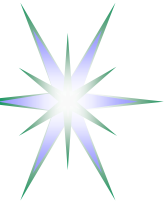
Инфраструктура безопасности для динамических Грид-приложений
(Security Infrastructure for Dynamic Grid applications)

Обзор технологий

Technology Overview

RELARN2006
16-21 июля, 2006

Yuri Demchenko <demch@science.uva.nl>
SNEG, University of Amsterdam



Содержание

- Технологии Грид
  - Развитие Грид и основные проекты
  - Определение Грид
- Грид и виртуализация ресурсов
  - Использование Виртуальных Организаций для создания динамических ассоциаций безопасности в Грид
- Особенности модели безопасности в Грид
  - Динамические Грид-сервисы и требования к инфраструктуре безопасности
  - Контроль доступа в Грид-системах и контекст безопасности
- Перспективные направления научных исследований

Существующие проекты и развитие стандартов для Грид

- Общая инфраструктура сервисов (middleware) - Globus (US) vs gLite (EU)
- LCG (LHC Grid) и EGEE (Enabling Grid for E-sciencE) - EU
  - Large Hadron Collider – запуск в апреле 2007
  - Участие России в EGEE
- OSG (Open Science Grid) Consortium и TeraGrid - US
- Стандартизация в Грид
  - GGF (Global Grid Forum) – стандарты в Грид
  - OASIS – стандарты XML и Веб-сервисов
  - Промышленность – IBM, Microsoft, Sun, HP, Verisign, BEA
  - Большие проекты – Globus, EGEE, OSG

Развитие Грид и эволюция основных определений

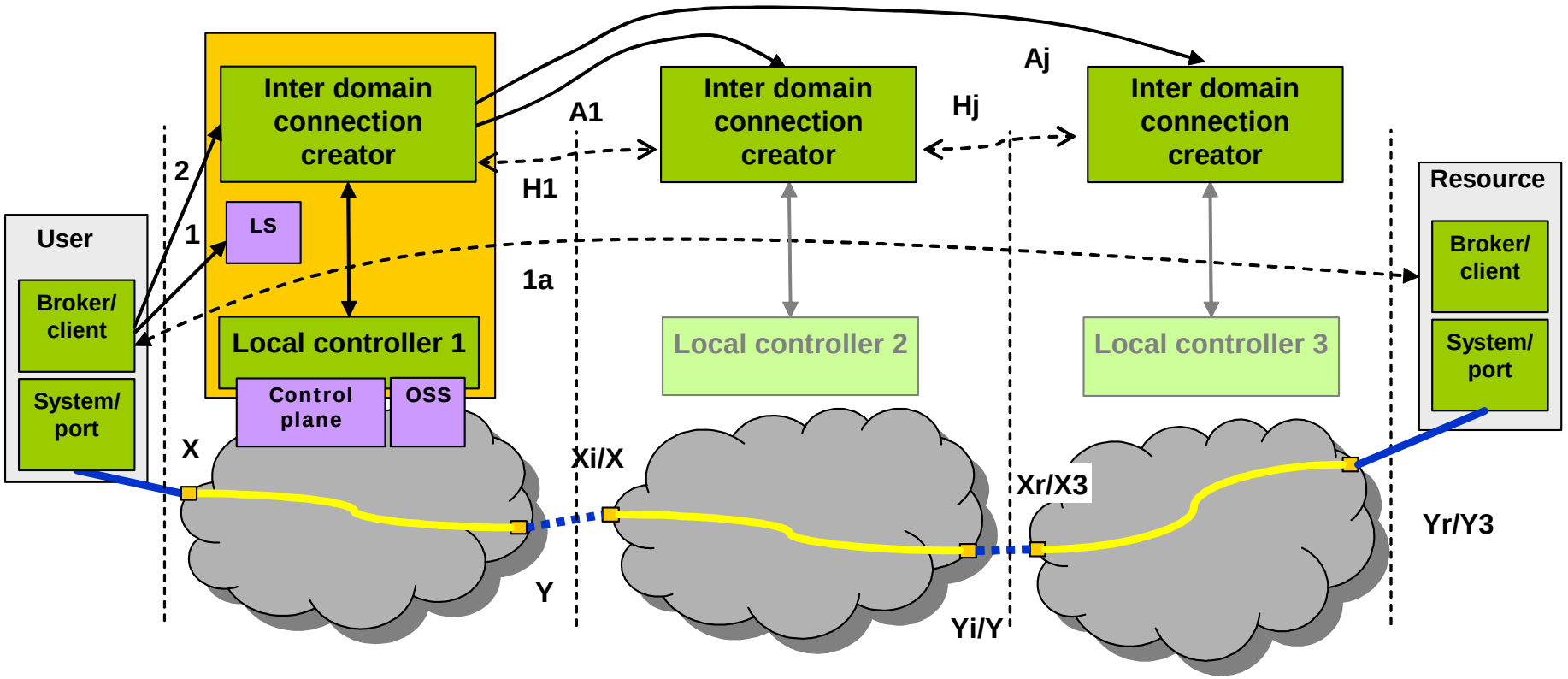
- Ранние маркетинговые идеи
  - “Computing power from the tap” – «вычислительная мощность из краника»
- Схожие коммерческие идеи
  - Autonomous computing by IBM
  - Utility computing by HP
  - .NET by Microsoft
    - Движение Microsoft в сторону распределеных вычислений и Грид
- Ключевая исходная технология для Грид – XML Web Services (WSA)
- Дивиргенция в WSA против OGSA (Open Grid Services Architecture)
- Конвергенция от OGSI (Open Grid Services infrastructure) к WSRF (Web Services Resource Framework)

