Venture Data
- Supplier's data
- New Designs
- Class A Surface
- Carry over data
- Patent Pending Supplier data
- Research and Advance technologies for concept vehicle

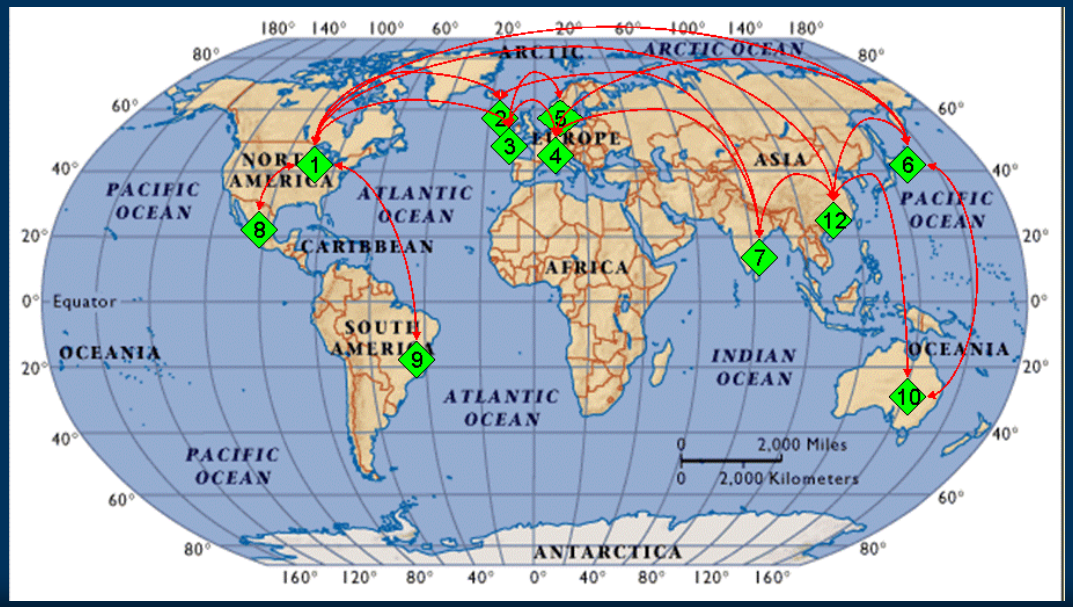
Topics

- Teamcenter Implementation overview at Ford
- Teamcenter Core Security Elements
  - Groups
  - Intellectual Property (IP) Classification
  - Projects
  - Dataset Security
  - Intellectual Property (IP) License
- Ford Proprietary Security Elements
  - Restriction List
  - User Access Registration System (UARS)
  - User Access Audit System
- Ford Security PLM Challenges
- Summary
- Q & A

Teamcenter Implementation at Ford

UGS CONNECTION AMERICAS 2008

- 11 TCe installations globally
- 13450 users, internal and external located globally
- 1000+ supplier Companies i.e. groups
- 100+ TB of Data Stored



Teamcenter Core Security Elements

- Groups
- Intellectual Property (IP) Classification
- Projects
- Dataset Security
- Intellectual Property (IP) License

Group Based Security

Type of Groups

General and Secure group

Business Need

To share the data among the functional activity. Regular group data is available for member of the group and also to non-member based on access rules. Secure group data is locked in the group and can not be accessed by users outside the group.

