



InterPROM – A Collaborative Framework Driven by Business Needs

7th - 10th of August, 2006
Setúbal, Portugal

Dr. Carsten Huth
chuth@essex.ac.uk

Dr. Norbert Völker
norbert@essex.ac.uk

Dr. Olaf Hahl
ohahl@pavone.de

Björn Reinhold
breinhold@pavone.de



Overview

- Motivation and context
- System Architecture
- Service Orientation
- Organisation Management in Cooperative Networks
- Security Mechanisms for Collaborative Applications
- The Application Manager
- Synthesis of Project and Workflow Management
- Some Technical Details and the Development Environment
- Conclusions

Motivation and context

- New forms of supply chains emerging where suppliers, procurers, manufacturers of consumer products form collaborative networks.
- Possible management problems because of
 - Heterogeneity of the partners and their IT infrastructure
 - Application specific interactions
 - Requirement to share resources and to coordinate activities while trying to preserve autonomy

Motivation and context

- Characteristics of knowledge intensive services:
 - Intangible, highly specific and difficult to standardise
 - Tailoring to requirements of each application necessary
 - Spontaneous demand
- Examples:
 - Mergers and acquisitions projects
 - Marketing campaigns
 - Research and development projects
 - Construction projects
 - ...
- Collaborative IT platform aimed at facilitating business processes in inter-organisational networks, especially of SME and larger companies

Characteristics of SME

- **Decker/Schiefer/Bulander 2006:**
 - Enterprises which have less than 250 employees
 - Turnover not exceeding 50 million Euro
 - Small Companies
 - < 50 employees
 - < 10 million Euro turnover
 - 99% of companies are SME
 - Generate 50% of the GDP
 - Different legal form
 - Advantage of flat hierarchies and high flexibility (Often less formal, less structured approach)
- Lower investment volume, e.g. for IT infrastructures
(here especially collaborative environments)
Smaller project sizes
- **David E. Marca:**
“They [SME] are at a different position within the supply chain”

InterPROM – EU funded project

- InterPROM research project co-funded by the European Union (6th Framework programme)
- Funding volume of 1.3 million Euro
- 2 years project duration
- approx. 10-12 developers + management and academic leaders

- Participating partners:

- SMEs:

INVERA

interenterprise

kachel.

PAVONE

- RTDs:

 **UNIVERSITY OF PADERBORN**
The University for the information Society

 **University of Essex**

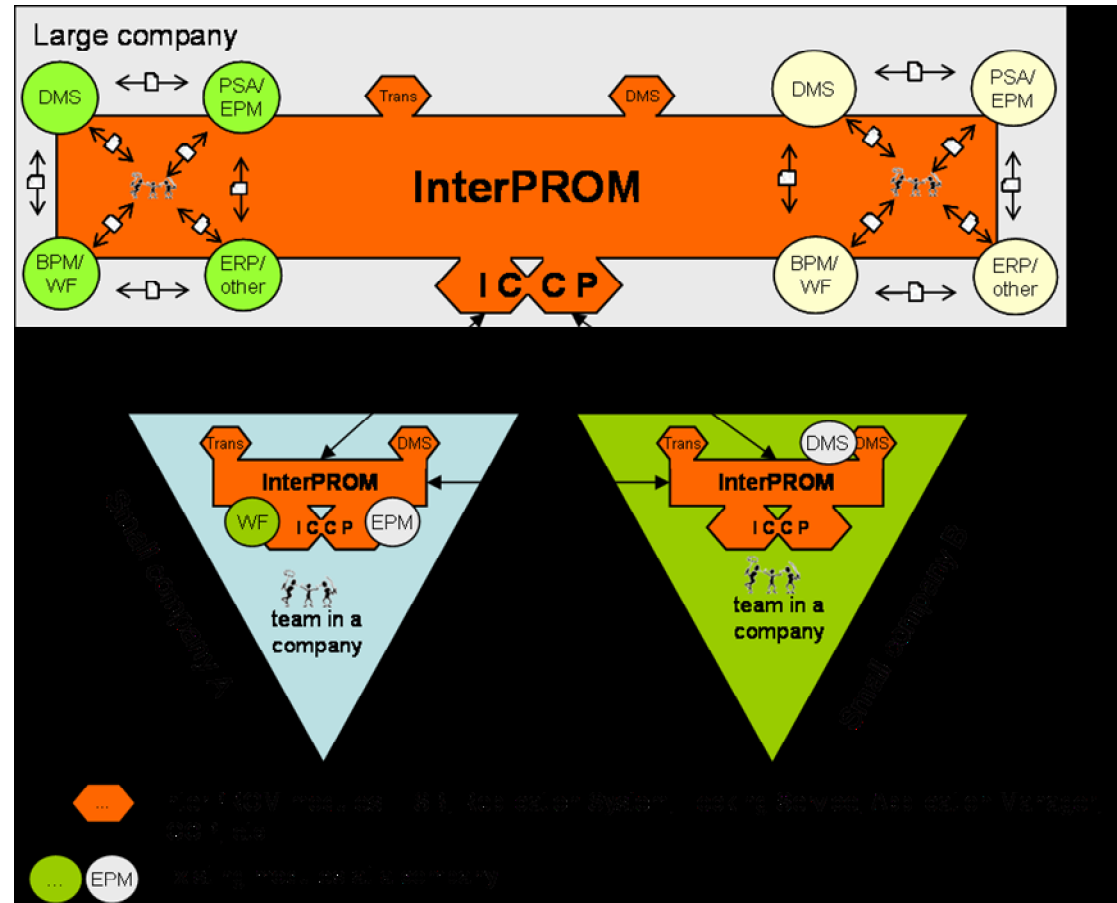
TECHNICAL UNIVERSITY OF VARNA

- End user:

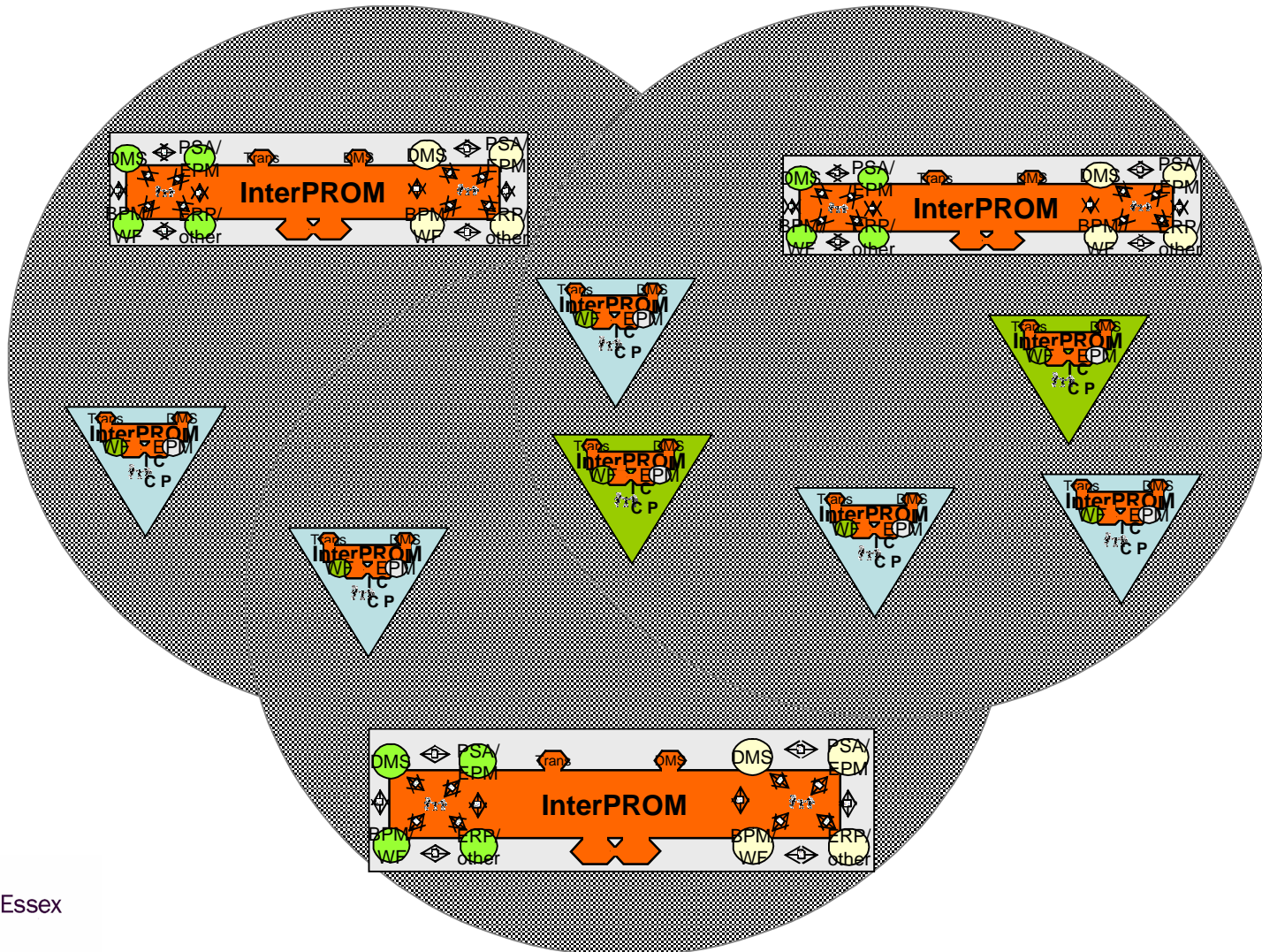
 **EADS**

Architecture – Basics

- Collaboration of SMEs and large companies (main intention, other configurations are possible as well)
- System Instance of the InterPROM system at each partner (orange filled rectangle, green and beige circles)



