

Teamcenter Enterprise Fulfilled the Company security demands

Nissim Cohen

H.A.A.K Technologies Ltd.

(Subcontractor of McKit System Ltd. – The exclusive distributor in Israel of UGS PLM Ltd.)

haak@inter.net.il

+972-4-8769243

Outline

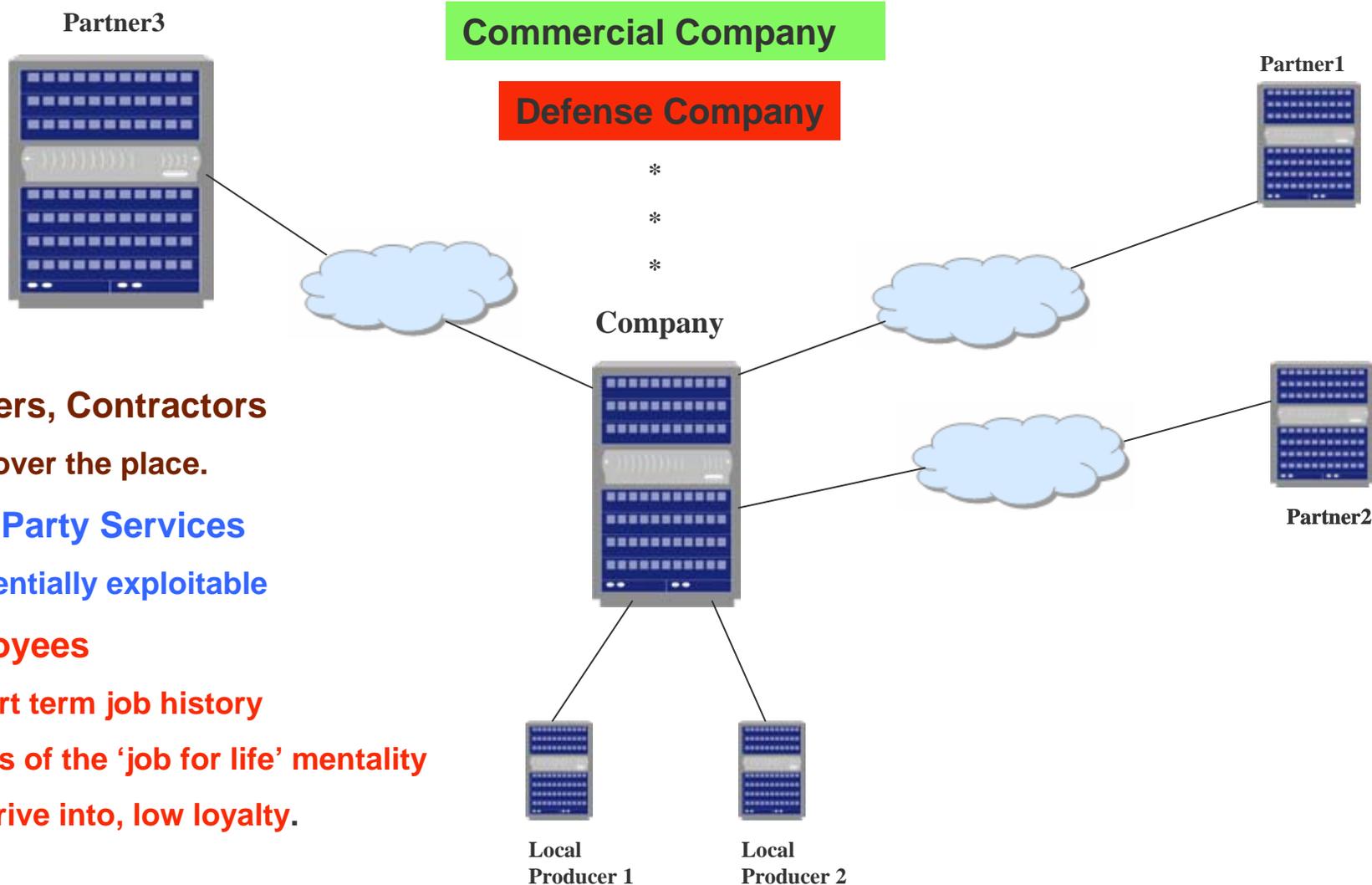
- **Motivations and Goals**
- **Company concern**
- **Organization and Project**
- **User and roles**
- **Partners**
- **Security & Protection**
- **Evaluation**
- **Related Work**
- **Conclusion**

- **Why fulfill the Company security demands?**
 - Expand business opportunities without stripping secured data by:
 - **Outsourcing**
 - Reduce manufacturing cost**
 - Share information with partners.
 - Extendability of the business volume**
- **What is challenging?**
 - Openness
 - Sharing
 - Mutual isolation, security and protection

Goals

- To build a value-added secure application service, based on a shared infrastructure, achieving:
 - **On-demand creation and provisioning**
 - **Privacy**
 - **Isolation**
 - **Protection**
 - **Reports**
 - **Accountability**

Company concern



- Partners, Contractors

- All over the place.

