Trust and Security in Grid Environment

CONFidence

2006-05-14

Jakub Dziwisz

jakub@dziwisz.org
http://jakub.dziwisz.org/

gridwise tech

Presentation Outline

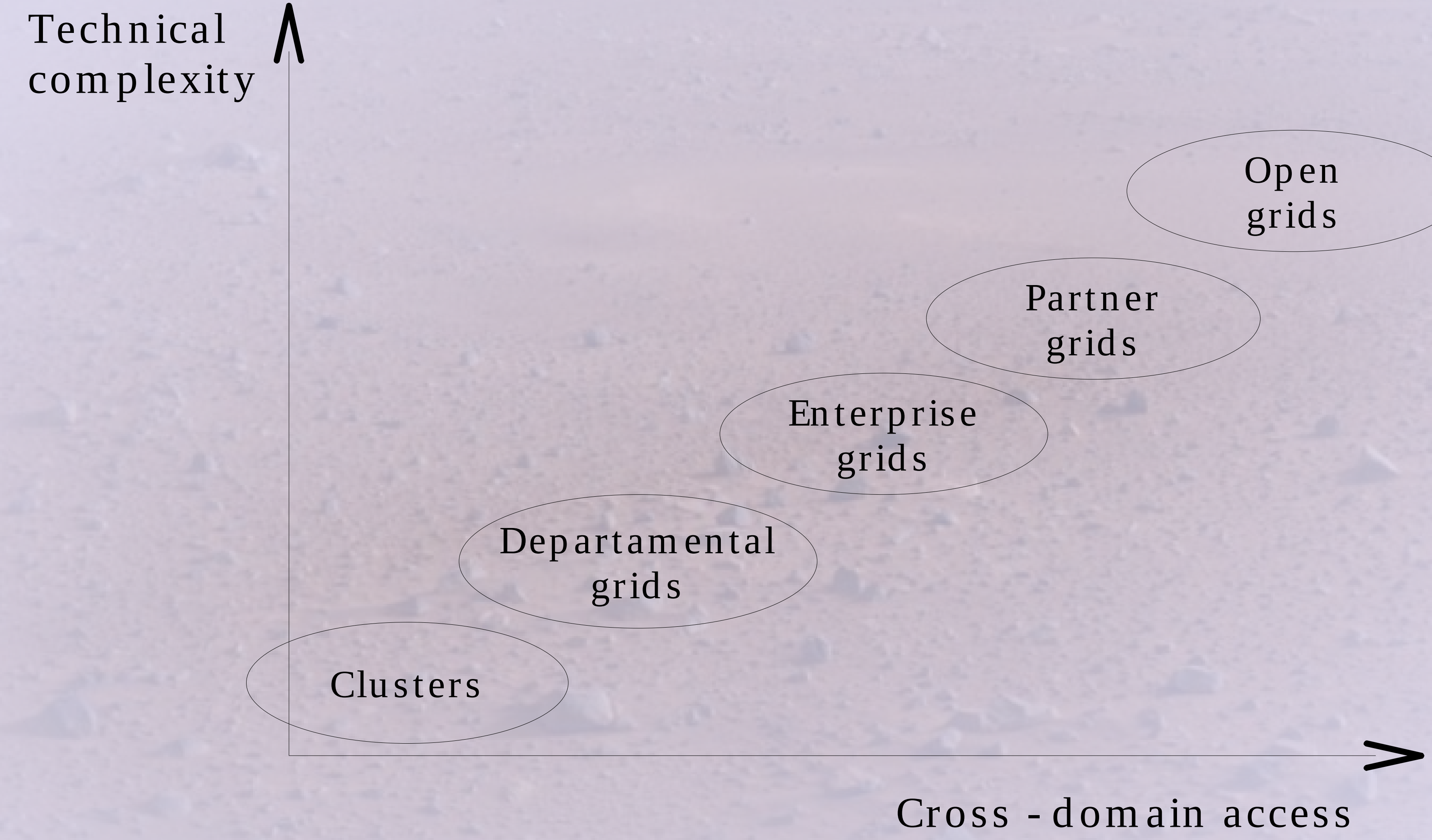
- Crash Course to Grid Computing
- Grid Security in Nutshell
- State-of-the-art
- Some Ideas

Grid computing?