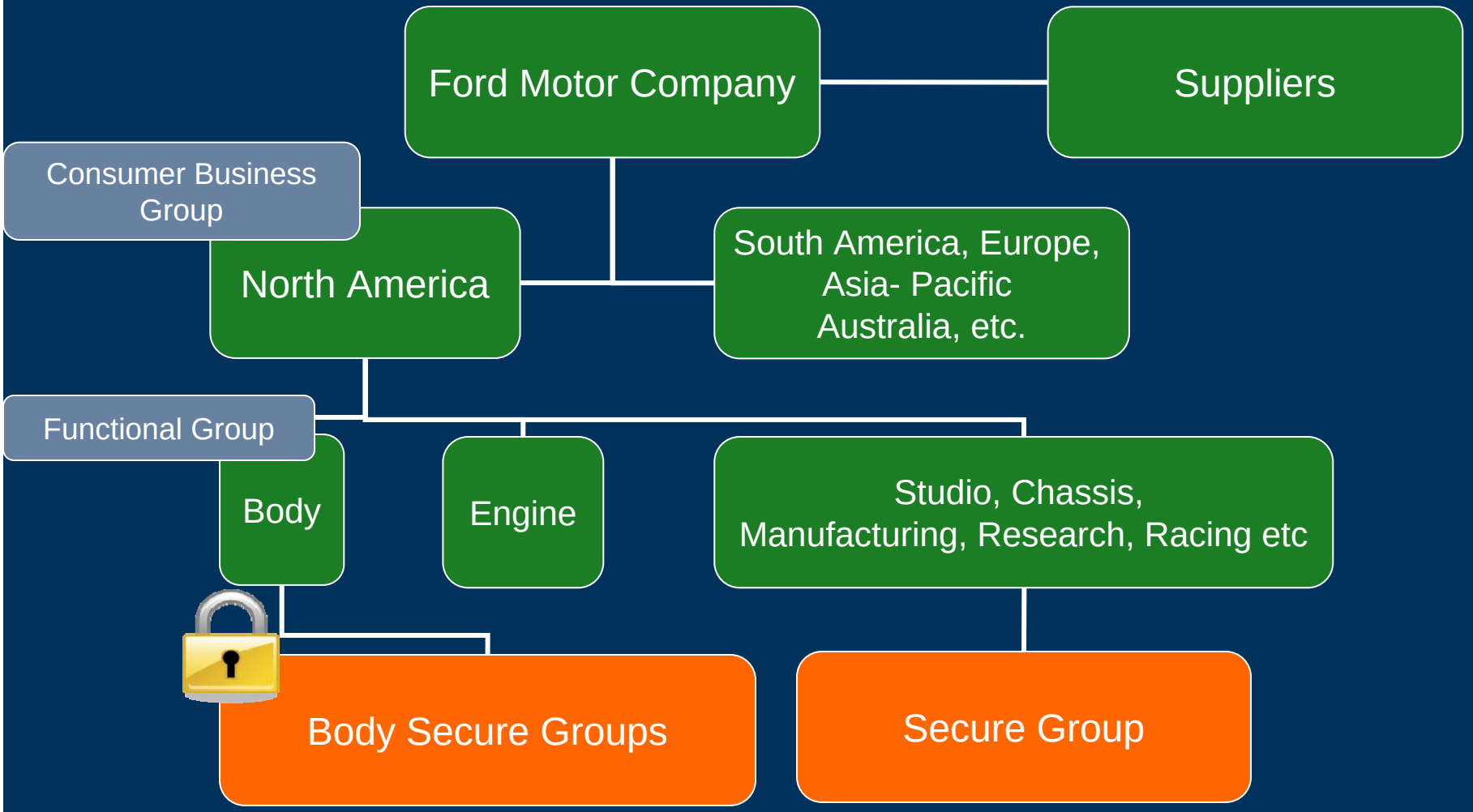
Functionality

Group based security, controls read and edit access. Provide read access to all member of the group and edit access to owning users.

Organization Structure

Groups are defined at high level functional activities rather then at department level to reduce the impact of re-organization.

Group Structure at Ford



Ford Data Classification Overview

According to Ford IT Policy Manual, data is classified as Secret, Confidential or Proprietary. Data classification can change over the lifecycle from one category to another. Security requirements regarding each of these data classification values are as follows:

- **Secret** – Only members of owning groups within Ford and all other users working on the same program have READ access.
- **Confidential** – All Ford internal users have READ access. All supplier or external users belonging to the same project as the data have READ access.
- **Proprietary** – All users have READ access irrespective or program membership.

READ privileges are granted based on users association to groups and roles and the data classification and project assignment for data.

IP Classification Concept

IP classification applies to data and specifies the clearance level required for users to access the data.

When users attempt to access classified data in Teamcenter, their clearance level is evaluated against the classification of the object based on Access Manager rules, and if the clearance level is equal to or greater than the classification on the object, access is granted.

Example

Has Class (Item)

Has IP Classification (Confidential) -> Confidential DC Privileges

Has IP Classification (Proprietary) -> Proprietary DC Privileges

Has IP Classification (Secret) -> Secret DC Privileges

IP Classification Concept Continued..

IP_level_list_ordering Site Preference

Defines a list of IP classification values and clearance levels that are assigned to data objects and users for IP access evaluation. Access Manager compares these values to determine user access rights to the object