- Third Party Services

- potentially exploitable

- Employees

- short term job history

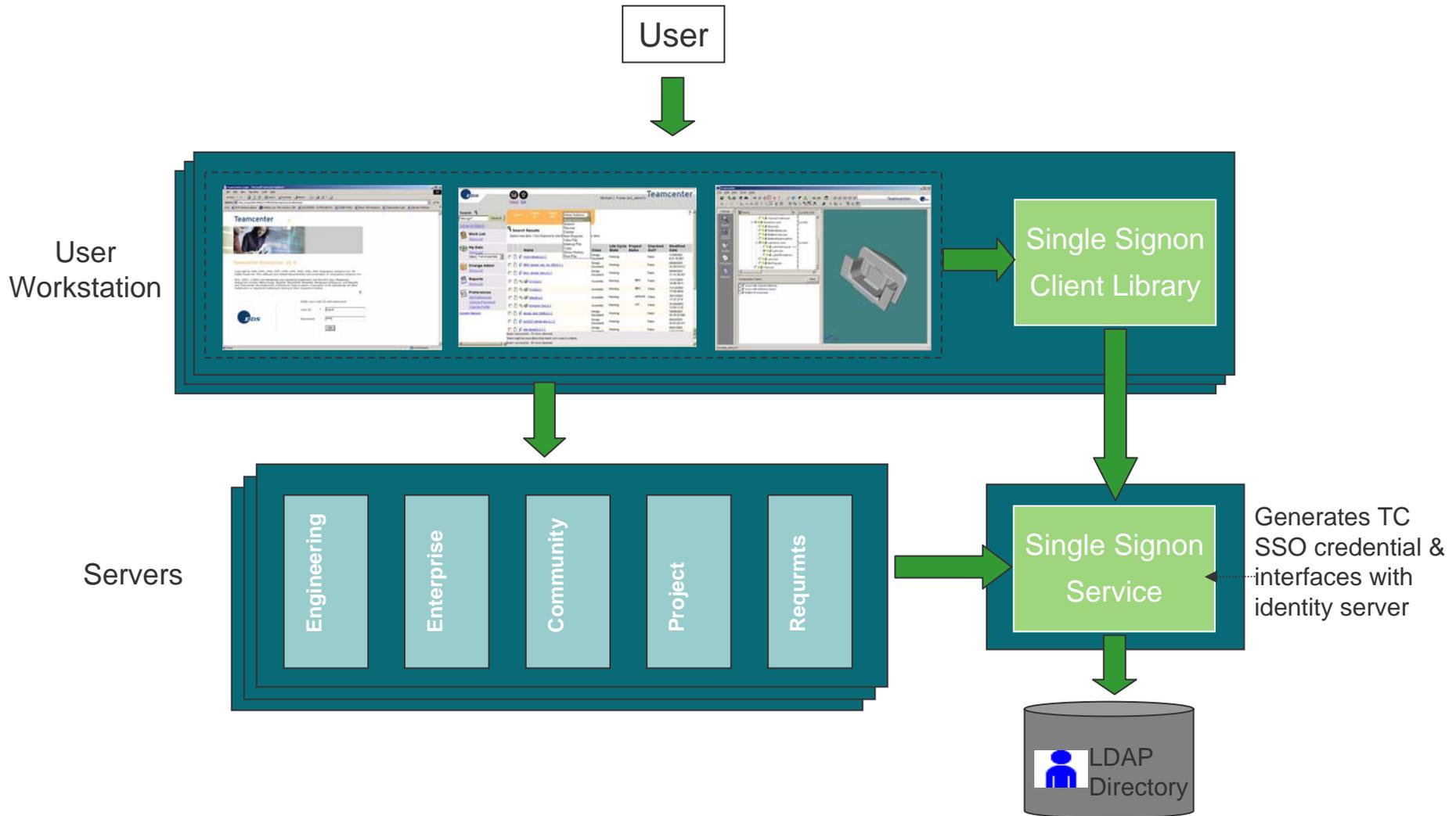
- Loss of the 'job for life' mentality

- drive into, low loyalty.

Company Security Demands

- **Single Signon(SSO)**
- **Access restriction**
- **Access authorization**
- **Application disable/hide features**
- **Organizations/Projects Isolation**
- **Compartment**
 -
 -

Single Signon(SSO)



Organizations and Projects

- **Organization**
 - A company
 - A company division
 - An external partner or producer.
- **Project**
 - A framework for a business undertaking with fixed goals to achieve with given resource:
 - A product
 - A product Major assembly
(Secured organizations)

User is restricted to access only the information that necessary to do his job, with that access defined by the role the user plays in the company.

—

- **External producer**
 - He is provided with the needed information to produce the Work Ordered by the company.
- **A contract Partner.**
 - He is provided with the needed information to manufacture a product assembly, based on the commercial contract agreement.

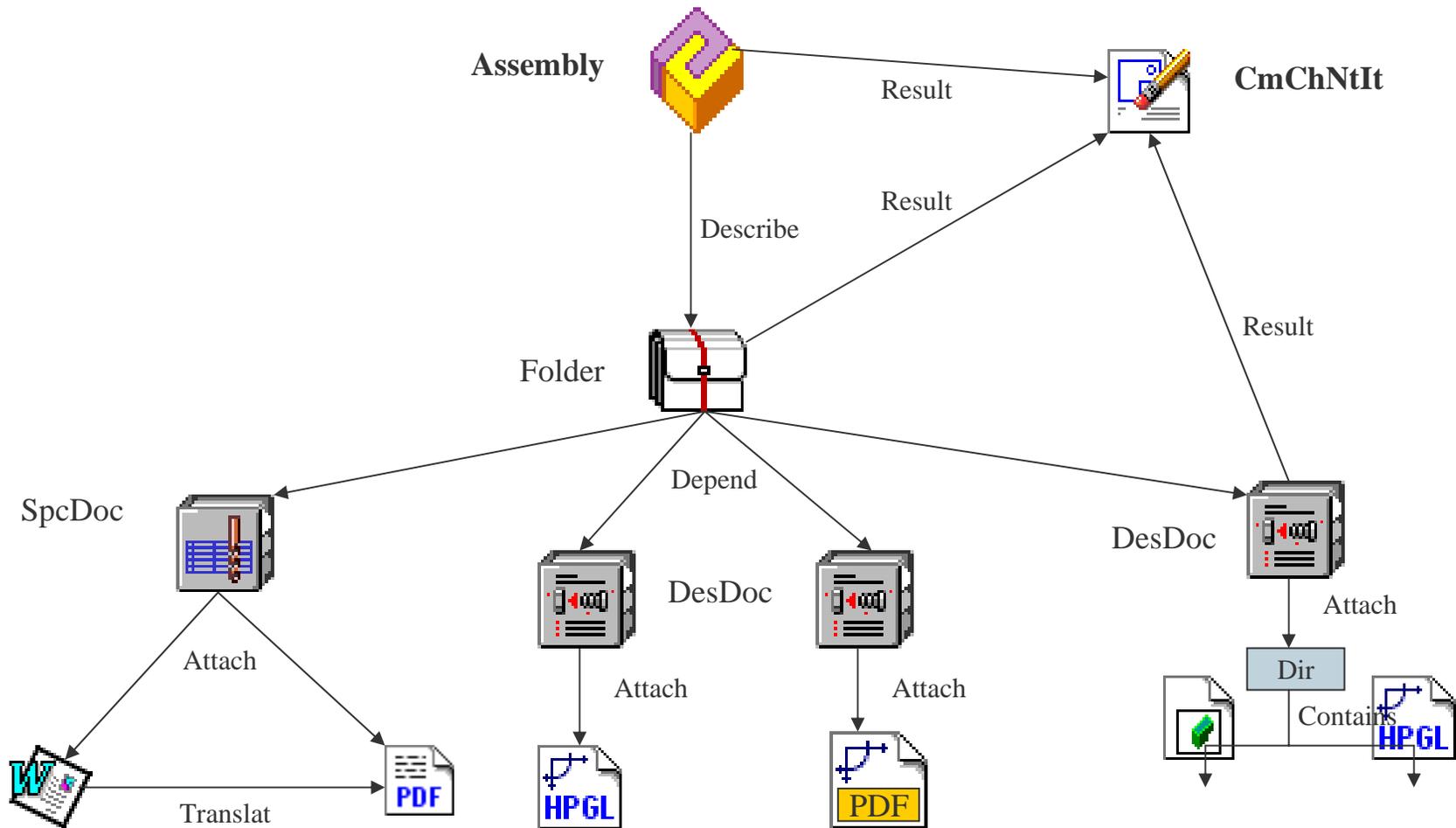
Teamcenter Enterprise

- . Provides Administration Objects as conditions, message accesses rules , role assignment, users and groups, to build the security infrastructure.**
- . The system restricts users to access files attached to Business Items using the Active Control List (ACL).**