Определение Грид

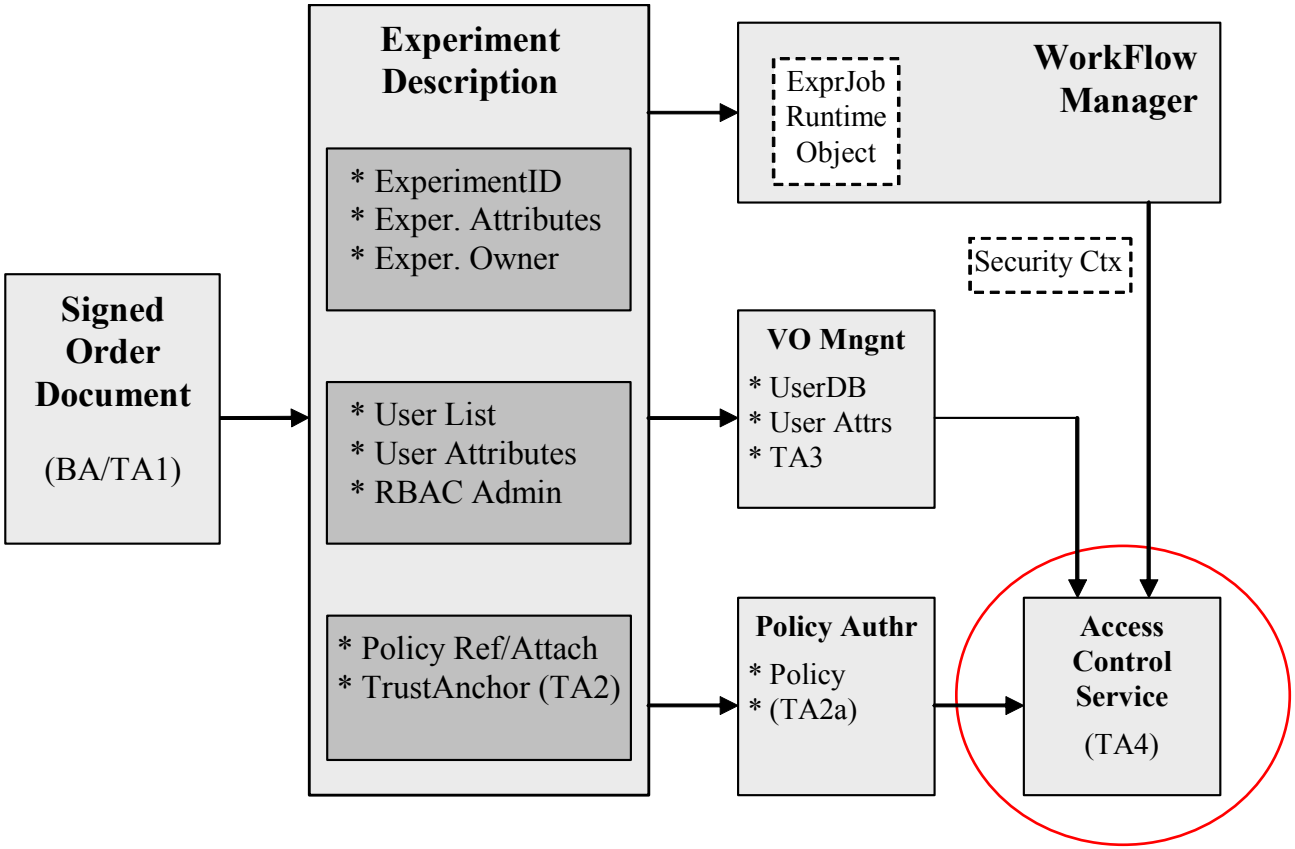
Грид-система

- Позволяет координировать использование ресурсов, которые не являются объектом централизованного управления
  - Виртуализация ресурсов и пользовательских групп в форме Виртуальных Организаций (ВО)
- Динамическое разворачивание сервисов по требованию
  - Предоставление *нетривиального* качества сервисов в сервис-ориентированной среде (SOA – Service Oriented Architecture)
  - Среда/домен безопасности определяется пользователем
- Использует стандартные, открытые и универсальные протоколы и интерфейсы на основе XML Web Services (Веб-сервисы), Web Services Resource Framework (WSRF) и Open Grid Services Architecture (OGSA)