- **Proprietary**
- **Confidential**
- **Secret**

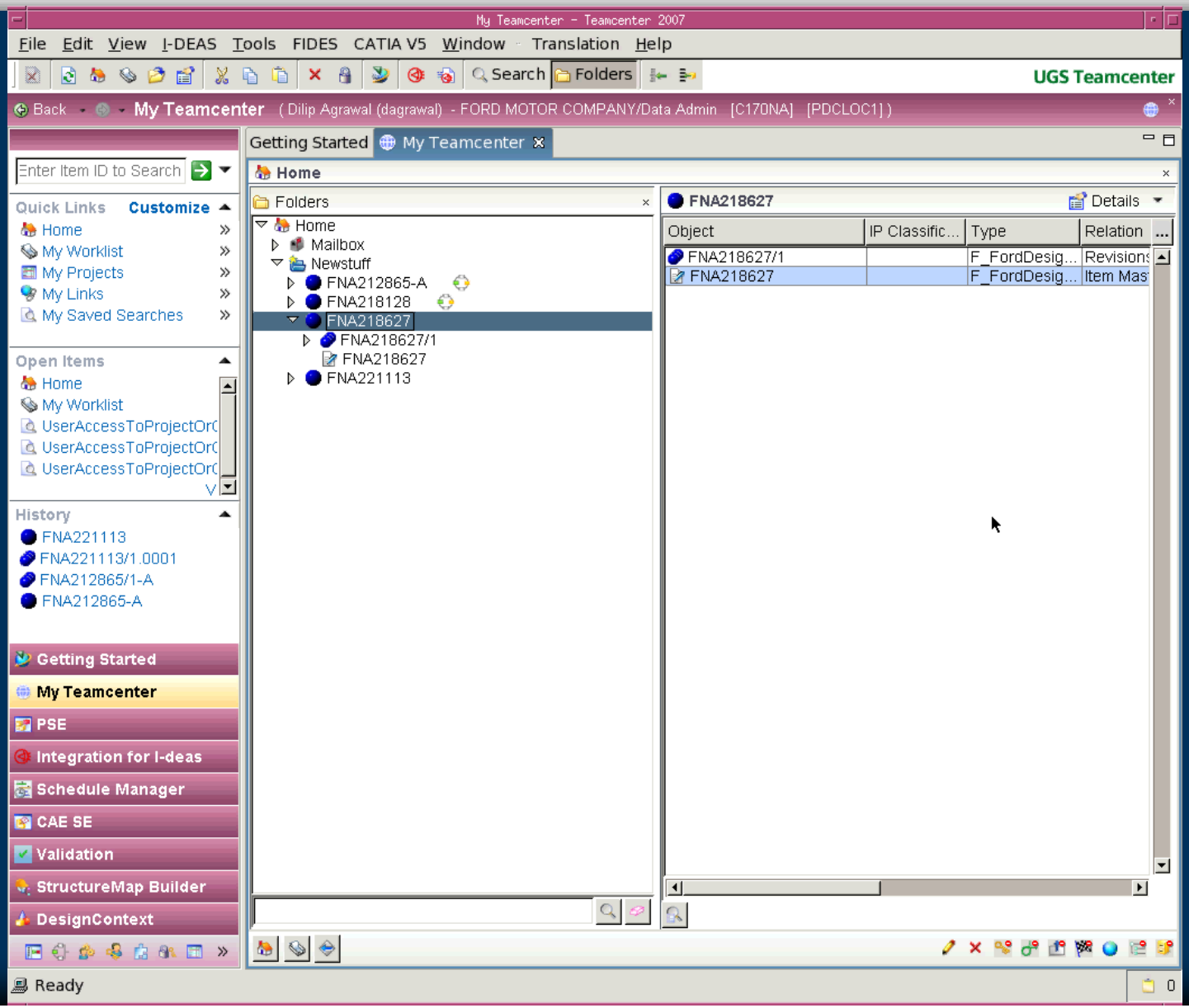
IP Classification Value Propagation

COTS propagation rules can be configured to cascade the IP Classification value from Item to its Revisions and Revisions to their attachments.

Behavior:

- If IP Classification value is set on Item object, system will automatically cascades the IP Classification value to its Item Revisions
- Based on the relationship types that are configured via COTS propagation rules, system will automatically cascades the IP Classification value from Item Revision to its attachments (Ex. Forms, Datasets, etc.)

IP Classification Demo



Project Based Security

UGS CONNECTION AMERICAS 2008

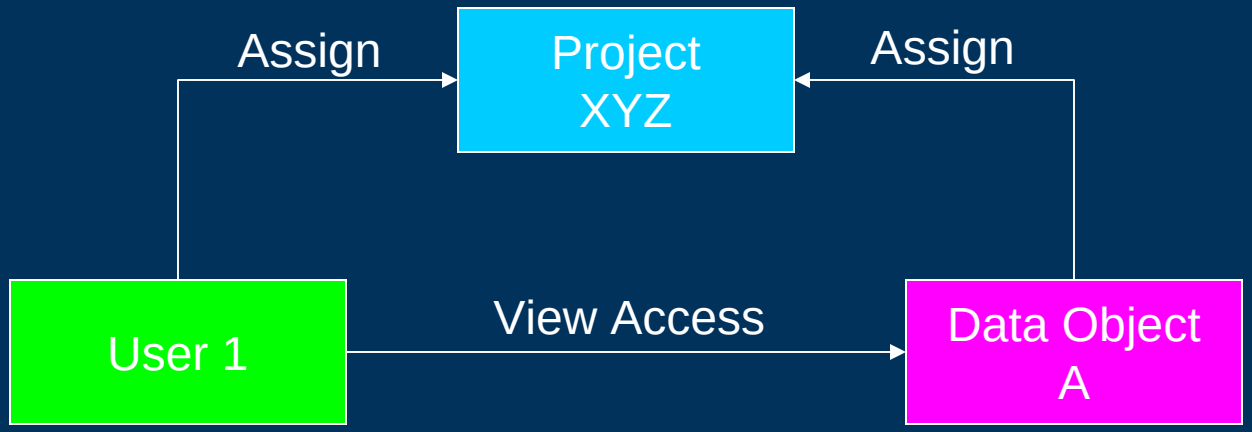
Business Need

To share and control the data among users working on a vehicle program across functional groups and suppliers.

Functionality

TCe Projects are an COTS concept that allows for the assignment of Users and Data Objects to a Project or Projects. By comparing the User and Data Object assignments, Project based security controls view access to Data objects.

Project Based Security



Advantage

- Propagation rules
- Cascade project assignment to Vehicle structure
- Multiple projects can be assigned.

Dataset Security

Business Need

Apply security on dataset objects which contain sensitive data and can be accessed directly i.e. without going through item revisions. It is important to note that dataset security is not configured on all dataset types to reduce load on server and improve performance.

Dataset security is achieved by configuring Teamcenter to:

- Cascade core security elements from parent item revision to attached datasets based on relationships
- AM rule tree evaluate the permission for specified dataset types during access

Advantage

Datasets can be shared via PLM XML and session files with required security controls.

Person-to-Person Sharing using IP Licenses

UGS CONNECTION AMERICAS 2008

Business Need

Sharing of a single piece or collection of data to identified individual. Data sharing with pre-sourced suppliers (Request for Quote).