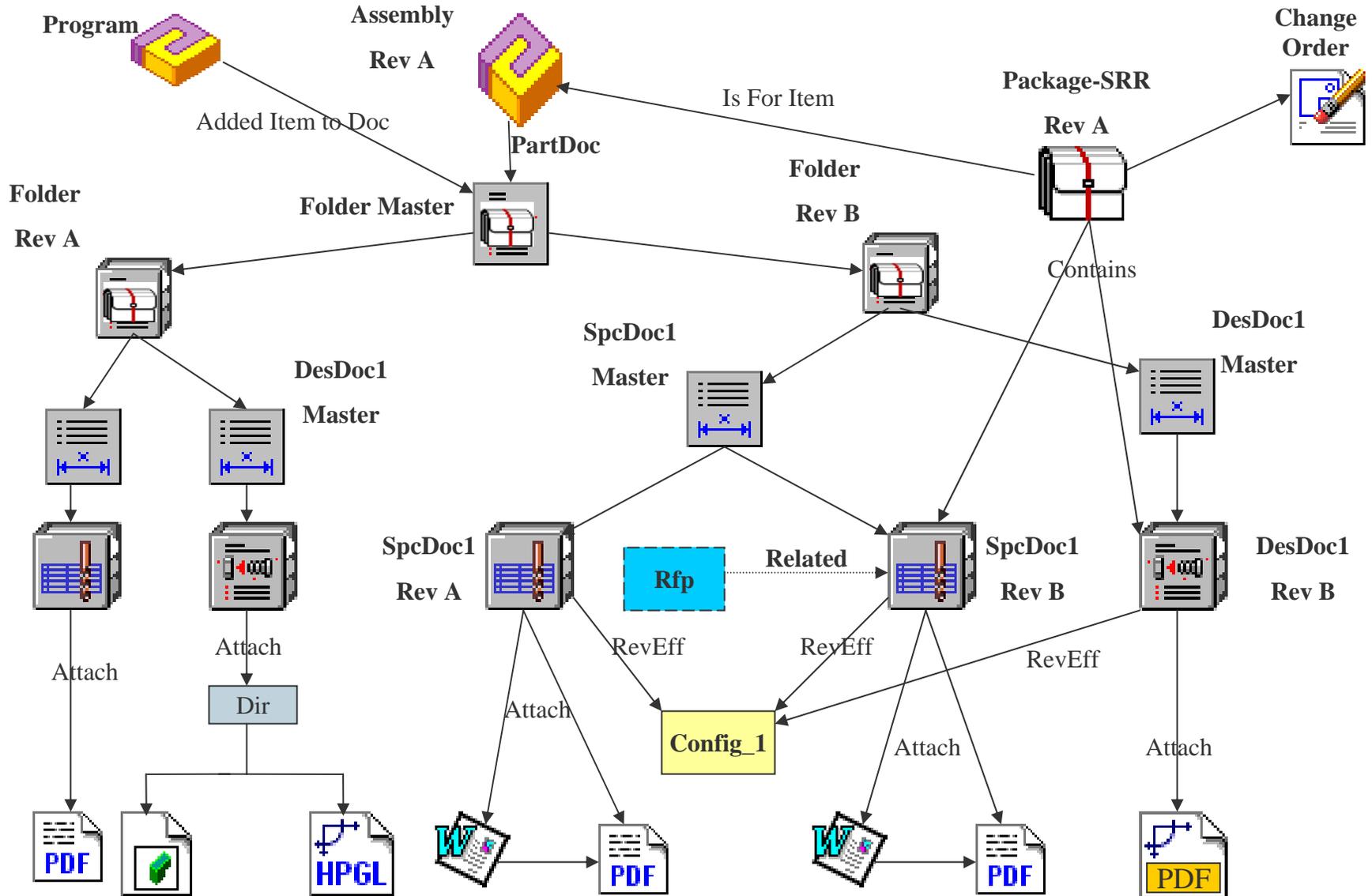
Teamcenter Enterprise Objects

- **Admin objects**
- **Process objects**
- **Configuration objects,**
- **Business items objects**
- **Data items objects**
- **Dynamic dialogs objects.**
- .

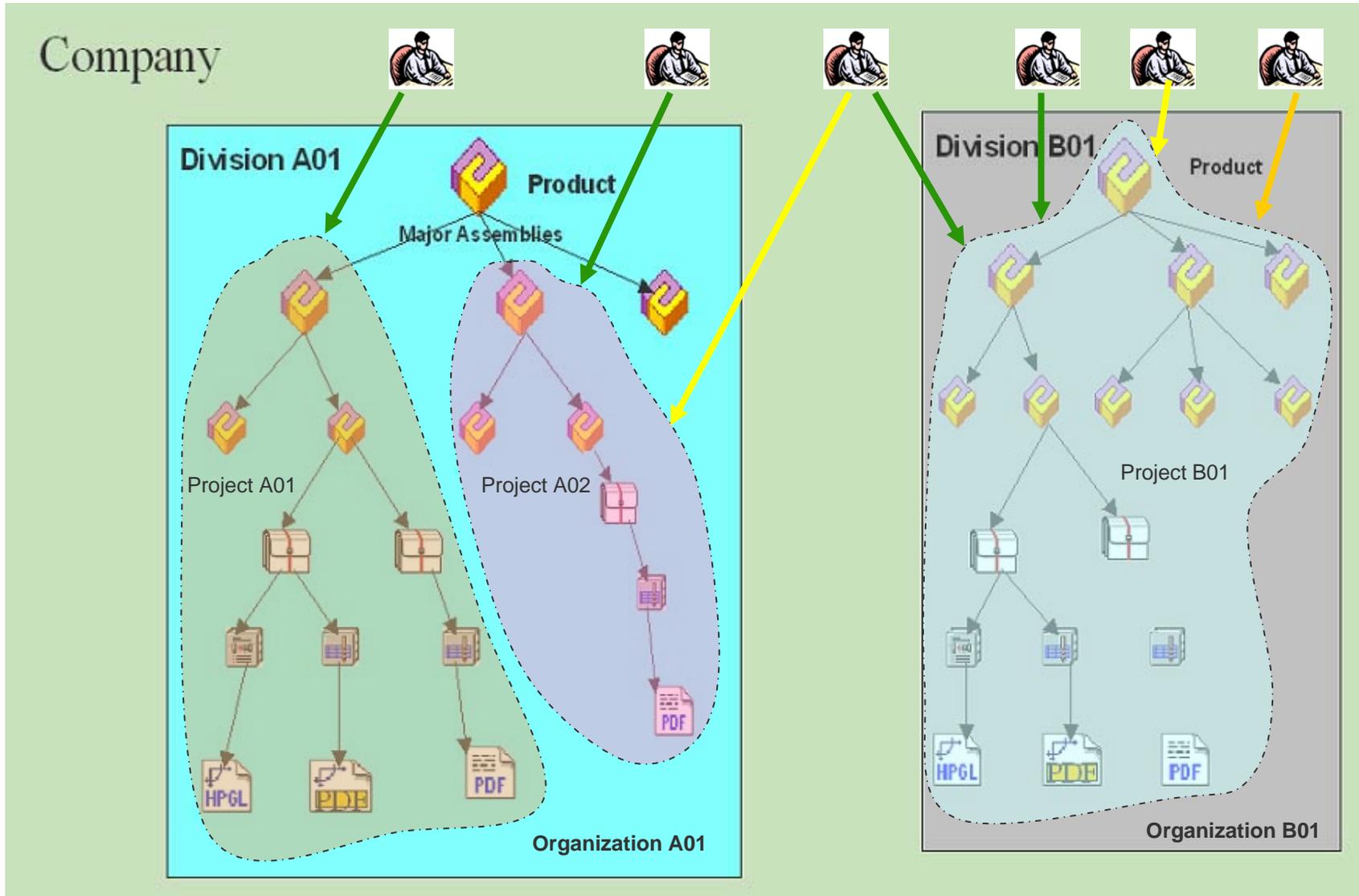
Typical Objects Relation



Typical Structure Document Objects Relation



Typical Security demand



Teamcenter Enterprise Rules

- **Default system access is: Not Allowed.**
- **Rules , accessing to user, group or role, to a defined activity, defined by a message or a group of messages, with :**
Message Access (MsgAcc), based on a condition