- Типы Грид:
  - Вычислительные Грид (Computer Grid), Грид данных (Data Grid), Семантические Грид (Semantic Grid)

Система Комплексного Разворачивания Ресурсов (СКРР) – Optical LightPath Provisioning (OLPP)



Системы коллективной работы (CKP) с динамическим разворачиванием (provisioning)



Experiment Description as a semantic object defining attributes for the workflow/job, user association in a form of VO, access control policy

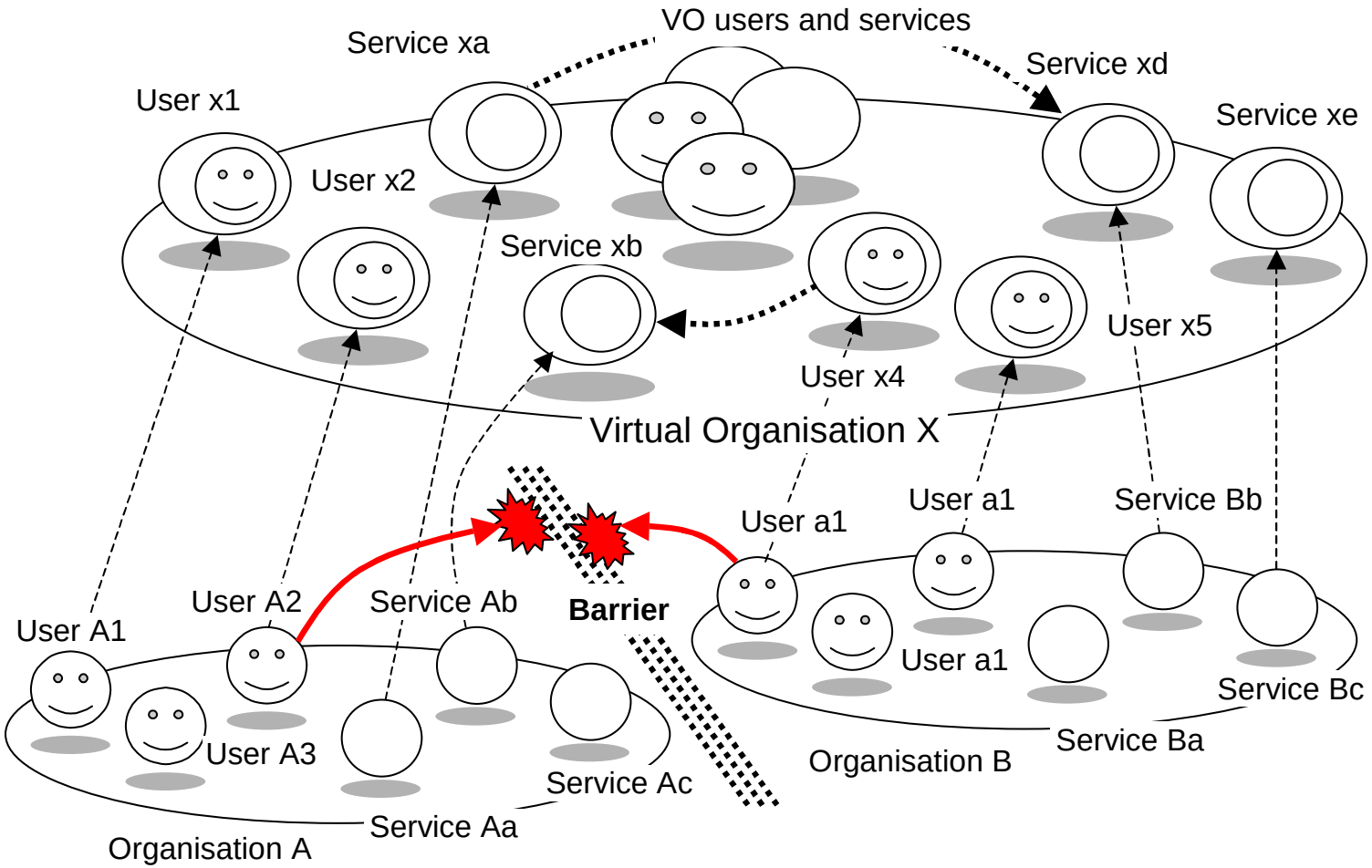
Trust domain based on Business Agreement (BA) or Trust Anchor (TA)