Functionality

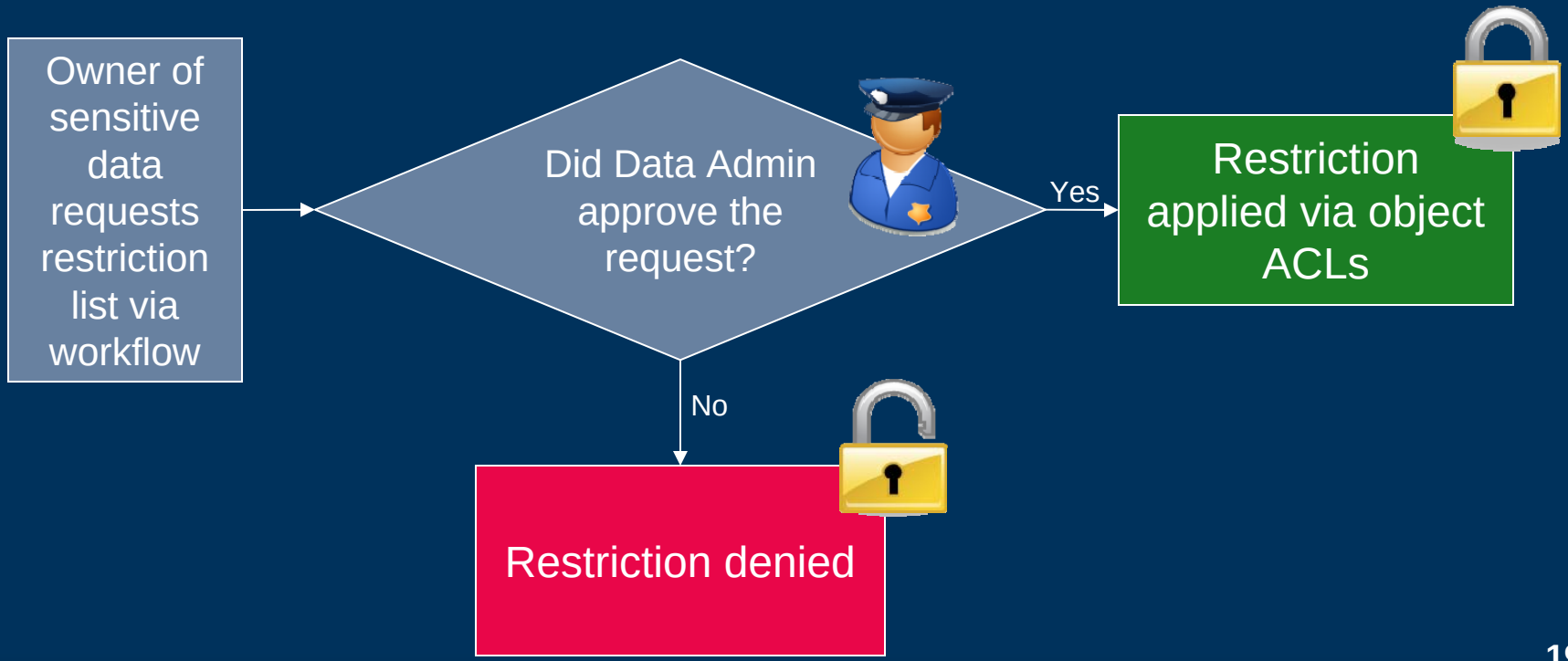
IP licenses grant discretionary access to data for a specific user or group for a specific period of time. P2P allows sharing a collection of objects while eliminating exposure of the entire program's data. It also provides ability to track access to pre-sourced suppliers and turnoff when needed.