Evaluation

- **Actions (e.g. CheckIn, Submit etc.) are defined by the role the user plays in the company.**
(i.g. Configuration managers, Reviewers)
- **Allow Query Access to Business Items.**
- **Restricted users from performing Actions to BusItems, based on Organization, Project and Security**
-
- **Restricted users accessing to DataItems, based on Project and Security level (i.g. secret and up ..)**
- **Restrict users to limited projects on all security levels.**

Solving security with provided tools

- **Security is built with MsgAcc rules and Conditions.**
- **Actions defined by the role and Access to Business Items, is ok as long we keep the amount of MsgAcc rules and Conditions to a reasonable number.**
- **Rules are not fully indexed. Raising the number of MsgAcc rules and Conditions, may affect system performance.**
- **Difficult to maintain an analyze problems.**

customize security solution

- **The solution should not affect the performance, or the Integrity of the system**
- **The customization security solution is in addition to the Teamcenter Enterprise Rules. .**
- **ACL is the carrier using ValidateACLForUsr message**
- **Compartment of user access permission is done, by single indexed search of user, Organization and project**
- **Bypass query permission check, based on project and security**
- Accessing level is based on Dialog action

Typical customer security demand

Typical customer security demand

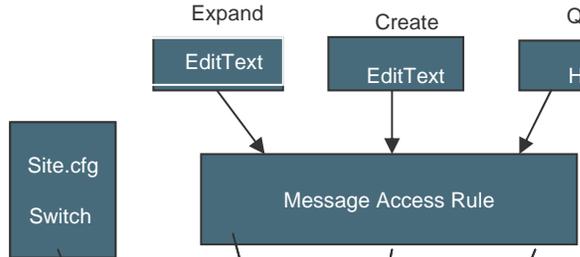
Action	Configuration Manager.			Designer			Reviewer			Viewer		
	Di	RI	Bi	Di	RI	Bi	Di	RI	Bi	Di	RI	Bi
	Query	v	v	v	v	v	v	v	v	v	v	v
Create	v	v										
CheckIn				v		v						
CheckOut							v					
Submit				v		v						
Revise	v	v	v									
Delete	v	v	v									

Security Action Table

Action	AccessLvl		
	Di	RI	Bi
	File	Relation	BusItem
Query	00	00	00
Create	10	10	10
CheckIn	20		20
CheckOut	30		30
Submit	40		40
Revise	50		50
Delete	70	70	70

Related Work

Dialogs Action



Usr Table

Project Table

Min.Security
Security

Security Level Table

Level	Security
20	TopSecrete
30	Secrete
40	Clasify
50	UnClasify

Override Vanila messages
 rulesAllowed = 1
 ACLAllowed = 0

File:ValidateACLForUsr
 BusItem:ValidateACLForUsr
 Relation:ValidateACLForUsr

Access permition Table

AccessLvl	OrgNm	Project	User
000000	orgNm1	prj1	usr1
707070	orgNm2	prj1	usr1

rulesAllowed = 1
 ACLAllowed = 1 or 0

Security Action Table

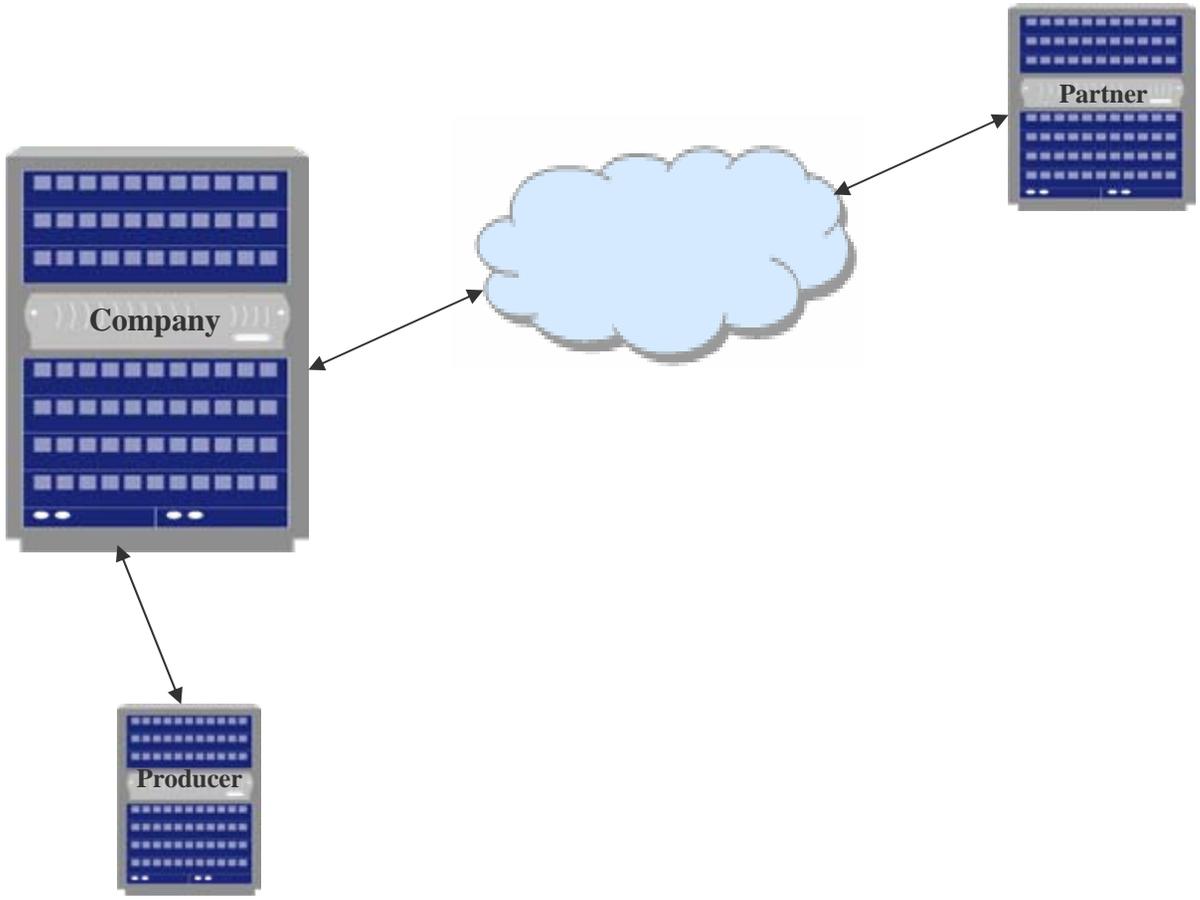
Action	AccessLvl		
	xx	yy	zz
	File	Relation	BusItem
Query	00	00	00
Create	10	10	10
CheckIn	20		20
CheckOut	30		30
Submit			40
Revise			50
Delete	70	70	70