Грид и виртуализация ресурсов и сервисов

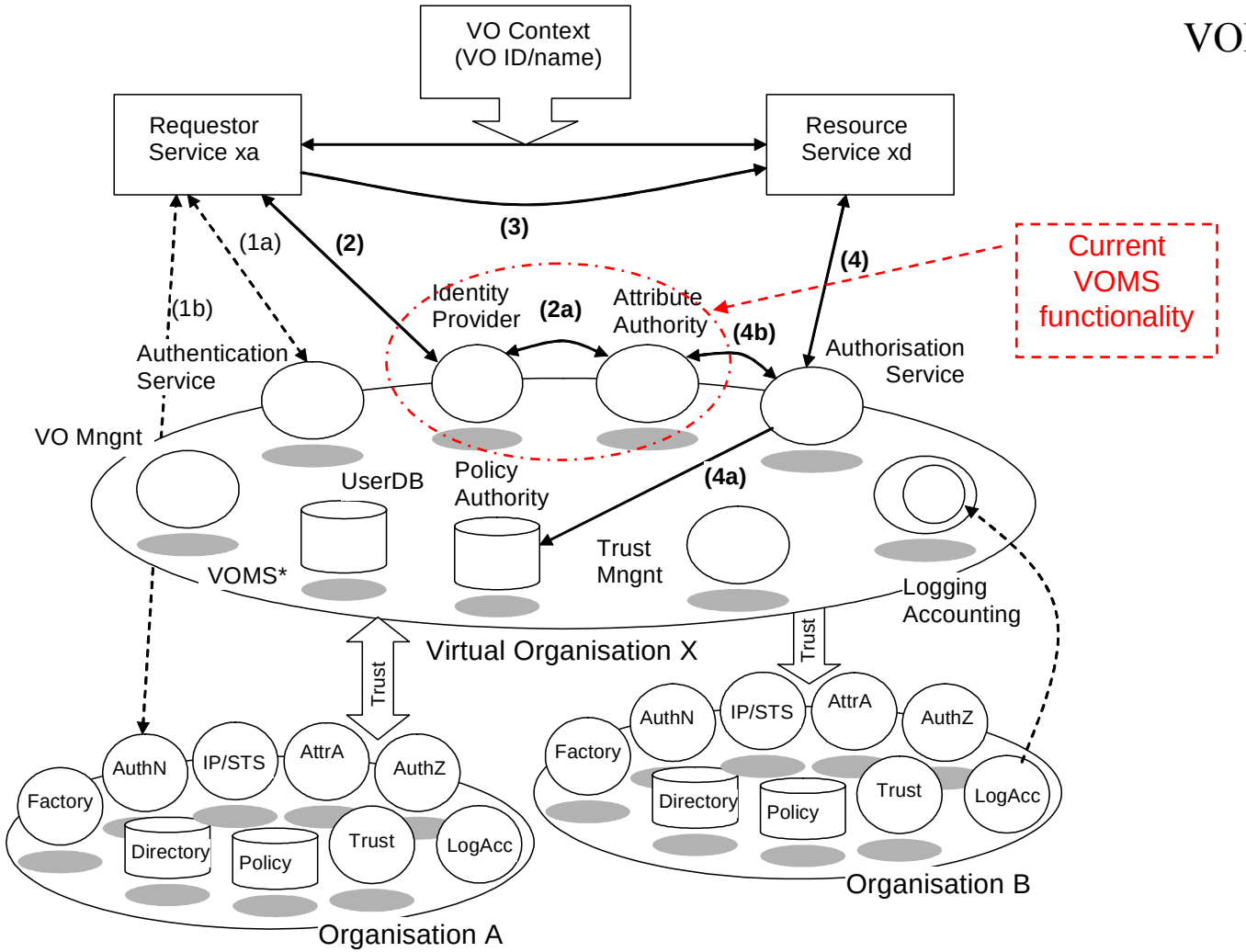
Виртуализация поддерживает согласованный доступ к ресурсам на множестве гетерогенных платформ, позволяет определять отображение множества логических экземпляров ресурсов на один и тот же физический и помогает управлению ресурсами в распределенной многодоменной среде