Ford Proprietary Security Elements

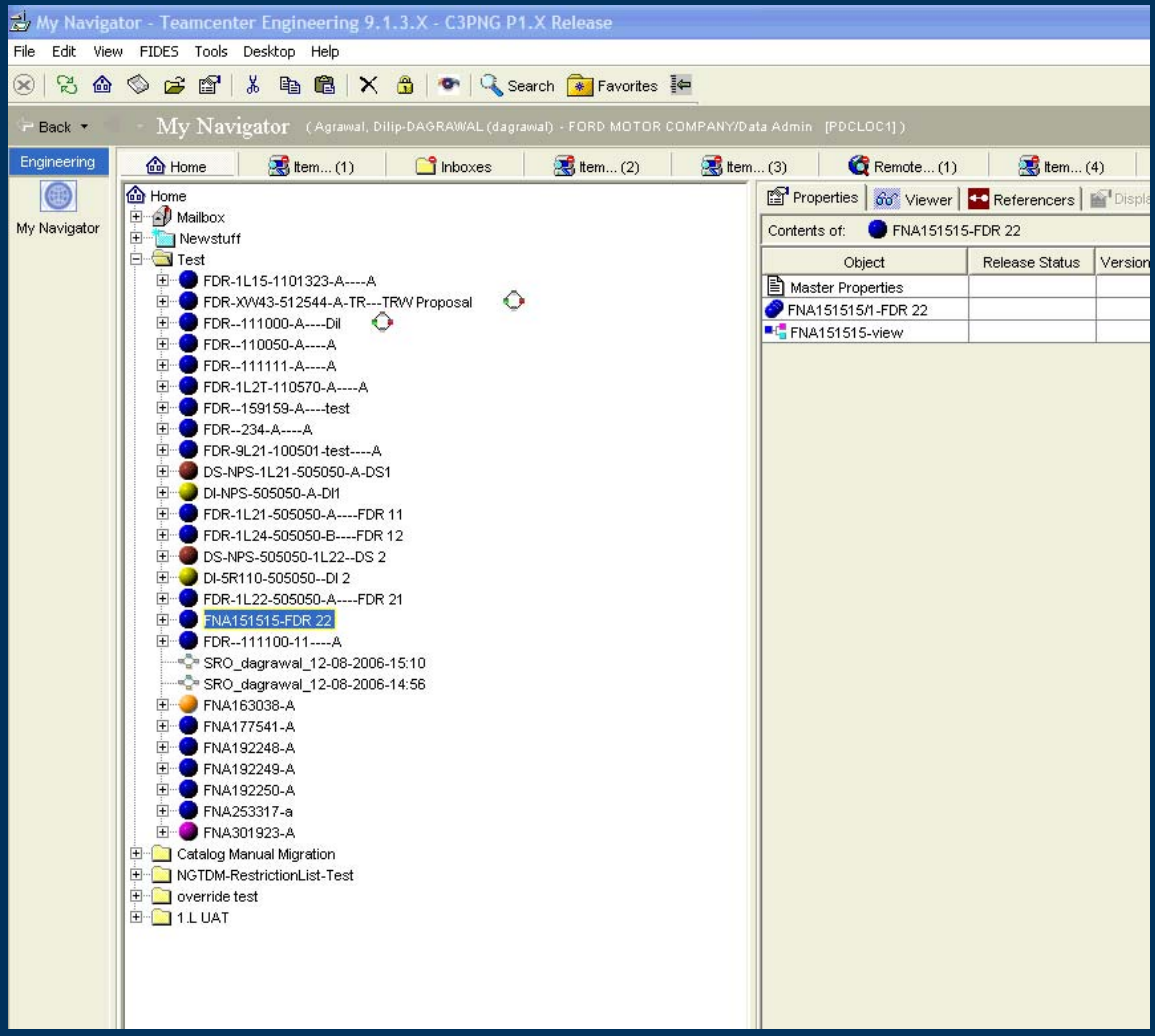
- Restriction List
- User Access Registration System (UARS)
- User Access Management System (UAMS)

Restriction Lists

Restriction list protect secret and patent pending data from suppliers working on the same vehicle program. It override access granted by other mechanism and apply restriction to all users for specified supplier companies. Restriction must be approved by Ford Engineering via Teamcenter workflow. Supplier can easily request restriction to be applied to sensitive data. Ford admin can review and approve the requests.



Restriction List Demo



Ford Restriction List Vs. Teamcenter Exclude License

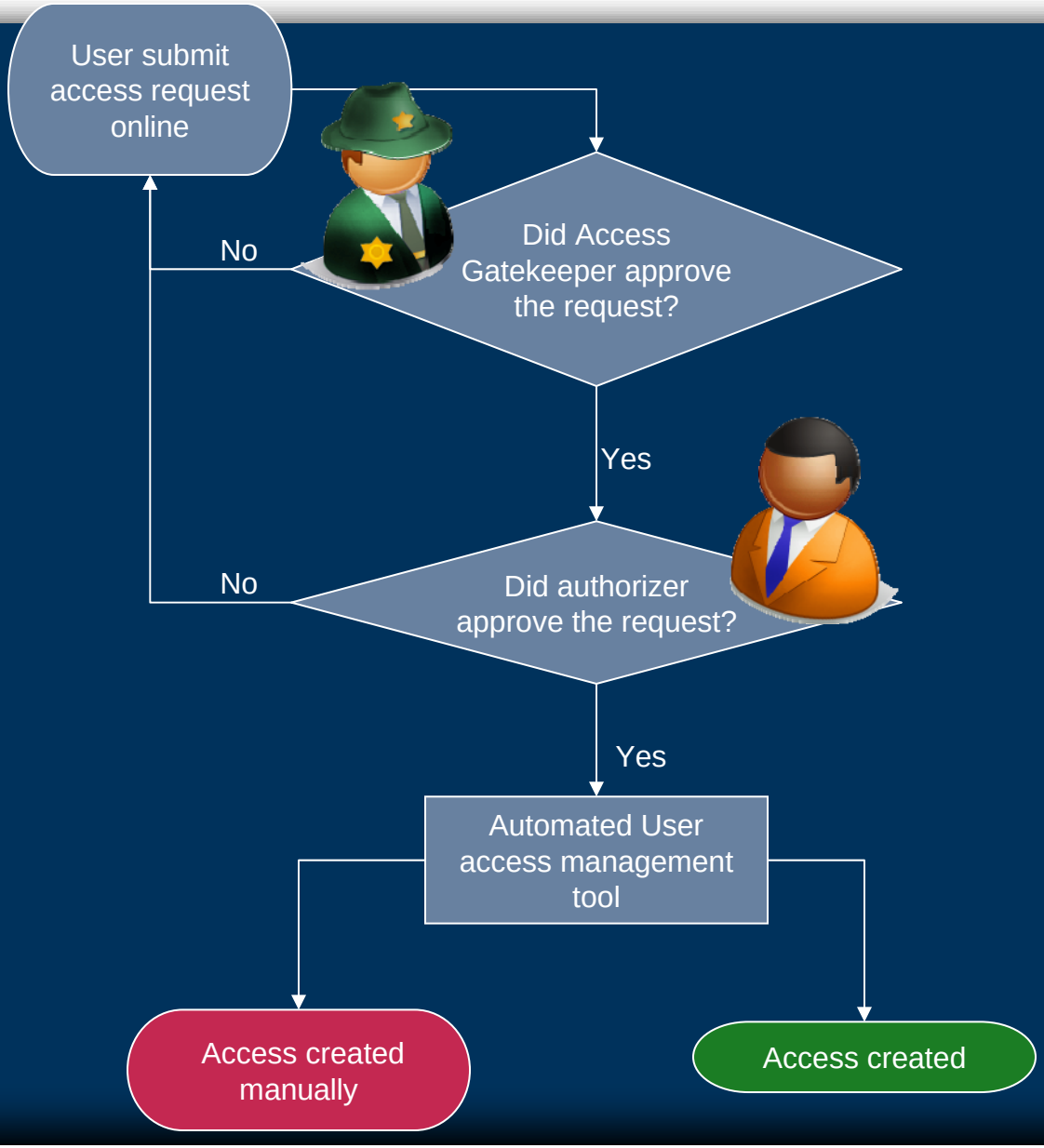
Restriction List	Exclude License
▸Available in PSE, MSE and My Teamcenter.	▸Only available in My Teamcenter
▸Data Admin or other roles can be configured to approve the restriction	▸IP Admin in DBA group is needed to create/update/delete licenses
▸Workflow based approval	▸Non workflow based
▸Sub group can be restricted	▸Only applied to users and top level group
▸Easily find out who applied the restriction	▸No tracking available.
▸No Expiration date	▸Has a expiration date