Architecture – Partner Networks



Service Orientation

- Service Oriented Architecture (SOA)
 - Provision of well defined, independent IT services offered by service providers.
 - Service consumers access and use these services.
- Motivation:
 - Service reuse, “programming in the large”
 - Services can be assembled dynamically (“service orchestration”, “service choreography”)
 - Use languages such as WSBPEL (Web Services Business Process Execution Language).
 - Loosely coupled and standardized but open protocols independent from particular programming languages (mostly takes the form of XML based standardized web services)
 - Aids incremental integration of legacy systems by use of adaptors

Service Bus, ESB

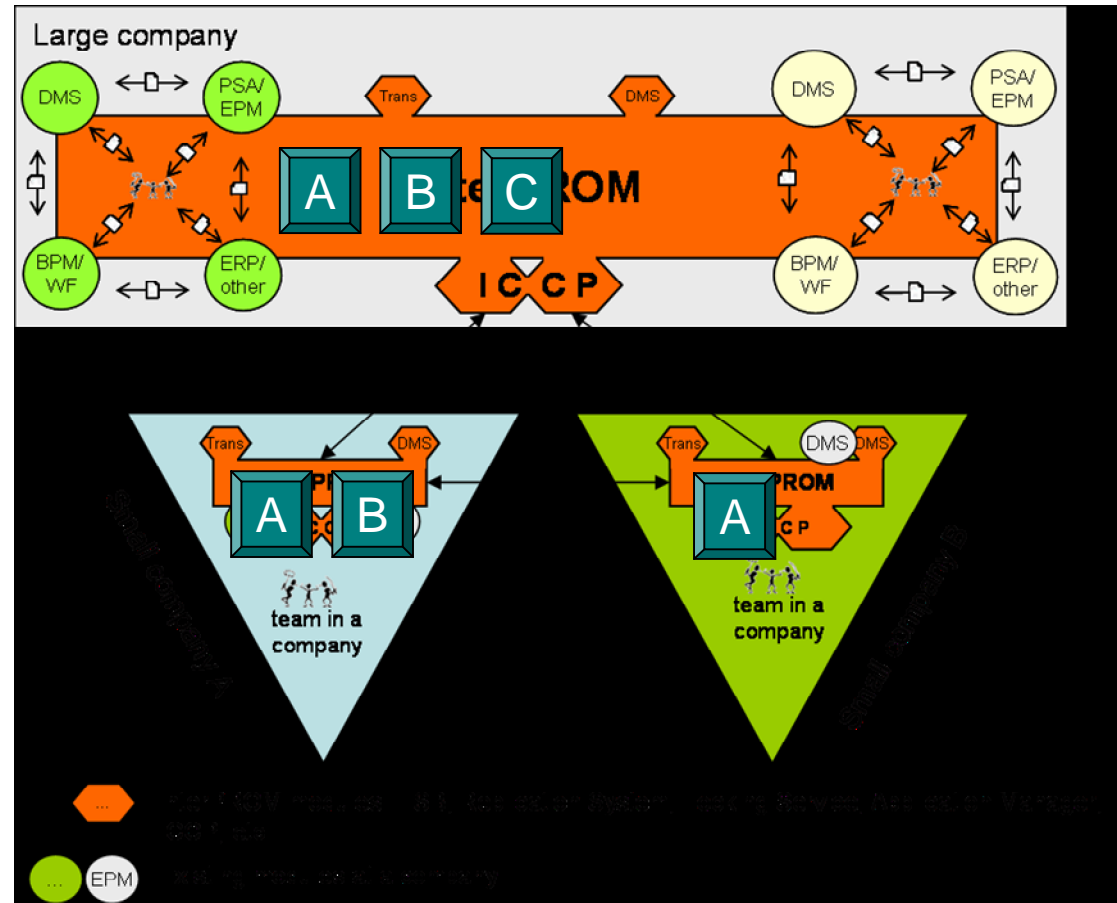
- Shortcomings of service integration:
 - Direct point-to-point connections between service providers and service consumers makes it difficult to enforce binding rules concerning security, Quality of Service (QoS), or the logging and billing of services
 - Many applications set further requirements for the IT infrastructure such as support of transactions, asynchronous communication (messaging) and the dynamic detection of services
- Introduction of an *Enterprise Service Bus* (ESB, or short service bus):
 - Standardized medium to which services can be bound in order to be located and executed
 - Core of an ESB is a messaging system which mediates between the service providers and service consumers
 - ESBs often also offers supporting services like the transformation of data formats and the controlling and auditing of the network traffic

Service Bus, InterPROM ESB

- InterPROM ESB uses XML web services and J2EE
 - Largely follows the guidelines of the Java Business Integration (JBI) (JSR 208) standard.
- The InterPROM ESB offers additional extensions
 - Connect ESBs of different companies:
 - ESB instances of different companies within a network of collaborating partners can be connected to each other. Thus, applications of one company that only have access to their own ESB can transparently use services of another company.
 - Control visibility of services:
 - The visibility of services beyond the border of the ESB of one company can be limited.
 - Services can be offered locally (within the domain of only the originating company itself), globally, or within a selected number of other companies who take part in collaborative activity.
 - Incorporates security mechanisms which perform authentication and authorisation of service requests as well as the encryption of messages.

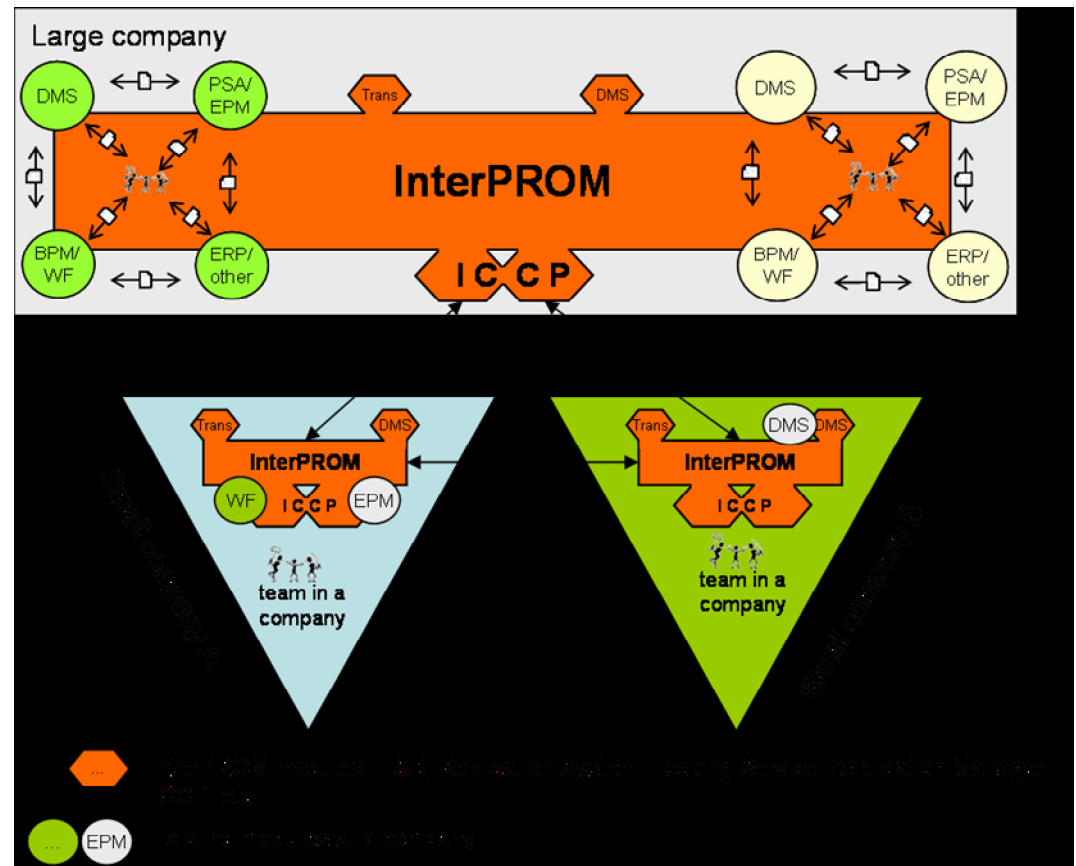
Architecture – InterPROM App.