- Виртуализация Грид-сервисов позволяет отображать общее семантическое поведение сервисов на оригинальные механизмы платформы
- Виртуальные организации (VO - Virtual Organization) представлятт собой форму обьединение ресурсов и пользователей, ориентированных на выполнение определенных задач и предоставление определенных сервисов
  - Позволяют формировать новые сервисы из компонентных ресурсов и сервисов
  - ВО создается на основе соглашения и обязательно включает правила в форме политики ВО
  - Могут содержать специфические сервисы для всей VO
- Позволяют стандартным образом обойти ограничения системы безопасности предприятия

Структура Виртуальной Организации



Пример работы услуг безопасности BO



VOMS (VO Membership service)

- Standard-de-facto для службы членства в BO
- BO как иерархическая структура
- BO как иерархическая структура
- Атрибуты пользователя включают триаду:
  - Group/subgroup
  - roles
  - capabilities
  - VOMS X.509 Attribute Certificate (AC) включает Fully Qualified Attribute Name (FQAN)
- VOMS поддерживает регистрацию пользователей и административные функции

Особенности модели безопасности Грид (1)

- Использование концепции **Виртуальных Организаций**
- **Модель безопасности, ориентированная на услуги** и позволяющая ассоциировать услуги и политику безопасности с Грид-сервисами или данными
  - Представление в виде идентификатора единого формата End Point Reference (EPR)
- Использует **механизмы безопасности на уровне сообщений**
  - информация, относящаяся к безопасности, включается в заголовок SOAP
- Контроль доступа основан на **мандатах идентификации** (Identity Credentials) с использованием для целей аутентификации (AuthN) специального типа временных мандатов **прокси-сертификатов** (X.509 Proxy Certificates)
  - использование для **единого доступа к Грид-ресурсам** (Single-Sign-on)
  - делегирование пользовательских полномочий при запуске распределенных задач
- Использование **глобальной системы управления доверием** для Системы Открытых Ключей (СОК, PKI – Public Key Infrastructure) в Грид
  - Основана на международной федерации IGTF (International Grid Trust Federation, http://www.gridpma.org/)

Особенности модели безопасности Грид (2)