User Access Management System (UAMS) Concept

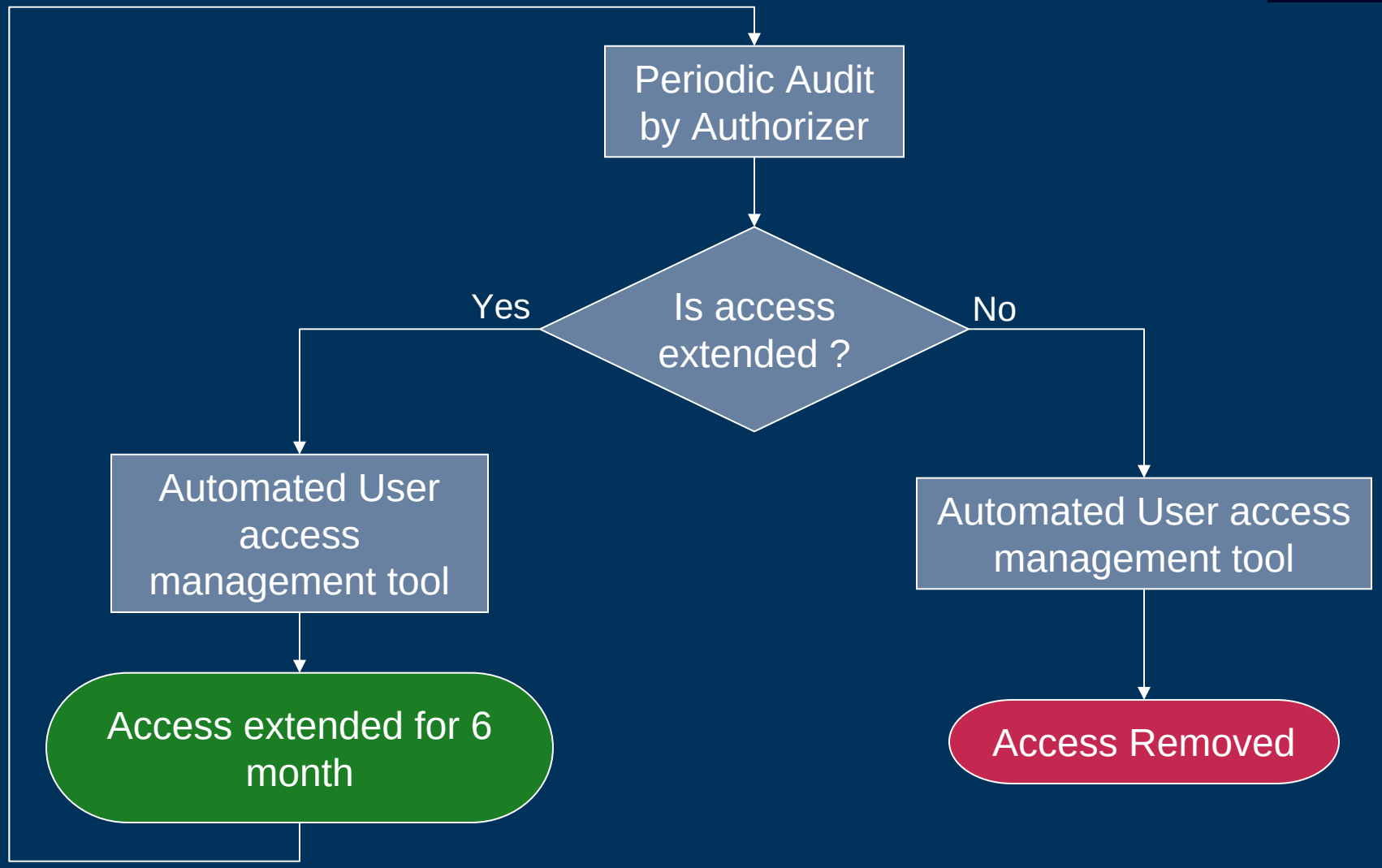
At Ford Motor Company, we have 13,450 user with 178,000 permissions in Teamcenter. These permissions are authorized by user's supervisors or access gatekeeper located globally.