- InterPROM Applications
 - Collaborative applications based on the InterPROM system
 - Running on an InterPROM server
 - Use different services of the InterPROM system (e.g. Process Support, Replication, ESB, connectors, etc.)



Architecture – ESB, Replication

- Custom *ESB* provides the SOA infrastructure (orange filled rectangle and connection arrows)
- ESB is additionally used to plug in connectors to legacy systems (green and beige circles)
- *Replication services* allow the synchronisation of data at the different partners.
- When modifying shared data, write conflicts are avoided with the help of *locking services*.

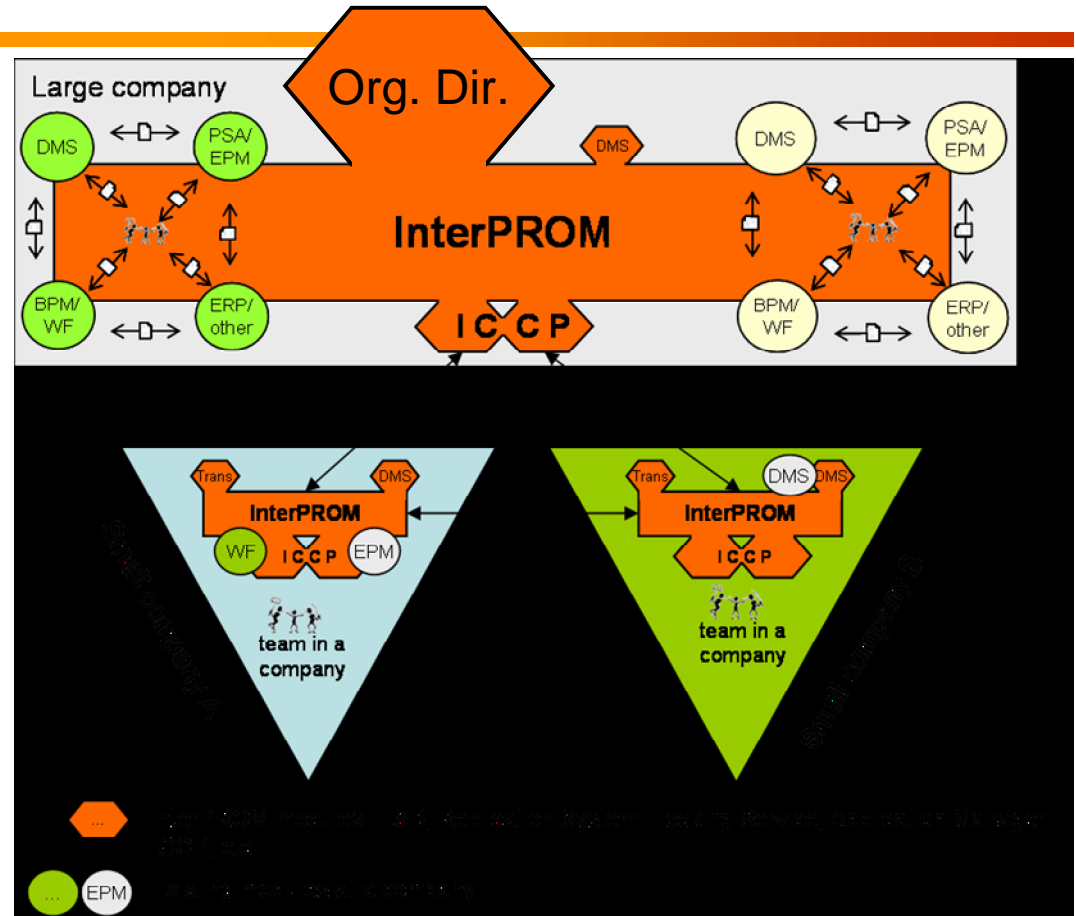


Replication

- Synchronous replication
 - Shared data which is modified is immediately replicated via the ESB to all the other partners within the partner network
- Pros/Cons:
 - + Guarantees the consistency of data
 - High availability of servers required
 - High performance data connections required
- Plans to provide additional synchronisation strategies in later versions of the InterPROM system.

Architecture – Organisation Directory

- Distributed *Organisation Directory*
 - Generally representing organisation structure of the partner networks
 - Base for the security system (Authentication and Authorization)
 - Base for the Process support (Projects/Workflow)



Organisation Management in cooperative networks

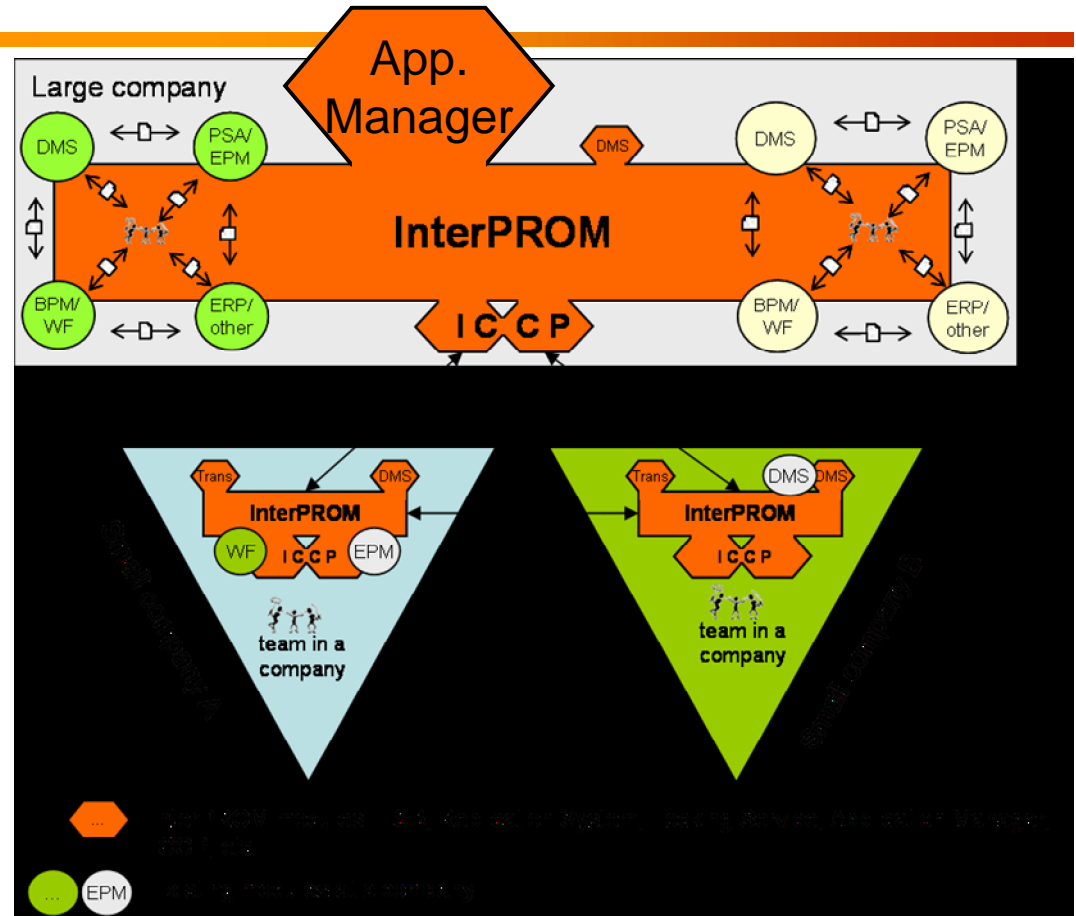
- An instance of the organisation directory resides at each of the partners running the InterPROM system
- Each instance is divided into a public and a private section
 - *Public* means that the information is to be shared within a particular partner network
- *Private* section of the OD
 - Hidden from all other partners
 - Contains the structural organisation of the company to which this InterPROM server belongs
 - List all persons, resources, etc. that will be take part in a partner network in which this company is involved
 - Connection facilities are provided to import organisation information from existing directories and keep them automatically synchronised
 - Contains specifications of the *partner connections* between the organisation and its partners within the different partner networks