Grid computing is about **virtualization of resources**, and on-demand provisioning of these resources in the utility model

gridwise tech

Taxonomy



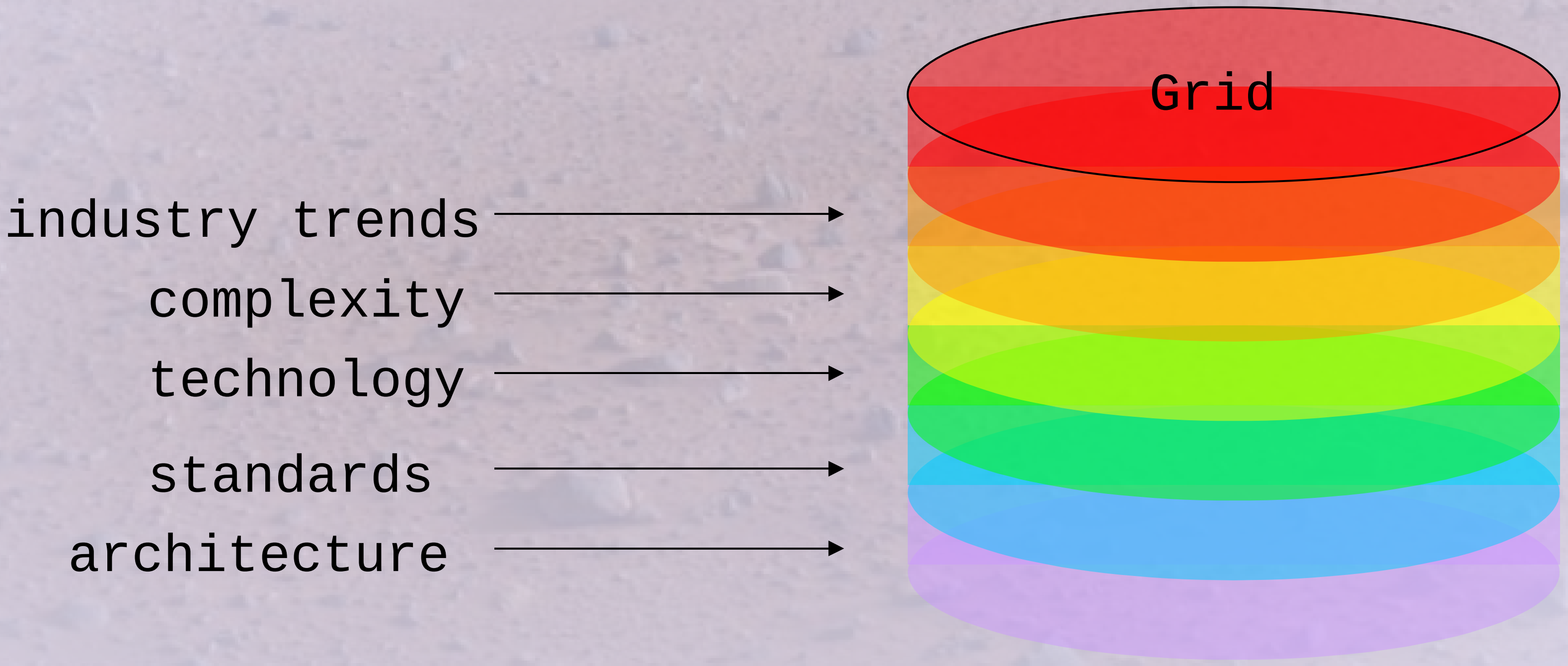
Technical complexity
Open grids
Partner grids
Enterprise grids
Departamental grids
Clusters
Cross - domain access

Advantages

- Virtualization and usage optimization of IT resources
- Saves
  - ✓ Cost
  - ✓ Speed
  - ✓ Work
- Introduces efficient collaboration environment
- Integration of large or highly distributed infrastructure
- Facilitation of data centers management