Automation of user access management process was required to improve user administration cost and reduce access granting/removing time. Significant tangible cost savings in form of license fee by removing inactive users and reduced user administration cost was achieved. Further UAMS adds intangible cost saving because of enhanced data security.

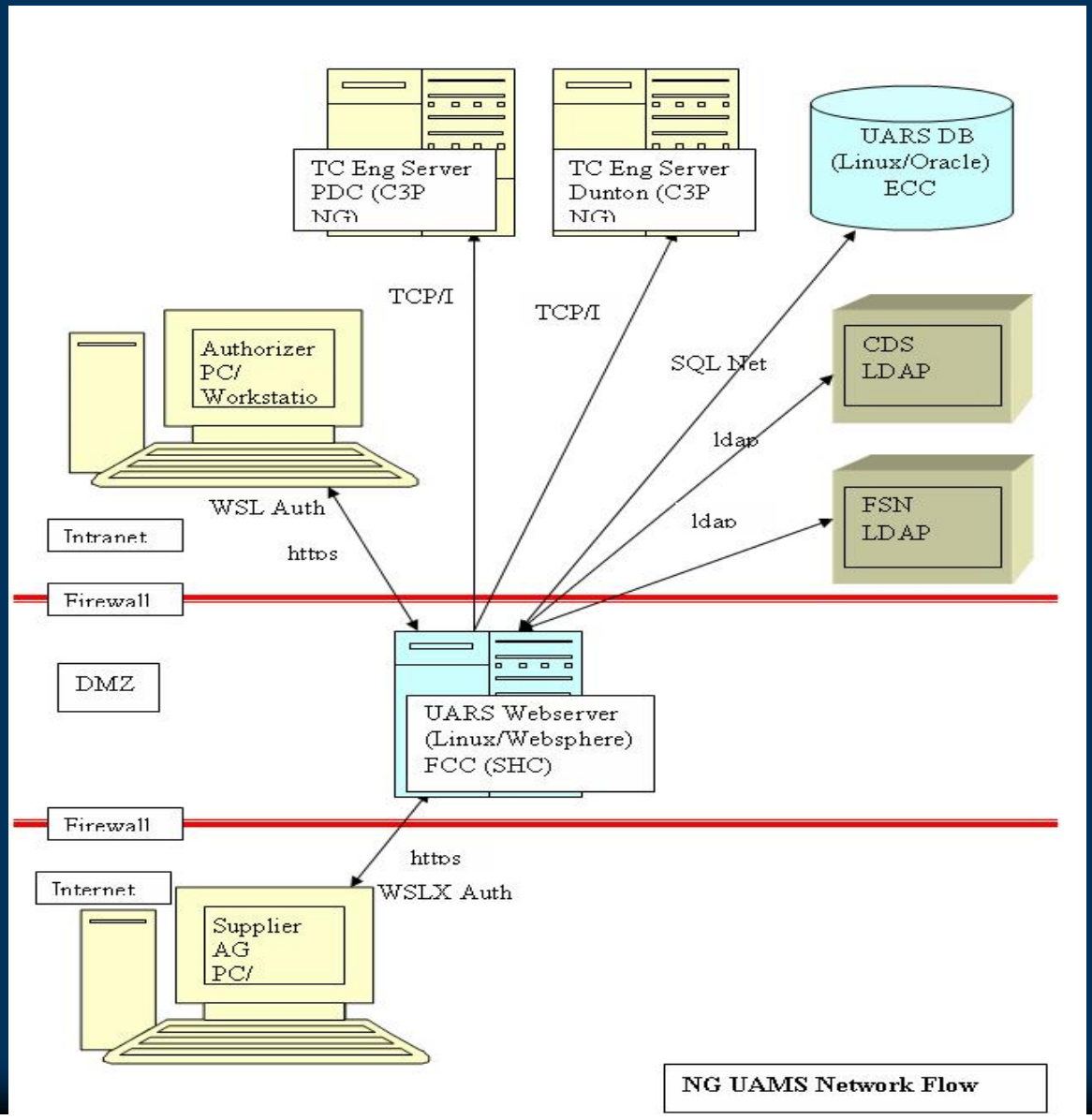
User Access Registration System Process Flow