- **Авторизация и контроль доступа используют сертификаты атрибутов**, выдаваемых службой членства в ВО (так называемый VOMS X.509 Attribute Certificate)
- Использование стандартного формата WSDL (Web Services Description Language) для **динамического добавления сервисов и политики безопасности** к основным сервисам во время разворачивания и конфигурации этих сервисов
- В частном случае доступа к распределенным компьютерным ресурсам, модель контроля доступа строится на основе принятого в распределенных компьютерных системах **динамического запуска пользовательских задач от имени одного из системных пользователей (так называемых pool accounts)**, назначаемых динамически на время выполнения текушей задачи
- С точки зрения сетевой безопасности и сетевых экранов, некоторые Грид-сервисы могут использовать **нестандартные сетевые порты** из диапазона, который многие системы обнаружения атак могут расценивать как внешние атаки.
  - Например, один из наиболее важных протоколов для обмена огромными массивами данных в Грид GridFTP может использовать одновременно несколько параллельных потоков данных через порты в диапазоне выше 1024, который выделен для свободного использования сетевыми приложениями

Требования к динамическим сервисам безопасности

1) Гибкая конфигурация доверительных доменов и средства меж-доменного установления доверительных отношений

2) Динамическое управление контекстом безопасности:

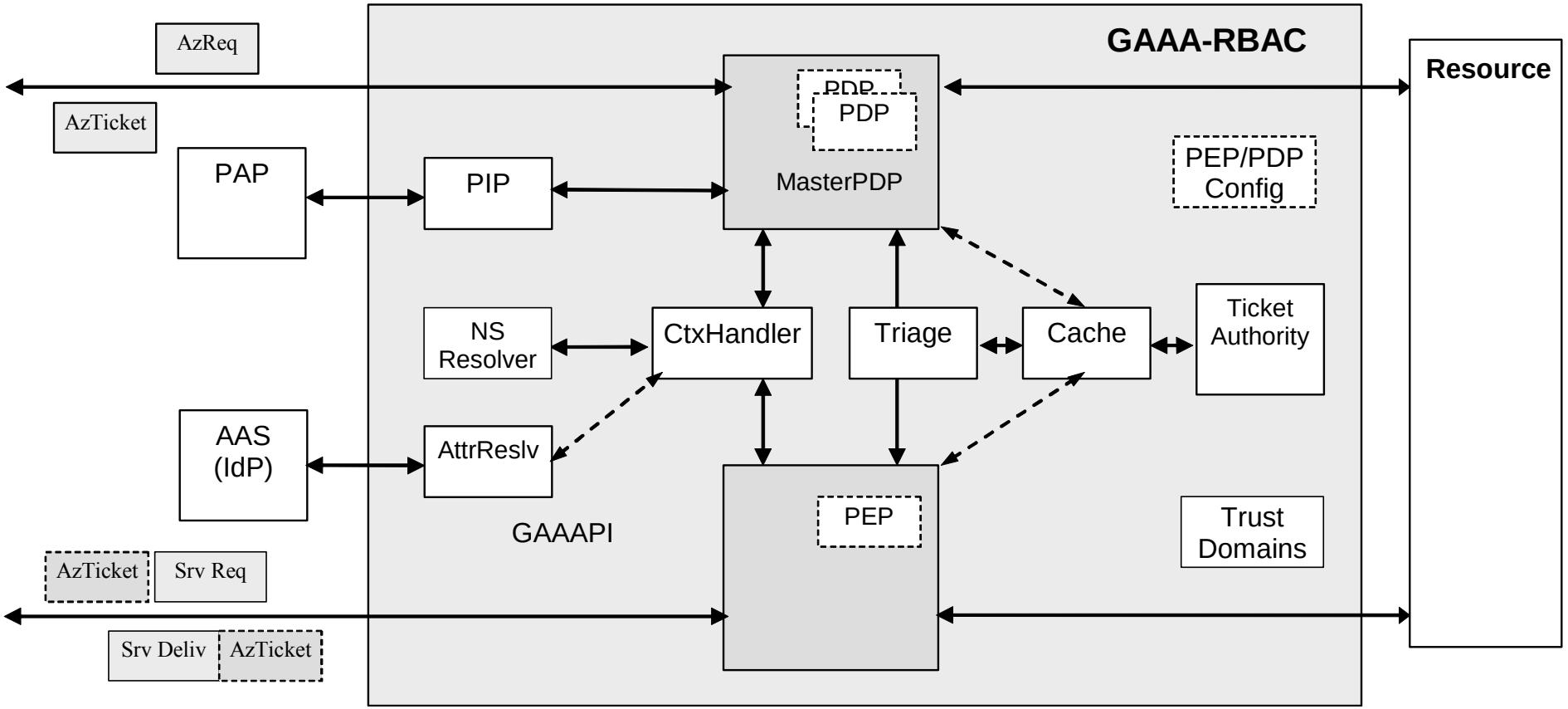
- параметры среды и административных/структурных доменов сервисов или ресурса;
- параметры среды и пользовательские полномочия текущей сессии авторизации;
- политика доступа;
- пространство имен атрибутов (Attributes namespaces);
- формат пользовательских сертификатов и мандатов (credentials);
- доверительные домены и центры удостоверения (trust domains and authorities)