Legend

New	Exists - Cust.
Exists-Vanila	

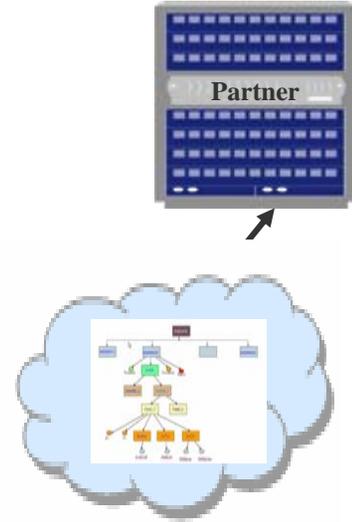
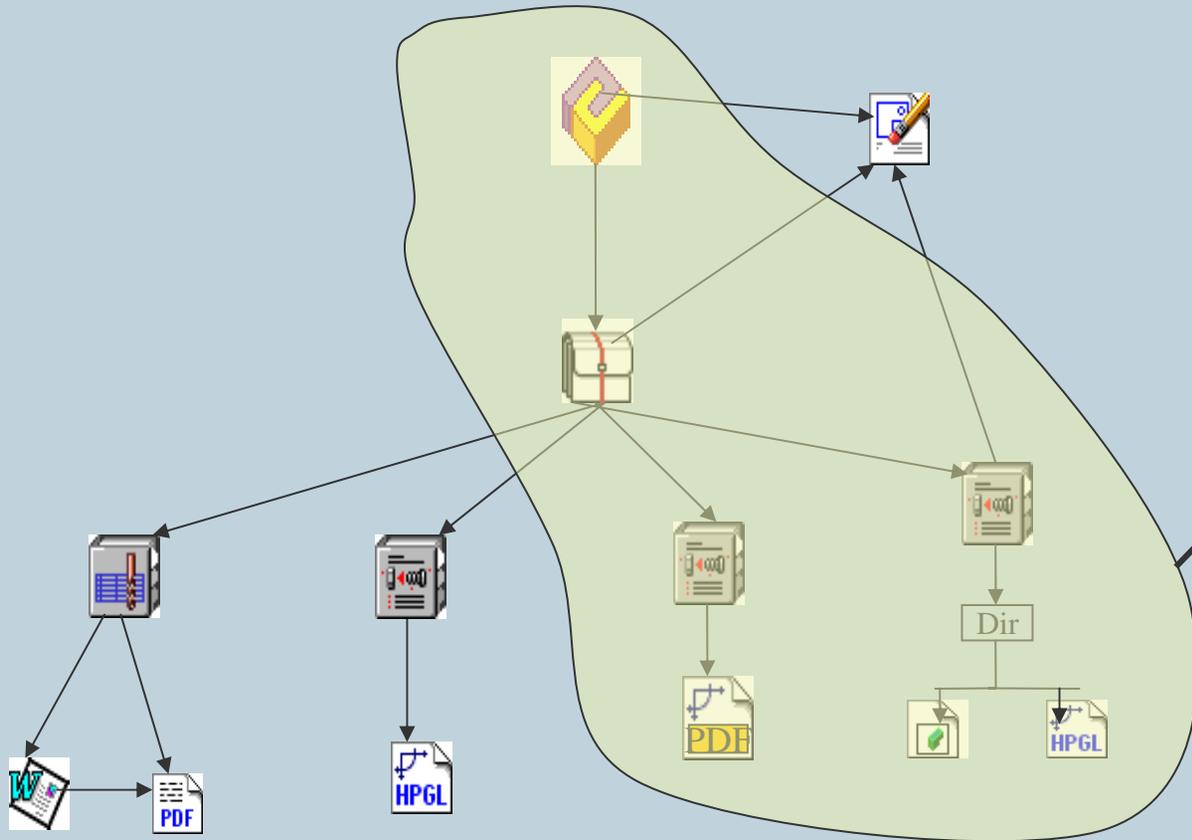
Share data with partners

Send Compartment Data to an external Recipient, based on contract agreement.