Organisation Management in cooperative networks, OD public section

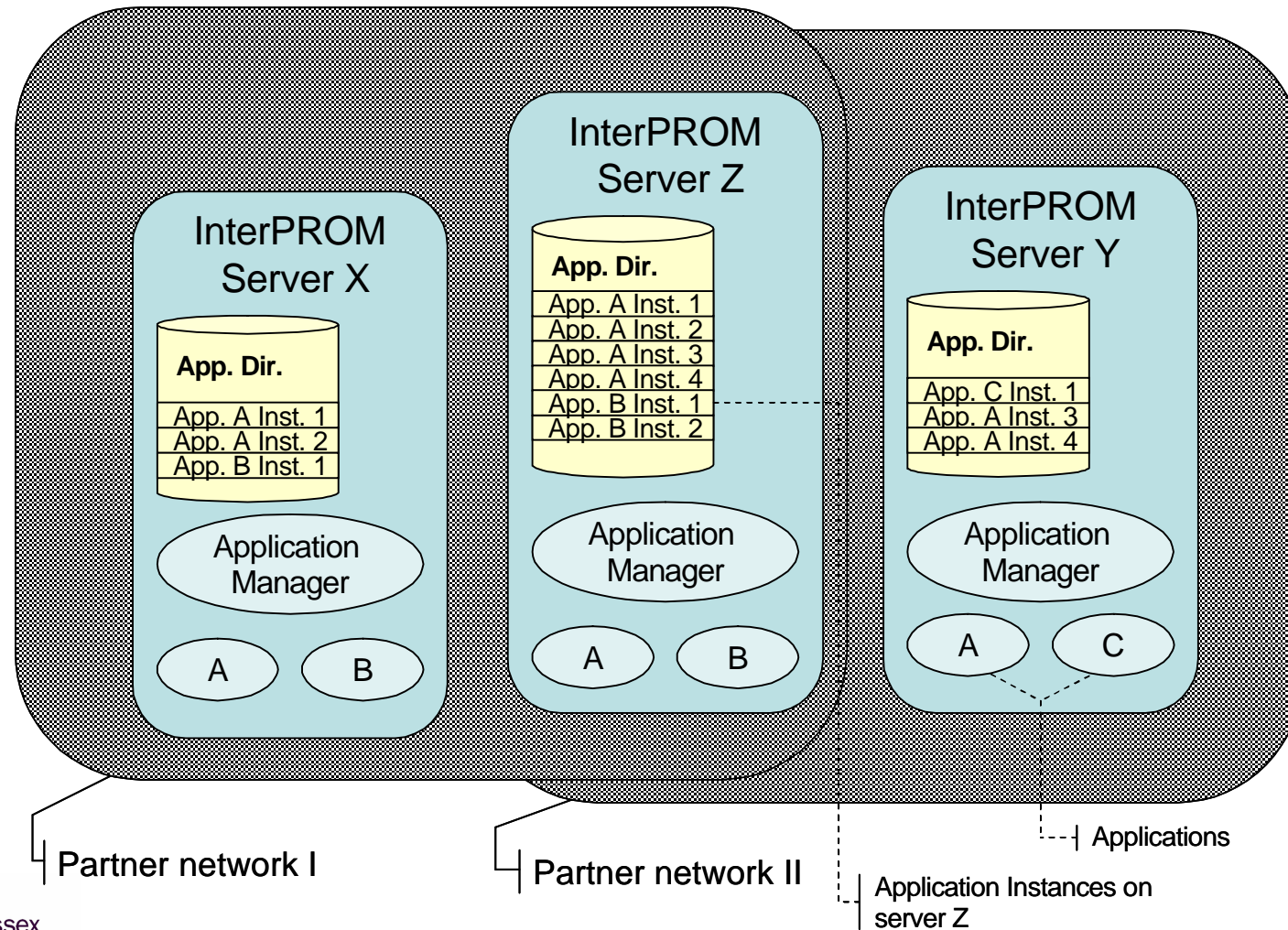
- *Public* section of the OD:
 - Basis for the management of InterPROM applications in a partner network.
 - Needs to specify the employees, resources, roles, etc. that are involved in the collaboration.
 - Typically done by a list of UUIDs which refer to entities in the private sections of the ODs
 - Creating new entities, such as network specific groups and roles, which only exist within the context of a particular partner network is also possible.

Architecture – Application Manager

- The Application Manager
 - Easy set up and maintenance of InterPROM applications
 - Manages the distribution of applications on the partner network
 - Application lifecycle management



The Application Manager



Application Manager – User Interface

InterPROM - Application Instances - Microsoft Internet Explorer

Address: http://localhost:8080/appManager-ui-1.0-SNAPSHOT/showAppInstancesPage.do?appID=AppA-004-602d-40e1-89d5-7b97ab4bee24

Application Instances for
Application ID/Name: AppA-004-602d-40e1-89d5-7b97ab4bee24

80 items found, displaying 1 to 10.
[First/Prev] 1, 2, 3, 4, 5, 6, 7, 8 [Next/Last]

Application instance name	Default locale	Application instance ID	PNID/Name	Status
Discussion Space for the InterPROM project	en	01a1cafc-60f5-46f5-accb-1e08c8396e33	PN-I	Runni
Diskussionsforum der Universität Essex	de_DE	01d24f79-844b-4091-ace6-84b9e52f8f50	PN-I	Runni
Discussion Space for the InterPROM project	en	03257d2d-968b-47a7-b5db-8f160f9bcf22	PN-I	Runni
Discussion Space for the InterPROM project	en	0a7e58fd-e3db-4485-ae8f-4ba0473dad24	PN-I	Runni
Discussion Space for the InterPROM project	en	0ccea6f3-064d-4cf8-95c5-0a0b01fcaa7d	PN-I	Runni
Discussion Space for InterPROM at Essex	en	0d0b99dc-6029-4d43-948f-4f9bd2087118	PN-I	Runni
Discussion Space for the InterPROM project	en	0f2a4048-4207-40de-8e93-20909aae6314	PN-I	Runni
Discussion Space for the InterPROM project	en	13990f54-a6a9-4cdd-93fa-a24281223d3c	PN-I	Runni
Discussion Space for the InterPROM project	en	1435c873-2f75-4978-85ca-1b1f77019d0e	PN-I	Runni
Discussion Space for the InterPROM project	en	17902f17-49c9-4b63-911c-be32065b9365	PN-I	Runni

| All applications | All instances |

InterPROM - Application Instance Meta Information - Microsoft Internet Explorer

Address: http://localhost:8080/appManager-ui-1.0-SNAPSHOT/showAppInstanceInfoPage.do?appInstanceID=01a1caf

Application Instance Meta Information

App instance name: Discussion Space for the InterPROM project

Description: This is the discussion space for the InterPROM project in general - modified

Default locale: Language: en Region:

App instance ID: 01a1cafc-60f5-46f5-accb-1e08c8396e33

Partner Network: PN-I

Creator: e5a4d635-1b8a-4fef-baae-2d5abf1007c0

Privacy level: Public

Status: Running Locally

ACL: [Edit ACL](#)

Application instance aliases:

- . ab_AL Testname
- de_DE d
- * en Discussion Space for the InterPROM project

* Default locale

[Update Application Instance Meta Information](#)

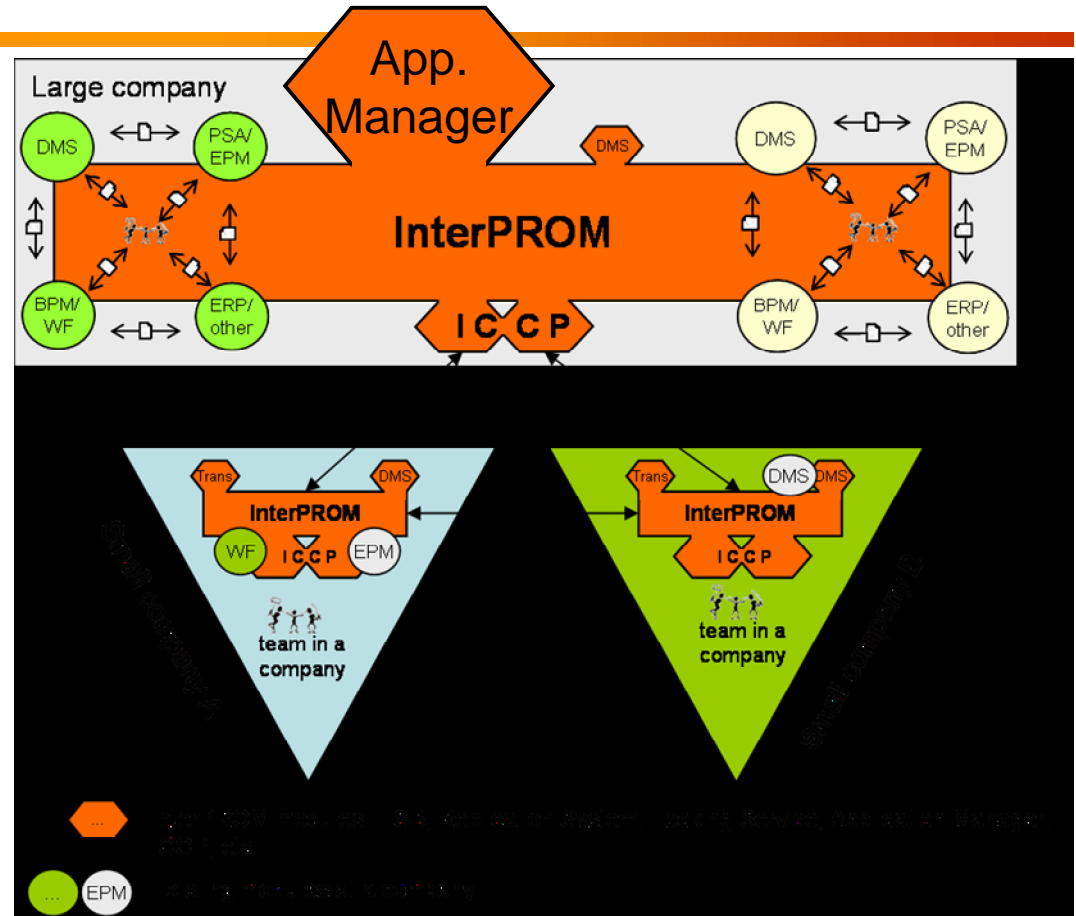
Operations:

- Delete this application instance locally
- Delete this application instance globally
- Copy this application instance to another partner network
- Move this application instance to another partner network

All applications | All instances

Architecture – Application Manager

- The Application Manager
 - Easy set up and maintenance of InterPROM applications
 - Manages the distribution of applications on the partner network
 - Application lifecycle management



Security System

- Authentication
 - An InterPROM application authenticates a user by calling the login module.
 - The login module the InterPROM organizational directory or any other LDAP compatible directory in order to verify the user's credentials
- Authorisation
 - The security system provides services and functionality to secure access to applications (application level security) and their resources (item level security)
- Access control makes use of six predefined access levels
 - Each access level defines a set of privileges
 - It is not possible to add new types of access levels
 - The existing access levels can be customised within limits
 - The limitation of customization is done intentionally in order to preserve the meaning of the access levels

Security System – Access Level

Privileges/ Access Level	Create Items	Delete Items	Read Items	Write Items	Copy Items	Execute Items	Modify App ACL	Read public Items	Write public Items	Modify Item ACL	Tra- verse
Manager	Y	Opt/Y	Y	Y	Opt/Y	Y	Y	Y	Y	Y	Opt/N
Editor	Y	Opt/Y	Y	Y	Opt/Y	Opt/Y	N	Y	Y	Opt/Y	Opt/N
Author	Opt/Y	Opt/N*	Y	Y*	Opt/Y	Opt/Y	N	Y	Opt/N*	Opt/Y*	Opt/N
Reader	N	N	Y	N	Opt/N	Opt/Y	N	Y	Opt/N	Opt/N	Opt/N
Depositor	Y	N	N	N	Opt/N	N	N	Opt/N	Opt/N	N	Opt/N
No access	N	N	N	N	N	N	N	Opt/N	Opt/N	N	Opt/N

*: There are special rules in place for the access level "Author".
Optional privileges have a default, i.e. "Opt/N" means that the default is "No".

Types of ItemACL Entries

- An item ACL entry can be of one of four different types:
 - **DENY_NONEXCLUSIVE:**
Restrict access of a particular entity to a particular item without affecting the access of other entities to that item
 - **GRANT_EXCLUSIVE:**
Grant access of an item exclusively to a particular entity. Other entities will not be able to access that item unless they have an item ACL entries of the same category and privilege.
 - **SYSTEM:**
Permit access of a particular entity to a particular item without affecting the access of other entities to that item.
 - **PERMIT_EXCEPTIONAL:**
used to permit access of a particular entity to a particular item without affecting the access of other entities to that item whether or not that entity have the right privilege at the application level provided that the traverse privilege at the application level is set to true.
- Item ACL categories have different levels of priorities:
 - SYSTEM has priority over all other categories.
 - PERMIT_EXCEPTIONAL has priority over DENY_NONEXCLUSIVE and GRANT_EXCLUSIVE categories.

Logical Model for the Evaluation of Access Rights – Set Definitions

Set	Definition
ACL	Resulting privileges on the item level from entries of the Application ACL, i.e. the entities defined by the Application ACL and the actions they are capable of performing on the item level.
$ACL_{Traverse}$	Set of potential privileges which can be defined for entries of the Application ACL for whom the Privilege Traverse is set to true. These privileges have to be defined by Item ACL entries of the category PERMIT_EXCEPTIONAL.
Y_{Grant}	Privileges resulting from Item ACL entries of the category GRANT_EXCLUSIVE $Y_{Grant} \subseteq ACL$
Y_{Deny}	Privileges resulting from Item ACL entries of the category DENY_NONEXCLUSIVE $Y_{Deny} \subseteq ACL$
Y_{System}	Privileges resulting from Item ACL entries of the category SYSTEM $Y_{System} \subseteq ACL$
$Y_{Exceptional}$	Privileges resulting from Item ACL entries of the category PERMIT_EXCEPTIONAL $Y_{Exceptional} \subseteq ACL_{Traverse}$

Logical Model for the Evaluation of Access Rights – Set Expression

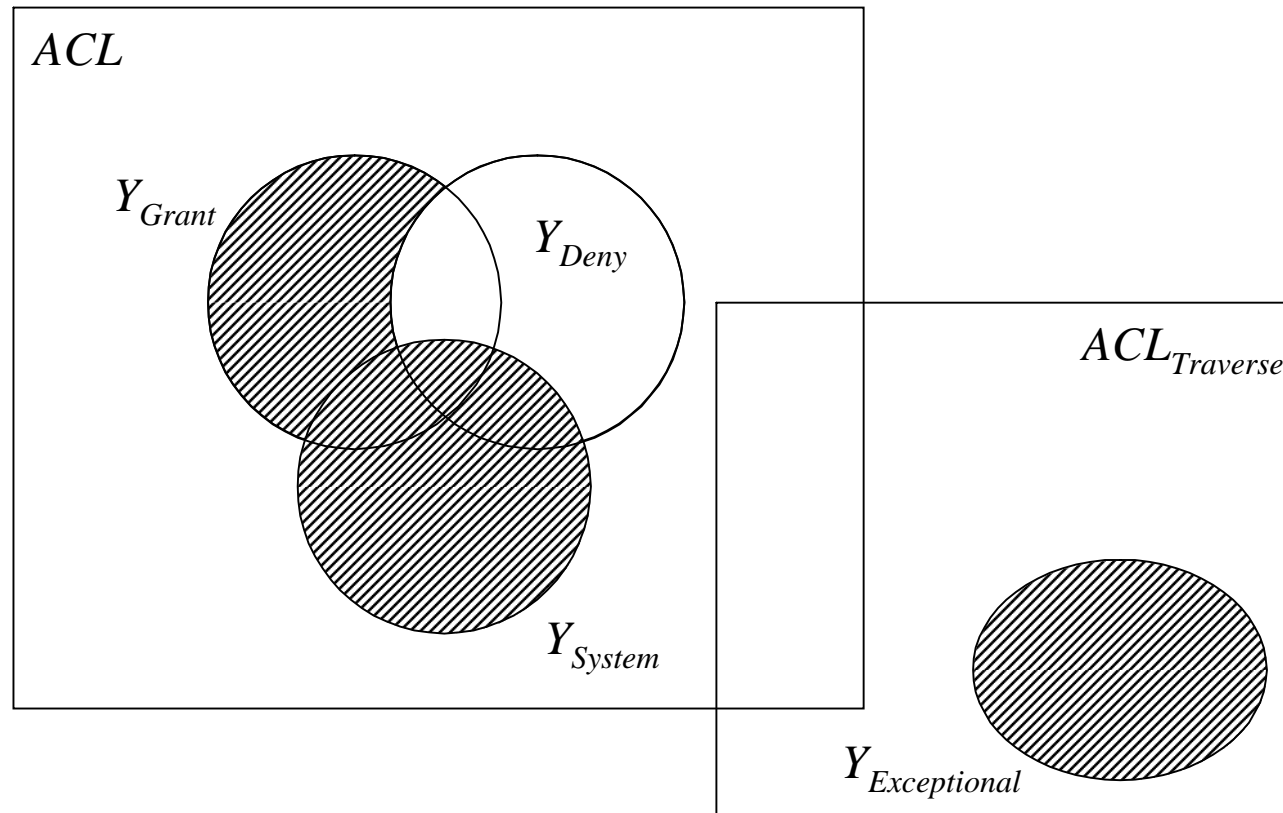
If $Y_{Grant} \neq \phi$ then:

$$ACL \cap Y_{Grant} \cap \overline{Y_{Deny}} \cup Y_{System} \cup Y_{Exceptional}$$

else:

$$ACL \cap \overline{Y_{Deny}} \cup Y_{System} \cup Y_{Exceptional}$$

Logical Model for the Evaluation of Access Rights – Visualisation



$$(Y_{Grant} \neq \phi)$$

Security System – ACL UI

The screenshot displays the 'Application Instance ACL' web interface. It features a navigation bar with 'Application Instance ACL Entries' and 'Application Instance Roles'. The main content area is divided into three sections: 'Access Control List', 'Attributes', and 'Roles'. The 'Access Control List' contains a list of users and roles, with 'Bjoern Reinhold (Manager)' selected. The 'Attributes' section includes an 'Access level' dropdown set to 'Manager' and a list of privileges with checkboxes. The 'Roles' section contains a list of roles with checkboxes. Callout boxes identify these sections: 'Entities (persons, groups, resources) selected from the organisation directory' points to the 'Access Control List'; 'Access level' points to the 'Access level' dropdown; 'Privileges' points to the 'Privileges' list; and 'Roles' points to the 'Roles' list.