4) Возможность обработки и управления пространствами имен всеми компонентами инфраструктуры безопасности

5) Гибкое управление политикой доступа, включая возможность использования множества форматов описания политики, средства комбинирования множества политик, средства разрешения возможных конфликтов в иерархической и многодоменной среде контроля доступа на основе политики.

6) Поддержка сессии доступа (или авторизации)

Расширение модели RBAC для поддержки динамических сервисов



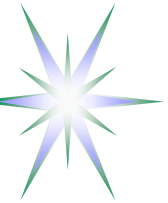
RBAC – Role Based Access Control

Перспективные направления научных исследований

- Виртуализация ресурсов и пользователей
  - Управление иерархическими группами пользователей и ресурсов
  - Координация политики доступа
  - Базовые операционные модели ВО
- Динамические Грид-сервисы
  - Динамические виртуальные ассоциации – динамические ВО
  - Виртуализация исполнительной среды и безопасность
  - Динамические сервисы безопасности и управление контекстом безопасности
- Информационные услуги в Грид – поиск и категоризация ресурсов
  - Стандартное описание Грид-задач – JSDL (Job Submission Description Language)
- Специальные области применения Грид
  - ЯФ/ФВЄ + биотехнологии, медицина, САПР, промышленость, и др.
- Разворачивание учебных програм по Грид-технологиям

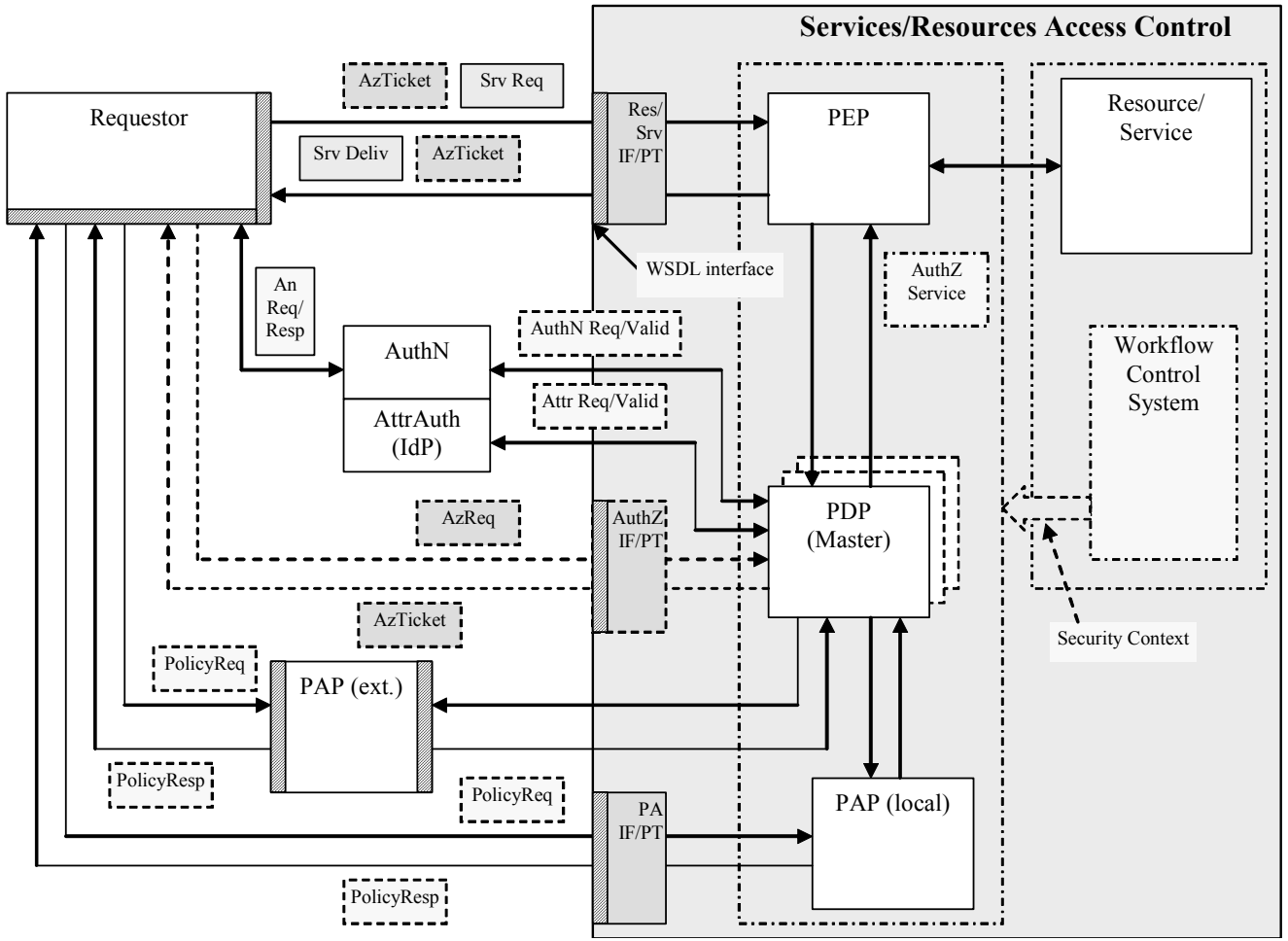
Цель – возможность участия в м/н проектах и сотрудничества с западными научными коллективами