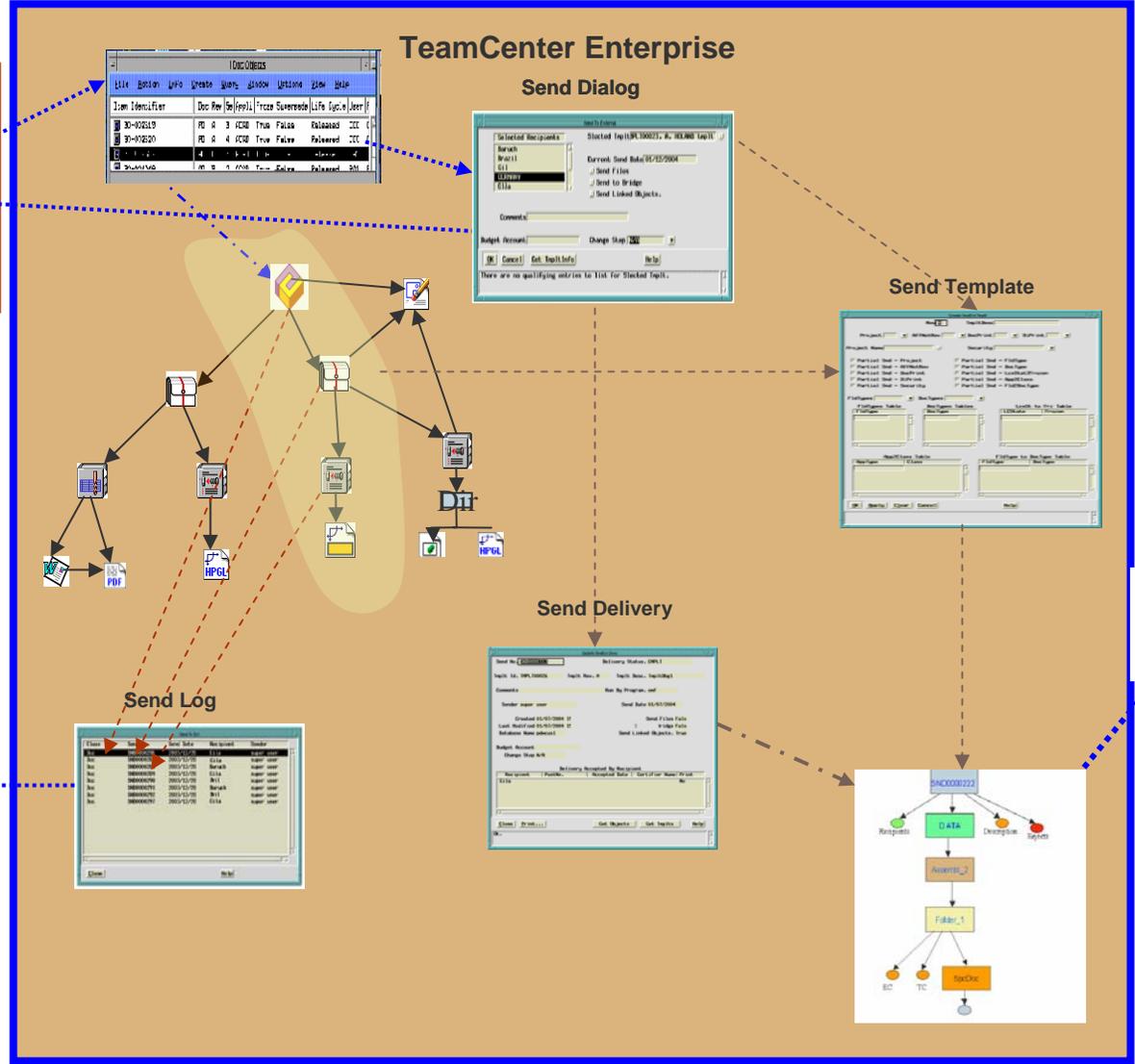
Partner Compartment

Company

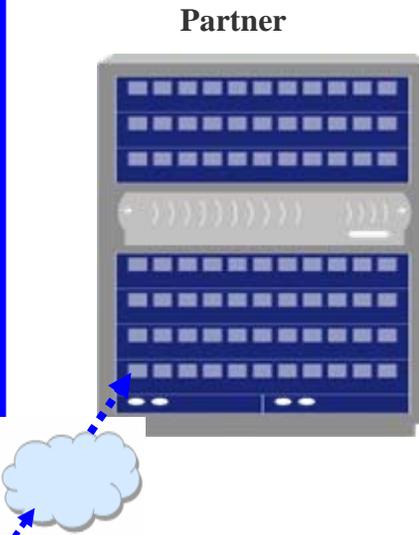
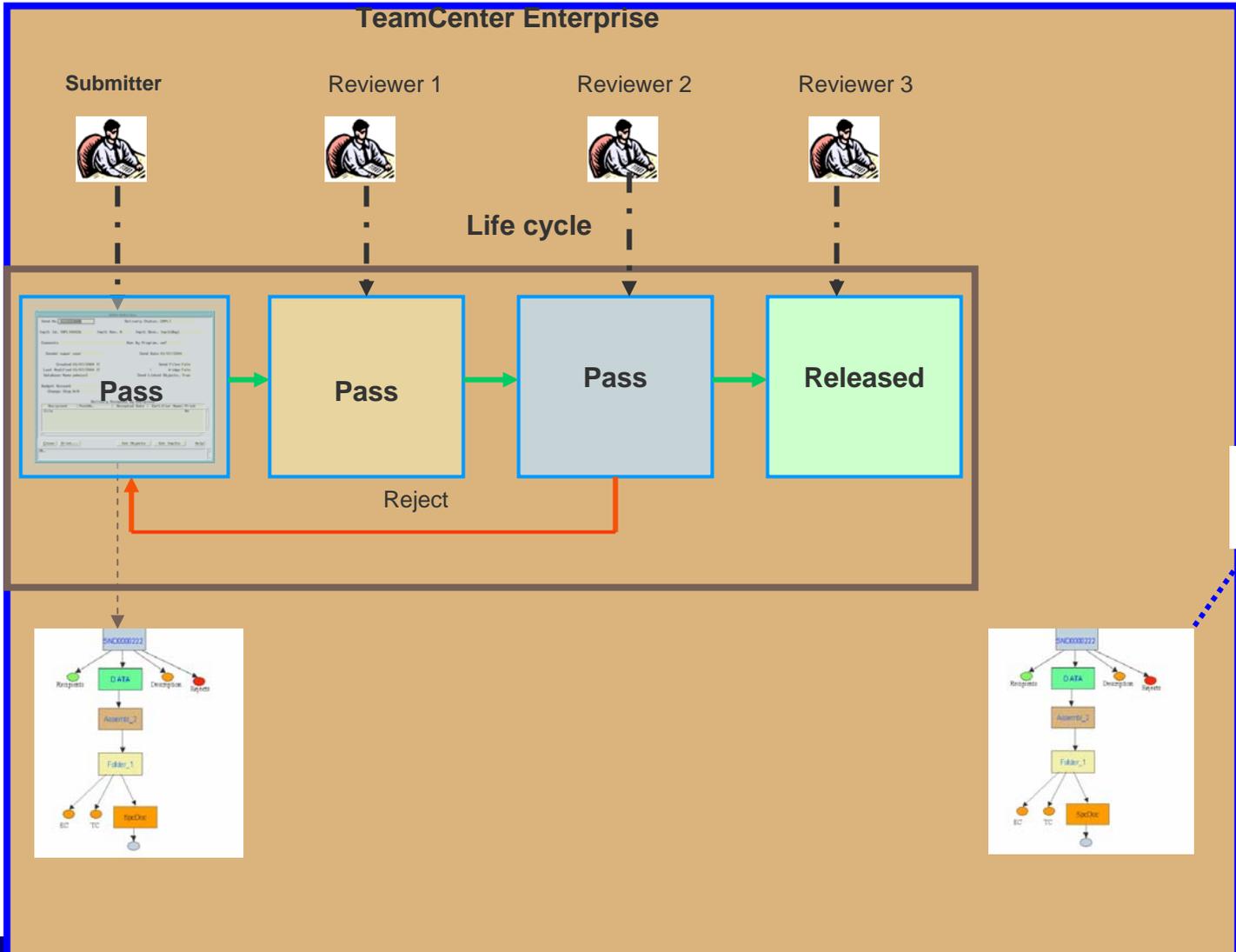