Entities (persons, groups, resources) selected from the organisation directory

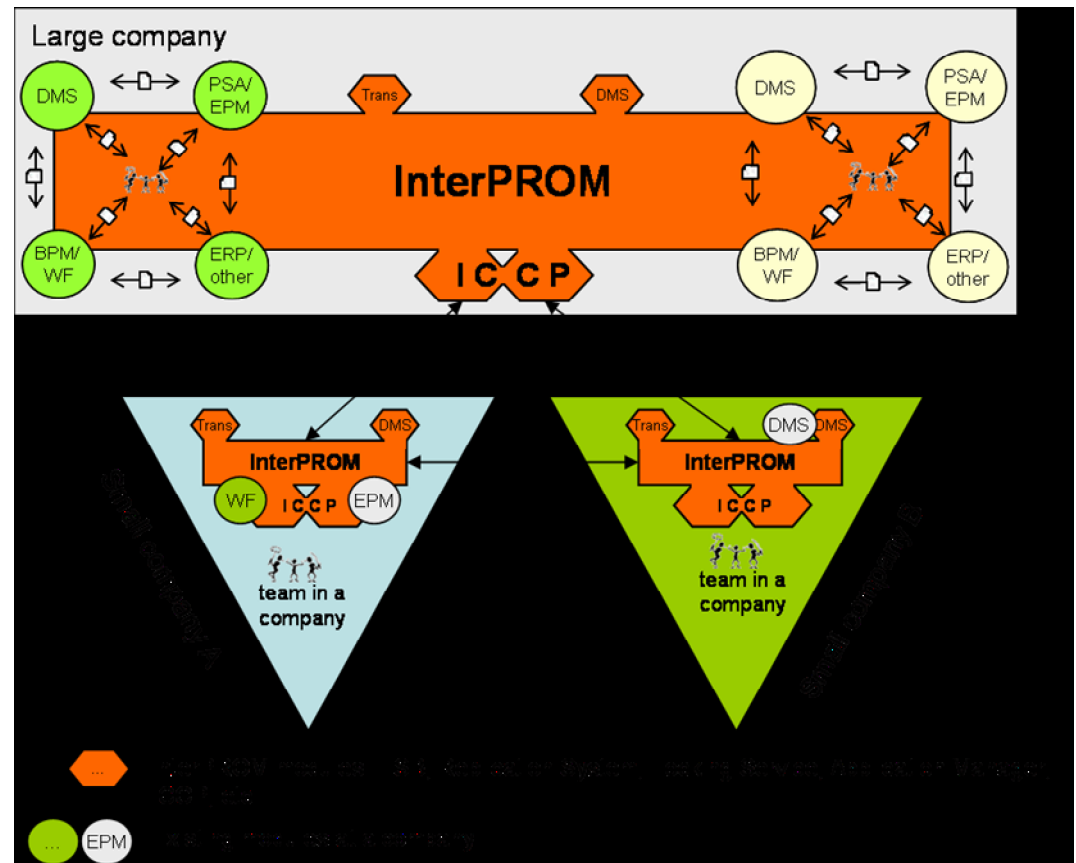
Access level

Privileges

Roles

Architecture – Processes/ICCP

- ICCP engine (InterPROM Collaboration Centric Processes)
- Integrated execution environment for projects and predefined workflows.



Integrated process management

- Empirical research carried out by PAVONE among their customers has shown that separation of workflow and projects is often viewed artificial
- Similar requests for more flexible process support from Agile Project Management approach
- Integration of projects and workflows in certain contexts requested

Project-Workflow intertwining

- In practice (especially in SME), business processes can involve both highly structured parts which follow a workflow pattern as well as less structured parts that are more suited to project management
- Example: Marketing campaign
 - Starts with a creative phase
 - Agreement on an idea is achieved and a first draft of the marketing material is created
 - After that the process can follow the structure of an established workflow including steps like revision and finally printing, distribution etc.
- On the other hand, a process which generally follows the pattern of a highly structured workflow instance might contain parts that are more of a project nature
- Example: Processing of software problem reports by a software provider
 - Majority of such problem can be answered and solved in a structured way, i.e. as a workflow instance
 - Some requests require a more thorough investigation in order to be solved or responded to
 - Initiation of a project seems an advisable action to take at such a point

Integrated process management

- A) Intertwining of processes**
 - B) Guided Process Type Conversions**
 - C) Extensions of Integrated Process Support**
-

A) Types of intertwining of processes

- Type A: Workflow instance or a project forming a sub-structure of the respective other type, i.e. a workflow instance is executed as a sub structure of a project task or vice versa
- Type B: A process changes its type permanently, i.e. a project turns at some point into a workflow instance, or a process that starts off as a workflow is turned into a project and completed as such

Integrated process management

B) Guided Process Type Conversions

- New workflows in organisations can emerge from project executions
 - A process that starts as a project in its first execution may become a successful reference example for the future
 - Especially for knowledge based services, best practises developed in a project might become more established
 - Hence it might be useful to formalize and automate that process in form of a workflow
- Result generated by the conversion tools needs to be further worked on
 - Project → Workflow
 - Abstract concrete persons or resources into roles or resource types
 - Endow the project tasks with conditionals and other control structures
 - Workflow → Project
 - Instantiations of roles and resource types
 - Linearization of workflow control structures
 - Task completion times and costs have to be allocated

Integrated process management

C) Extensions of Integrated Process Support

- Build a new type of process management system around a comprehensive shared task notion that combines aspects of workflow and project tasks (cp. Craven/Mahling 1995)
- Add Management of resource utilisation to the collaborative WFMS
 - Facilities for the posterior analysis of workflow instance resource utilisation, costs and duration will be provided. Averaging these values for a particular workflow type can help predicting the values for future executions of that type
- Function to predict project completion time and expenditure
 - Assign project tasks with conditions that have to be met for their completion
 - Assign expected probabilities for the failure of the conditions
 - A continuously updated prediction of the project completion time can then be made based on these probabilities
 - Calculation of delay times of tasks in conjunction with resource utilisation ratios
 - Corrective action can be taken in a timely manner. The corrective actions again lead to updated project completion time calculations

Some technical/development details

- Rely on open source technologies to provide the contractors with a platform which is free from licence costs for third party products.

(Important prerequisite for SMEs as the mainly addressed target market)