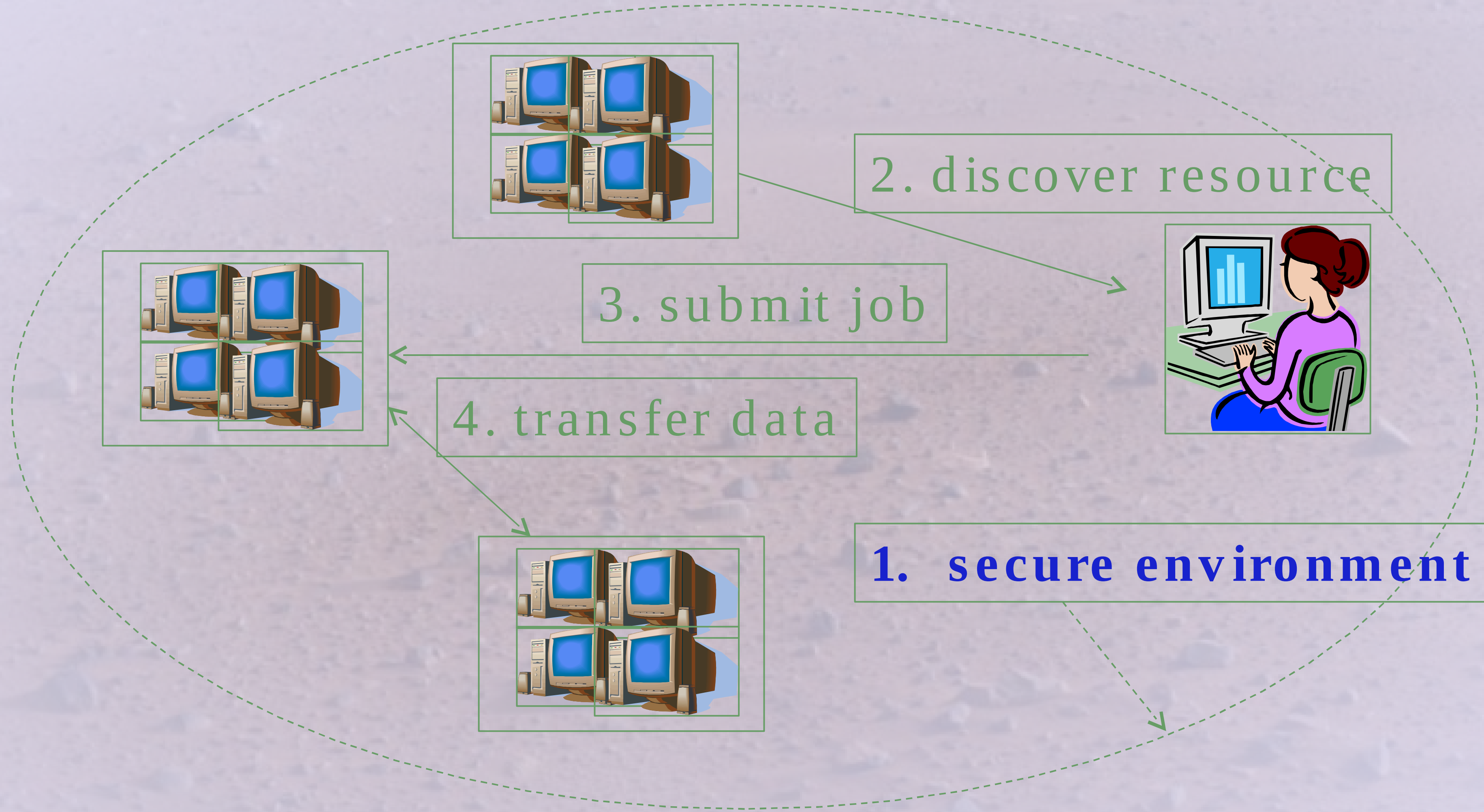
Understanding Grid Computing

The concept is difficult, as it is cross-cutting several layers of understanding.



gridwise tech

Grid Computing: Requirements



2. discover resource

3. submit job

4. transfer data

1. secure environment

gridwise tech

What is Grid Architecture?

- Three tier architecture
  - ✓ Presentation (access)
  - ✓ Service (could be multi-tiered SOA)
  - ✓ Resource
- Highly distributed (geographically and administratively) and loosely coupled
- Standard protocols & adherence to standard resource sharing procedures
- Scalable Virtual Organization security layer vertically cross-cutting the tiers
- Not application specific; can host many applications