Send data to external recipient

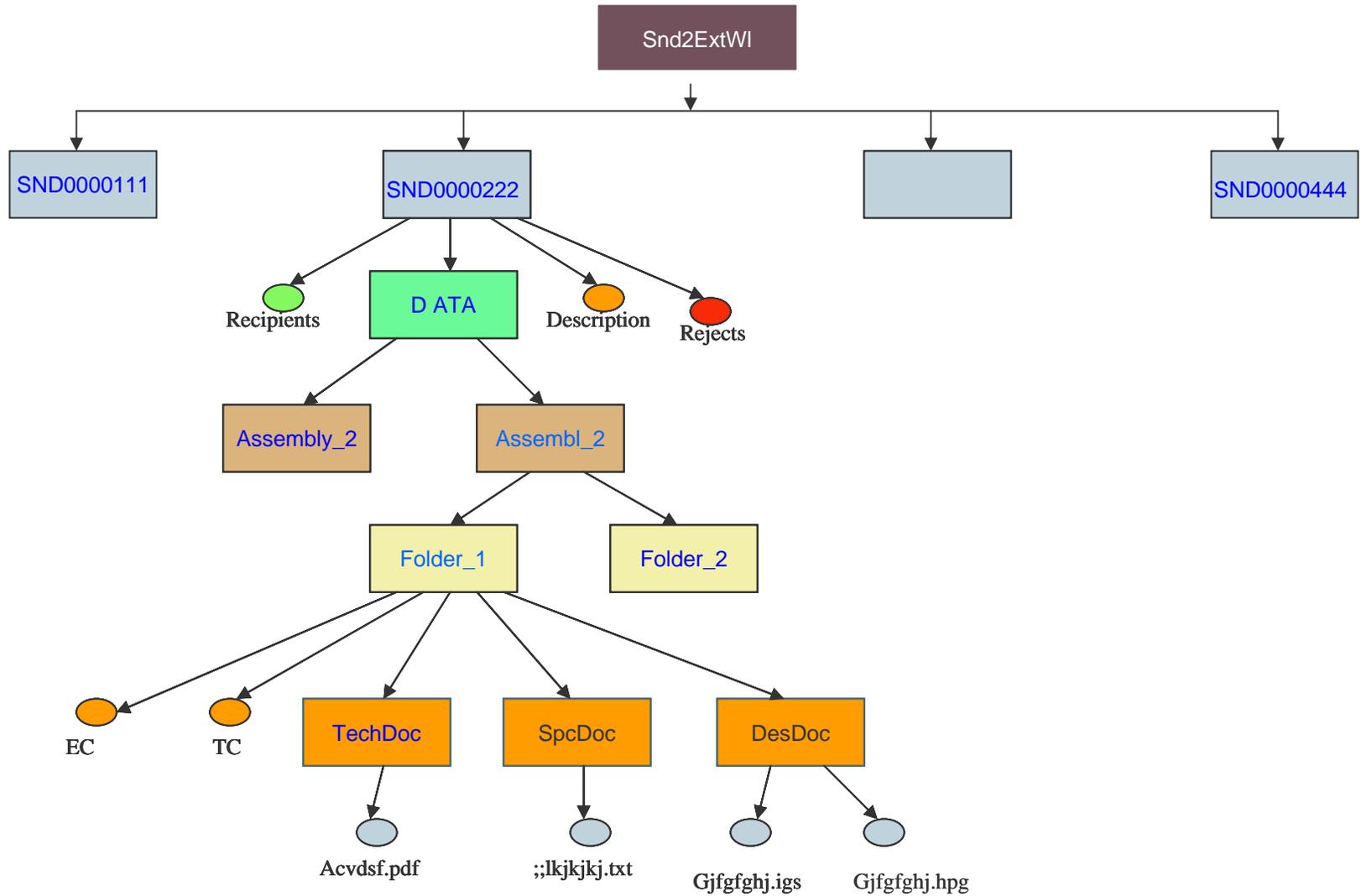
ERP
Request for Data
Budget account



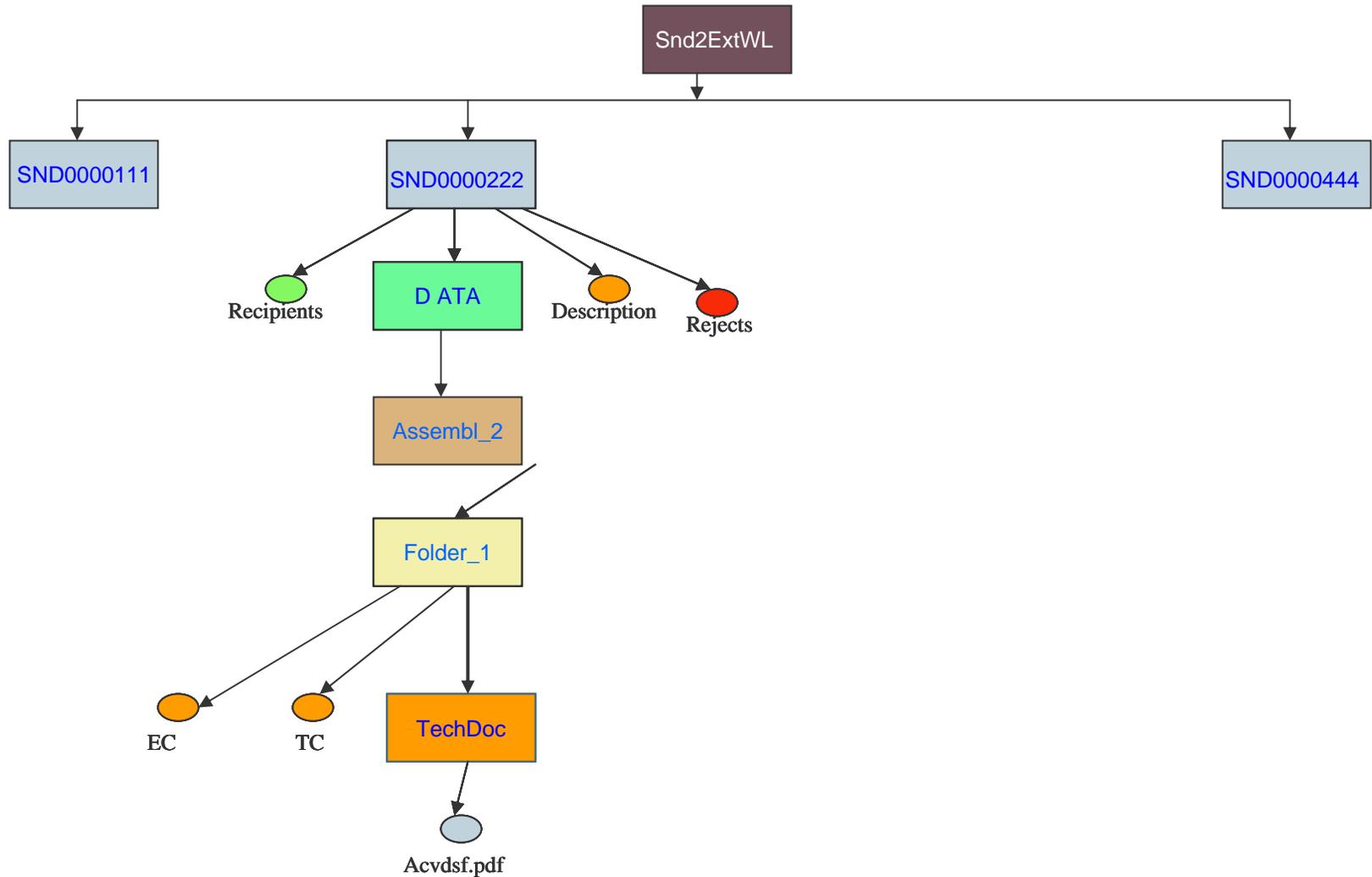
Submit Send Delivery to Life cycle



Send Data Work Location



Send Data Work Location



Send Data Dialog

Assembly Objects

Item Identifier	Class	Rev	Seq	Description1	Standard P
ASSEMBLY111	Assembly	A	1	1234	False
ASSEMBLY122	Assembly	A	1	1234	False
ASSEMBLY123	Assembly	A	1	1234	False
ASSEMBLY222	Assembly	A	1	1234	False
ASSEMBLY333	Assembly	A	1	1234	False
ASSEMBLY444	Assembly	A	1	1234	False
ASSEMBLY555	Assembly	A	1	1234	False

Send To External

Recipient List

Selected Recipients: TEST

Selected Tmplt: PLT00001, A, Test Template

Current Send Date: 03/14/2006

Single/Multi Selection: Single

Send Files

Send Original Name

Send Linked Objects.