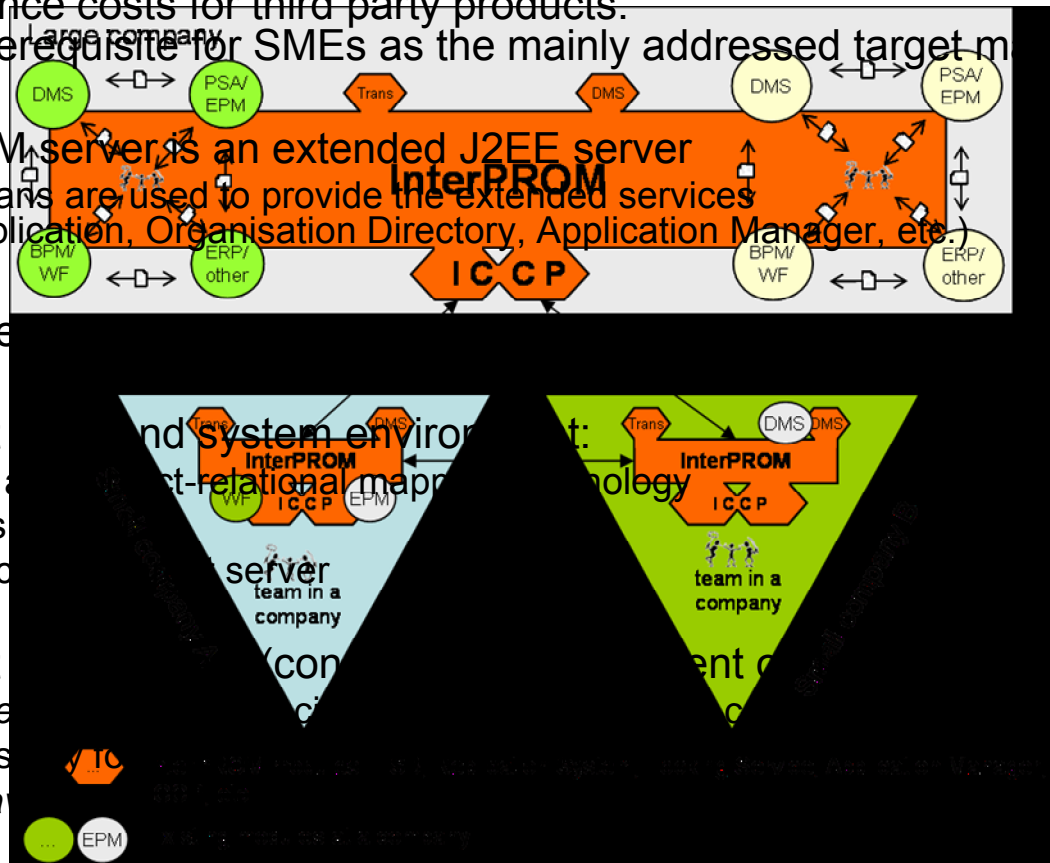
- An InterPROM server is an extended J2EE server
 - JMX MBeans are used to provide the extended services (ESB, Replication, Organisation Directory, Application Manager, etc.)

- User Interface

(speed-2)

- Development and system environment:
 - Hibernate as object-relational mapping technology
 - MySQL as database
 - JBoss as container

- Development tools (contractor's development environment):
 - Lotus Notes
 - SVN repository
 - Use of Maven



Conclusions

- The InterPROM system provides a J2EE based collaborative platform for the support of inter-organisational networks.
 - Decentralised
 - Service-oriented architecture
 - Easy to integrate third-party applications
 - Easy adaptations of partner networks (adding/removing of partners)
 - Security model allows fine-grained access control for applications and resources
 - Application Manager: Facilitates the life cycle management and distribution of application instances.
 - Integrated approach to project and workflow management.
- Component integration and test
 - Use of modules by other partners within the consortium
 - Enhancing and amending modules based on test experience
- First concrete applications are currently being developed based on the InterPROM platform: Project, risk and supply chain management solutions.
- The system will be evaluated in a pilot study at EADS as well as in other end-user projects.
- Future work will include implementation of further replication services, or enhanced support for service orchestration and choreography

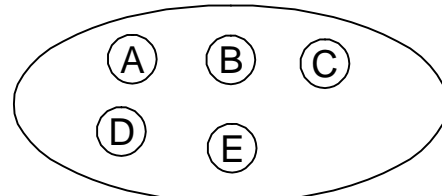
Additional Slides

Categories of ItemACL Entries

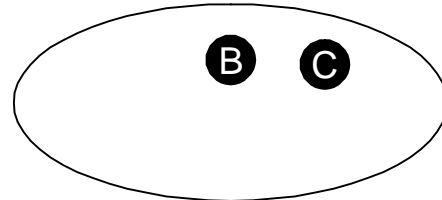
- An item ACL could be one of four different categories:
 - **DENY_NONEXCLUSIVE:**
Restrict access of a particular entity to a particular item without affecting the access of other entities to that item
 - **GRANT_EXCLUSIVE:**
Grant access of an item exclusively to a particular entity. Other entities will not be able to access that item unless they have an item ACL entries of the same category and privilege.
 - **SYSTEM:**
Permit access of a particular entity to a particular item without affecting the access of other entities to that item.
 - **PERMIT_EXCEPTIONAL:**
used to permit access of a particular entity to a particular item without affecting the access of other entities to that item whether or not that entity have the right privilege at the application level provided that the traverse privilege at the application level is set to true.
- Item ACL categories have different levels of priorities:
 - SYSTEM has priority over all other categories.
 - PERMIT_EXCEPTIONAL has priority over DENY_NONEXCLUSIVE and GRANT_EXCLUSIVE categories.

1) Basic use of deny ItemACL entries (Traverse = false)

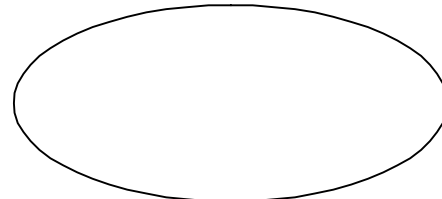
AppACL



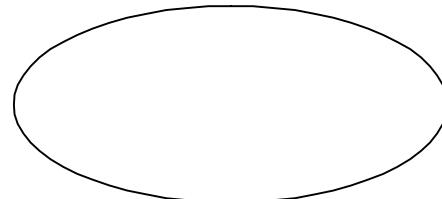
ItemACL deny
non-excluding



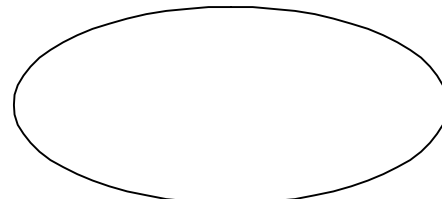
ItemACL grant
excluding



ItemACL
System

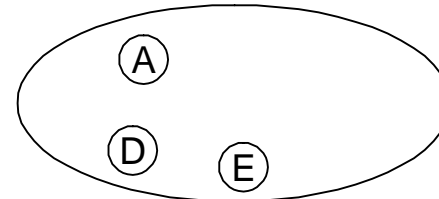


ItemACL
Exceptions



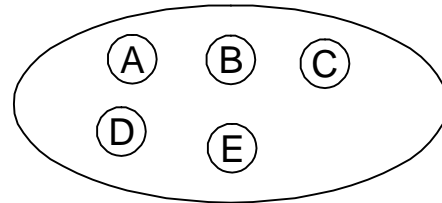
Explanations:

- Denying privileges is always non-excluding

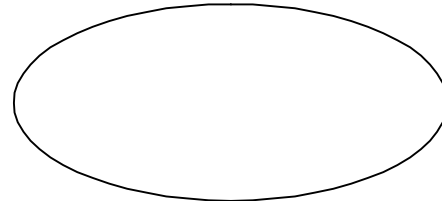


2) Basic use of grant ItemACL entries (Traverse = false)

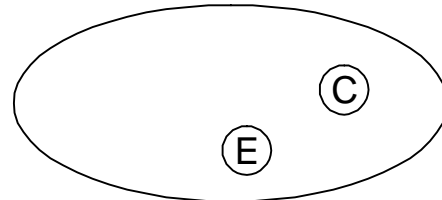
AppACL



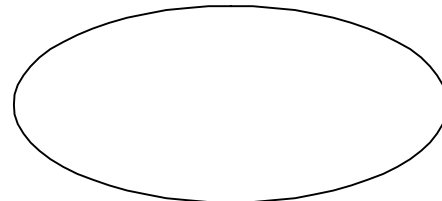
ItemACL deny
non-excluding



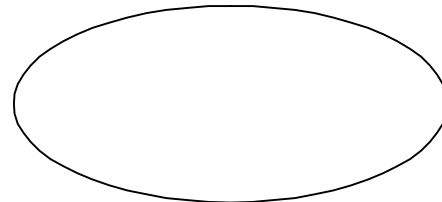
ItemACL grant
excluding



ItemACL
System

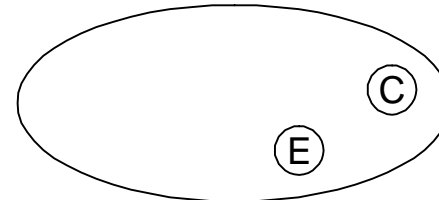


ItemACL
Exceptions
University of Essex



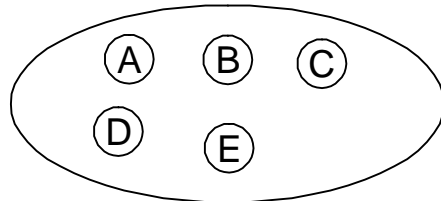
Explanations:

- Granting privileges is always excluding

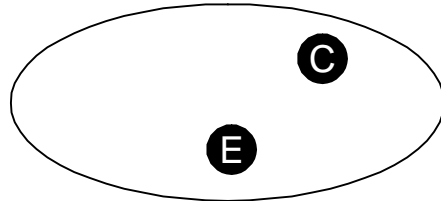


3) Basic use of System ItemACL entries (Traverse = false)