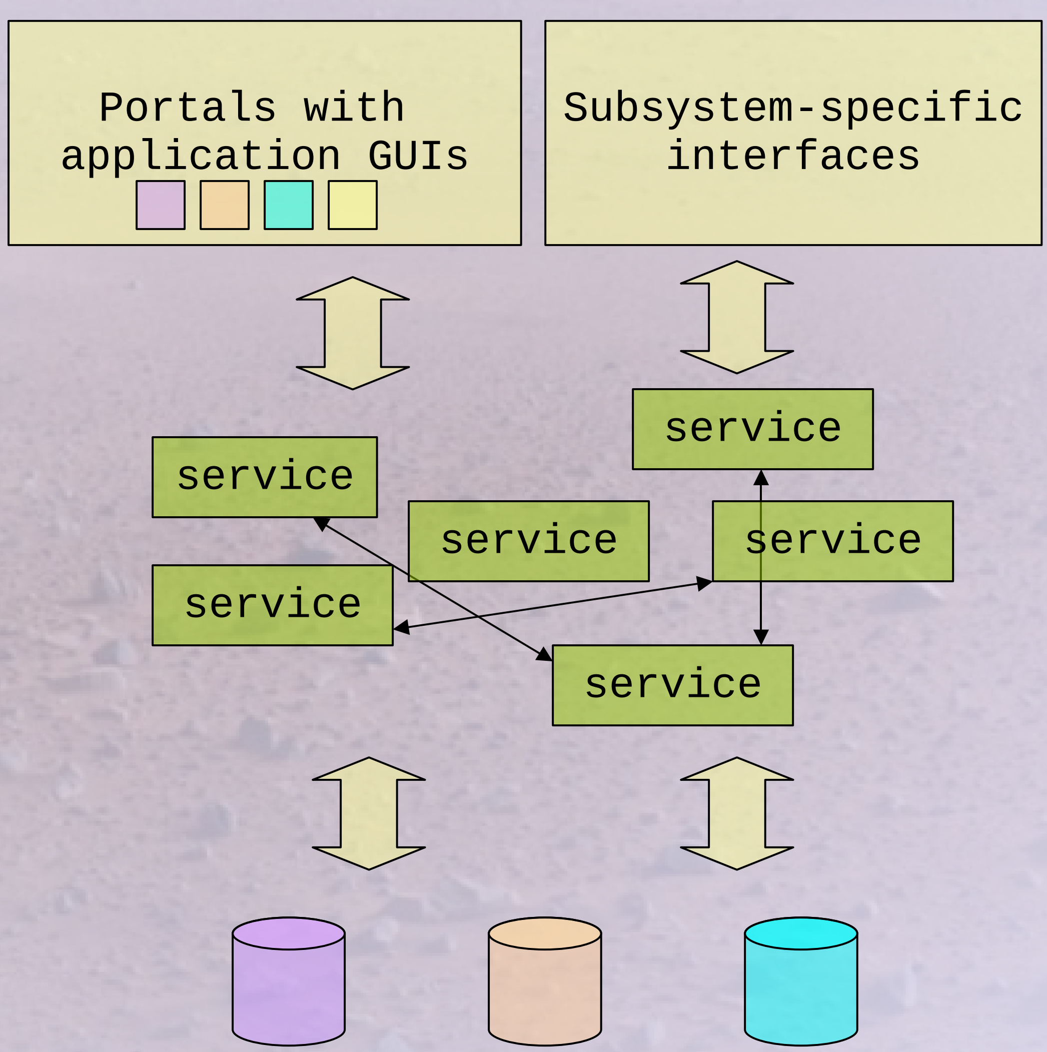
gridwise tech

Grid Architecture Diagram

PRESENTATION TIER
Location independent, infrastructure-transparent human access

SERVICE TIER
Multi-layered services represent resources, applications and Grid functional units to users