Send to Bridge

Comments: _____ Change Step: N/A

Budget Account: _____

OK | Cancel | Get Tmplt Info | Recipient/Forward | Help

Selected Tmplt field set to the single available value in the selection list.
Ok.

Send Data Template (Getinfo)

Getinfo SndExt Tmplt

Tmplt Id. **TMPL100001** Rev A TmpltDesc Test Template
 Project No AFFNotRev Yes DocPrint Yes DiPrint Yes
 Project Name Security Unclassified
 Partial Snd - Project True Partial Snd - FldType True
 Partial Snd - AFFNotRev True Partial Snd - DocType True
 Partial Snd - DocPrint True Partial Snd - LcsStat2Frozen True
 Partial Snd - DiPrint True Partial Snd - App2Class True
 Partial Snd - Security True Partial Snd - Fld2DocType True

FldTypes Exclude **DocTypes Exclude** **LcsSt to Frz Table**
 FldTypes Table DocTypes Tables LcsState | Frozen

FldType	DocType	LcsState	Frozen
		*	*

Security Organization Name Category Name

App2Class Table **FldType to DocType Table**

AppType	Class	FldType	DocType
A4MULT	A4Mult	*	*
ACAD	PdFFile		
DOCS-OPEN	PdFFile		
ERP	PdFFile		
INTRALINK	PdFFile		
TIF-A4	PdFFile		
TIF-G4	PdFFile		

Off to us?? Frozen?? Supermodified?? Document is Managed??

Owner TEST Creator super user
 Check Out User/Vault Database Name pdncusp
 Created 01/23/2006 21:58:59:697 Current Life Cycle
 Last Modified 01/23/2006 21:59:46:591 Life Cycle State Released

[Close] [Print...] [Help]

Send Data Template (Create)

Create SndExt Tmpl

Rev TmplDesc

Project AFFNotRev DocPrint DiPrint

Project Name Security

Partial Snd - Project
 Partial Snd - AFFNotRev
 Partial Snd - DocPrint
 Partial Snd - DiPrint
 Partial Snd - Security

Partial Snd - FldType
 Partial Snd - DocType
 Partial Snd - LcsStat2Frozen
 Partial Snd - App2Class
 Partial Snd - Fld2DocType

FldTypes DocTypes

FldTypes Table
FldType

DocTypes Tables
DocType

LcsSt to Frz Table
LCState Frozen

App2Class Table
AppType Class

FldType to DocType Table
FldType DocType

OK Apply Clear Cancel Close Help

Send Data Delivery

GetInfo SndExt Dlrvy

Send No. **SNDO000313** Delivery Status. **CMPLT**

Tplt Id. **TMPLT00026** Tplt Rev. **A** Tplt Desc. **TpltDbg1**

Comments **Run By Program. onf**

Sender **super user** Send Date **01/07/2004**

Created **01/07/2004 15** Send Files **Fals**

Last Modified **01/07/2004 15** ! **bridge Fals**

Database Name **pdmcus1** Send Linked Objects. **True**

Budget Account

Change Step **N/A**

Delivery Accepted By Recipient

Recipient	PostNo.	Accepted Date	Certifier Name	Print
Gila				No

Ok.

Send Data Delivery

GetInfo SndExt Divry

Send No. **SND0000313** Delivery Status. **CMPLT**

Tplt Id. **TMPLT00026** Tplt Rev. **A** Tplt Desc. **TpltDbg1**

Comments Run By Program. **onf**

Sender **super user** Send Date **01/07/2004**

Created **01/07/2004 15** Send Files **Fals**

Last Modified **01/07/2004 15** : **bridge Fals**

Database Name **pdncus1** Send Linked Objects. **True**

Budget Account

Change Step **N/A**

Delivery Accepted By Recipient

Recipient	PostNo.	Accepted Date	Certifier Name	Print
Gila				No

Close Print... Get Objects Get Tplts Help

Ok.

Send Data Db Log



The image shows a screenshot of a software window titled "Send To Ext". The window contains a table with five columns: "Class", "Send No.", "Send Date", "Recipient", and "Sender". The table lists eight rows of data, all with "Doc" as the class and "super user" as the sender. The recipients are Gila, Baruch, and Bril. The send dates are all 2003/12/28. The send numbers range from SND0000286 to SND0000297. At the bottom of the window, there are two buttons: "Close" and "Help".

Class	Send No.	Send Date	Recipient	Sender
Doc	SND0000286	2003/12/28	Gila	super user
Doc	SND0000287	2003/12/28	Gila	super user
Doc	SND0000288	2003/12/28	Baruch	super user
Doc	SND0000289	2003/12/28	Gila	super user
Doc	SND0000290	2003/12/28	Bril	super user
Doc	SND0000291	2003/12/28	Baruch	super user
Doc	SND0000292	2003/12/28	Bril	super user
Doc	SND0000297	2003/12/28	Gila	super user

Send Data Db Log

Class	ObjNo.	Type	Revision	Application
Assembly	ASSEMBLY222		A	
Doc	DOC132	AB	A	ERP
Doc	DOC222	AB	A	TIFF

Send Data Status

Assembly Objects

File Action Info Create Query Search Window Options View Help

Item Identifier	Class	Rev	Seq	Description1	Standard P
ASSEMBLY111	Assembly	A	1	1234	False
ASSEMBLY122	Assembly	A	1	1234	False
ASSEMBLY123	Assembly	A	1	1234	False
ASSEMBLY222	Assembly	A	1	1234	False
ASSEMBLY333	Assembly	A	1	1234	False
ASSEMBLY444	Assembly	A	1	1234	False
ASSEMBLY555	Assembly	A	1	1234	False

Objects found by the query: 1.
Objects found by the query: 1.
Objects found by the query: 6.

OK

SendToExt Validation Results

Class	TotCnt	OkCnt	Rej.Reason	Rej.Cnt
Assembly	000001	000001	*****	*****

Accept: Yes

Re.iFullPth /home1/cus o/Snd2ExUL/SND0000021/SND0000021.re.i

OK Help View Re.j

Security Access Selection

Security Access Level

Action	File	Relation	BusItem
Query	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Create	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CheckIn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CheckOut	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Submit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Revise	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delete	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Security Access Selection

Security Access Level

Action	File	Relation	BusItem
Query	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Create	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CheckIn	<input type="radio"/>		<input type="radio"/>
CheckOut	<input type="radio"/>		<input type="radio"/>
Submit			<input type="radio"/>
Revise			<input type="radio"/>
Delete	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Conclusion

- **Fulfilling the Company security demands,**
is becoming increasingly important in the world of software.
- **License enforcement, encryption, and authentication,**
are important, but not enough to Fulfilled the security demands.
- **Don't assume products you use are secure,**
the application security infrastructure, gives the frame.
- **The need for On-demand creation and fast provisioning,**
while keeping the product protected and isolated,
is becoming a complicated issue in the competitive world.
- **Make time for security. Add it to the project plan.**

The top of the slide features a dark blue header with a complex, abstract geometric pattern of overlapping lines and shapes in lighter shades of blue. The word "Questions?" is centered in the header in a white, bold, sans-serif font.

Questions?

Thank you.

For more information:

haak@inter.net.il