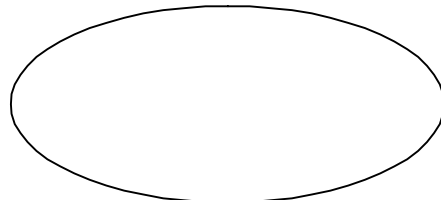
AppACL



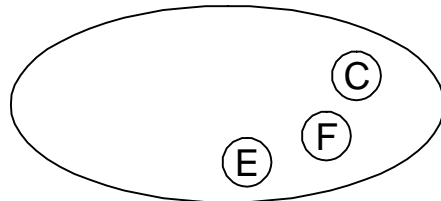
ItemACL deny non-excluding



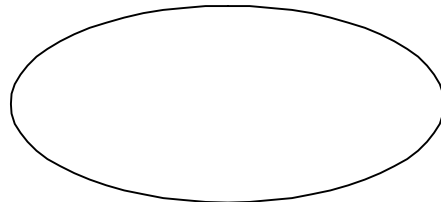
ItemACL grant excluding



ItemACL System

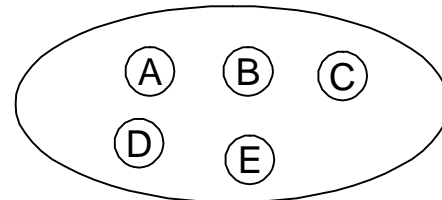


ItemACL Exceptions
University of Essex



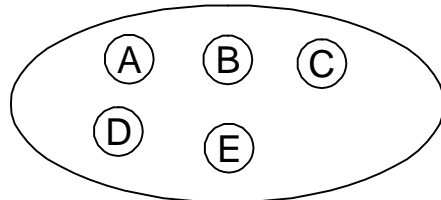
Explanations:

- The System ItemACL has always precedence before other ItemACL entries.
- However, it can still not be used to extend the privileges of the AppACL (cp. user F) unless the attribute Traverse is set to true within the AppACL

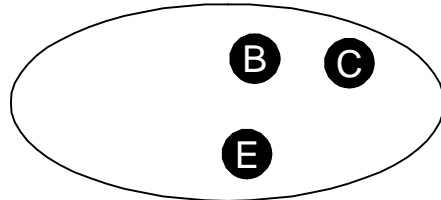


4) Conflict of excluding and non-excluding ItemACL entries (1/2)
(Traverse = false)

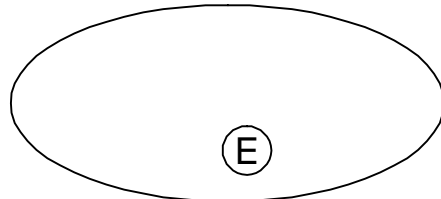
AppACL



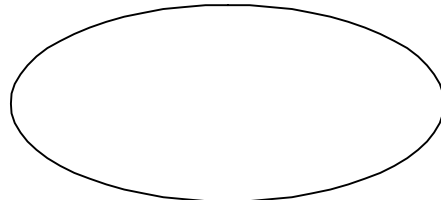
ItemACL deny
non-excluding



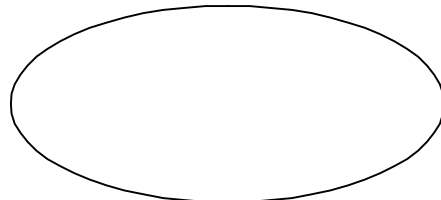
ItemACL grant
excluding



ItemACL
System

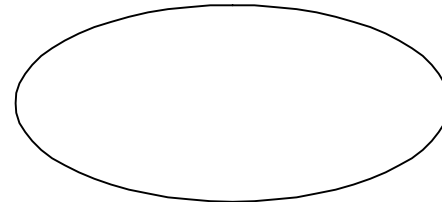


ItemACL
Exceptions



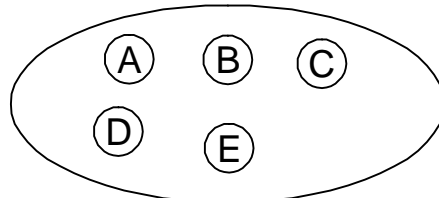
Explanations:

- If there are conflicting item privileges defined the current assumption is not to grant the corresponding privilege in this case.
- Therefore in this example nobody has got the privilege.

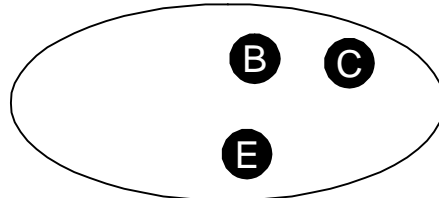


9) Basic example for Traverse set to true (Traverse = true)

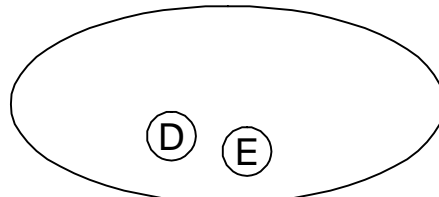
AppACL



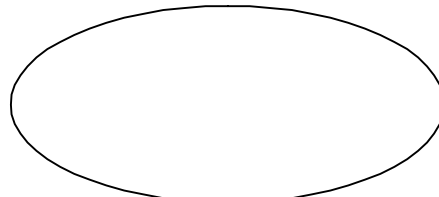
ItemACL deny non-excluding



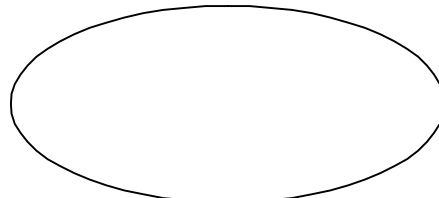
ItemACL grant excluding



ItemACL System

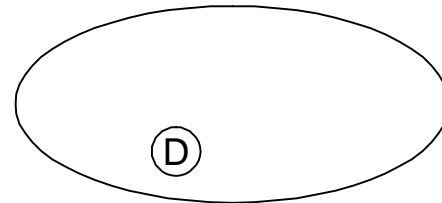


ItemACL Exceptions
University of Essex



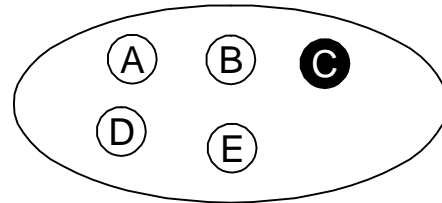
Explanations:

- In this example only user D has got the privilege. For user E the privilege is not given because of the contradiction between excluding and non-excluding ItemACL entries

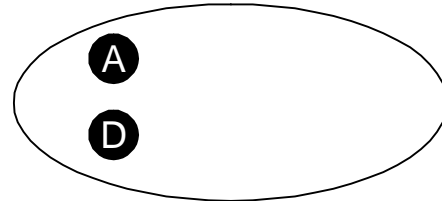


9) Basic example for Traverse set to true (Traverse = true)

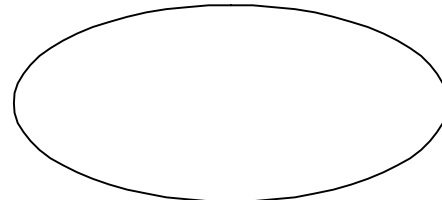
AppACL



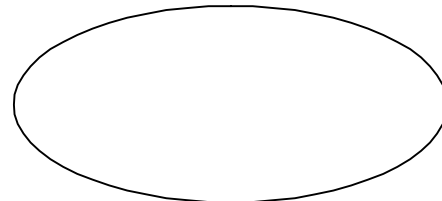
ItemACL deny
non-excluding



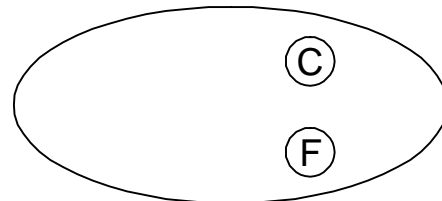
ItemACL grant
excluding



ItemACL
System



ItemACL
Exceptions

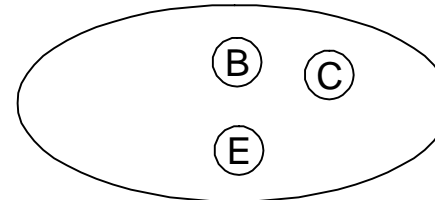


Explanations:

- Traverse is set to true for all entries except for the all users and anonymous entries within the AppACL

Explanations:

- User C gets the privilege since traverse is set to true. Therefore the privileges defined within the AppACL can be extended by the ItemACL
- However, it's not possible to add privileges for users who are not specified at all within the AppACL



- The precedence of system ItemACL entries is also valid if traverse is set to true.