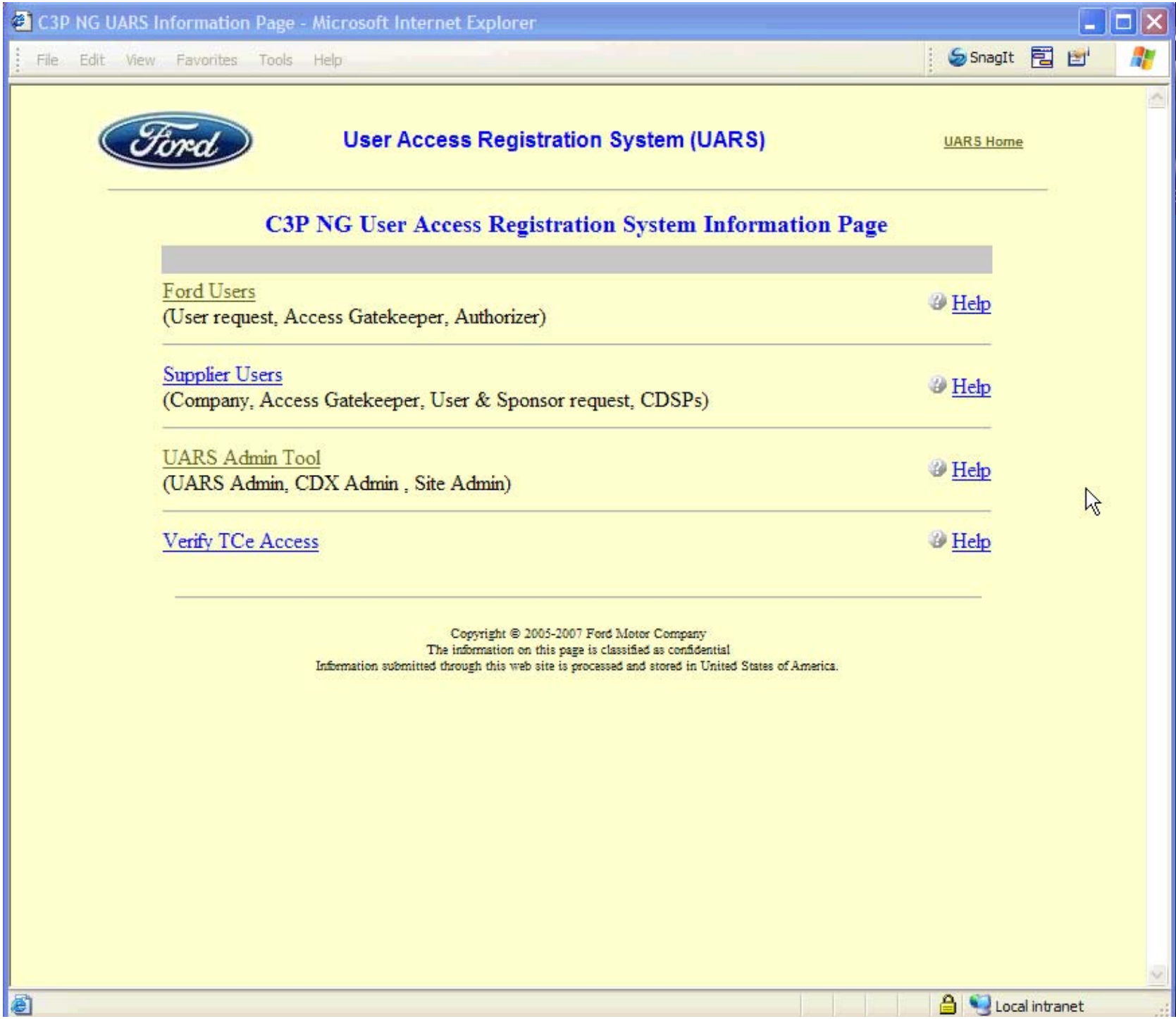


User Access Management System Process Flow



UAMS Architecture Diagram




C3P NG UARS Information Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SnagIt
User Access Registration System (UARS)
UARS Home
C3P NG User Access Registration System Information Page
Ford Users
(User request, Access Gatekeeper, Authorizer)
Help
Supplier Users
(Company, Access Gatekeeper, User & Sponsor request, CDSPs)
Help
UARS Admin Tool
(UARS Admin, CDX Admin , Site Admin)
Help
Verify TCe Access
Help
Copyright © 2005-2007 Ford Motor Company
The information on this page is classified as confidential
Information submitted through this web site is processed and stored in United States of America.
Local intranet

Ford UAMS Vs. Teamcenter External Authorization

UGS CONNECTION AMERICAS 2008

UAMS

- Support access management for project teams
- Can be linked to multiple LDAP server

External Authorization

- Only group and roles can be managed
- Can be only linked to one LDAP server

Ford Security PLM Challenges

- Joint Venture Security:
  - Sometimes it may be best to build a site at joint venture, however multisite does not support need to know requirement. Custom security solution are required to achieve the desired JV security in multisite scenario. This increase cost and complexity.
- Data Archival:
  - Teamcenter does not offers any strong functionality to support data archival policies. Ability to set up rule based archival is needed, so rules can be setup to archive the data based on condition met at the end of life cycle.
- Authorized Data Access
  - License creation/update is only available in organization application, hence requires DBA access to manage license. Also sub groups can not be included in license to grant/remove access.
- LDAP Synchronization or External Authorization:
  - LDAP Synchronization can not be bind to more than one directory server. Ford has separate directory for internal and external users. Also project access can not be managed via external authorization functionality.

Summary - How it all fit together

Security Elements	Function
IP License	Grant Access
Exclude License	Restrict Access
Secure group	Restrict / Grant Access
Restriction list	Restrict Access
Project Based Security	Grant Access
Data classification	Restrict / Grant Access
Group Access	Restrict / Grant Access

Q & A

UGS CONNECTION

AMERICAS 2008

PLM WORLD®
The Voice of Siemens PLM Software Users Worldwide

Siemens PLM Software

SIEMENS

Ford Security PLM

Dilip Agrawal
dagrawal@ford.com