- Грид-консорциумы, проект EGEE и Университет Амстердама заинтересованы



Дополнительная информация

Работа системы контроля доступа в Грид/Веб-сервисах



- Message-level Security services are linked to SOAP header
- Linking dynamically all components of the access control system
- Policy is attached to any component of the service description in WSDL format
- Interacting services can fetch policy document and apply restrictions/rules to elements, which declared policy compliance requirements

Динамический контекст безопасности: Механизмы управления

Context dependent information/attributes:

- Service/Resource environment/domain
- Policy
- Trust domains and authorities
- Attribute namespace
- Credential format

Mechanisms to communicate/manage context related information

- Service and requestor/user ID/DN format that should allow for both using namespaces and context aware names semantics.
- Attribute format (either X.509/X.521 or URN/SAML2.0 presentation).
- Context aware XACML policy definition using the Environment element of the policy Target element
- Security tickets and tokens used for AuthZ session management and for provisioned/booked resource/service identification
- Security federations for users and resources, e.g. VO membership credentials

Dynamic Security Associations

- **Session** – establishes security context in the form of session key that can be a security token or simple UID bound to secure credential/context
  - Session may associate/federate users, resources and actions/processes
- **Job/workflow** – more long-lived association and may include few sessions
  - May need to associate more distributed collection of users and resources for longer time required to deliver a final product or service
  - Job and workflow may contain decision points that switch alternative flows/processes
  - Security context may change during workflow execution or Job lifetime
  - Job description may contain both user and resource lists and also provide security policy and trust anchor(s) (TA)
- **Project or mission oriented cooperation** – established for longer time cooperation (involving people and resources) to conduct some activity
  - This is actually the area of currently existing VO associations
- **Inter-organisational association or federation** – established for long-term cooperation, may have a wide scope of cooperative areas
  - This is the area of inter-university associations
    - Shibboleth Attribute Authority Services (SAAS) is designed for this kind of federations

VO Operational Models

- **User-centric VO (VO-U)** - manages user federation and provide attribute assertions on user (client) request
- **Resource/Provider centric VO (VO-R)** - supports provider federation and allows SSO/access control decision sharing between resource providers
- **Agent centric VO (VO-A)** - provides a context for inter-domain agents operation, that process a request on behalf of the user and provide required trust context to interaction with the resource or service
- **Project centric VO (VO-G)** - combines User centric and Provider centric features what actually corresponds to current VO use in Grid projects