RESOURCE TIER
Resources use services as interfaces
To external world



Portals with application GUIs

Subsystem-specific interfaces

service

service

service

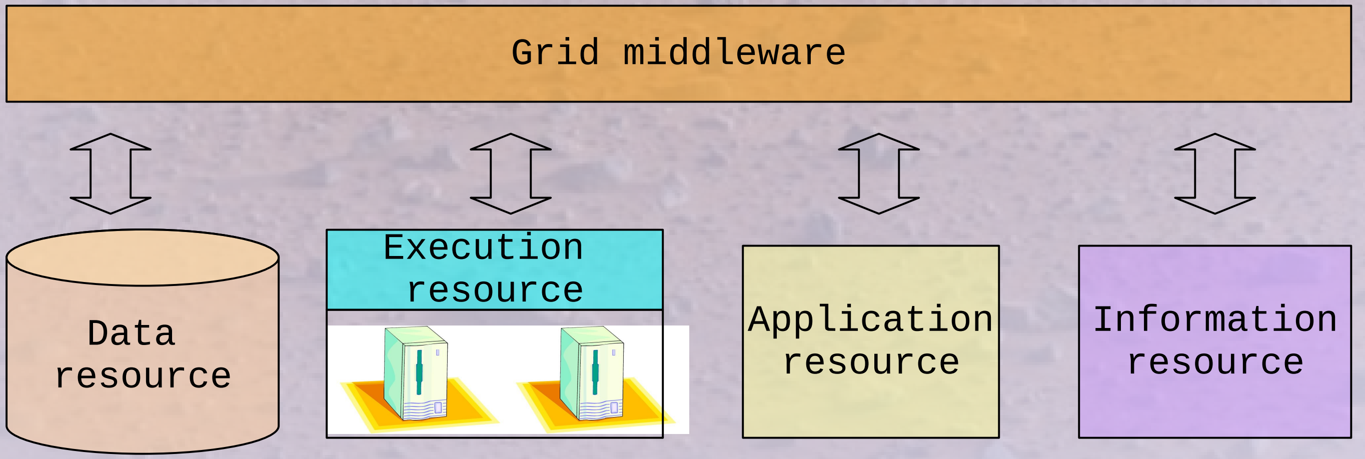
service

service

service

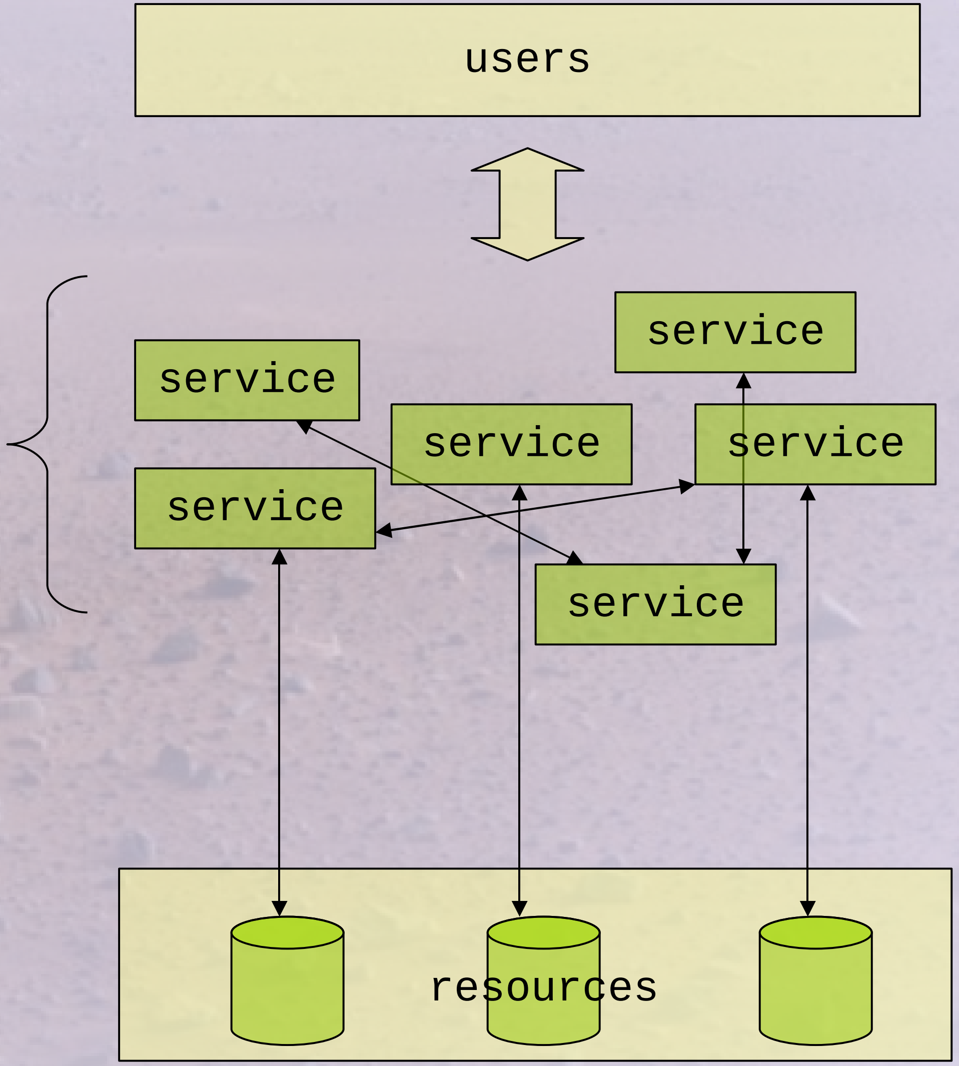
Grid Resources

- Distributed IT resources:
  - ✓ CPU, storage, network, application, administrative unit (UNIX account), information system
- Distribution can be geographic or administrative
- Grid helps share and access these resources in a controlled manner



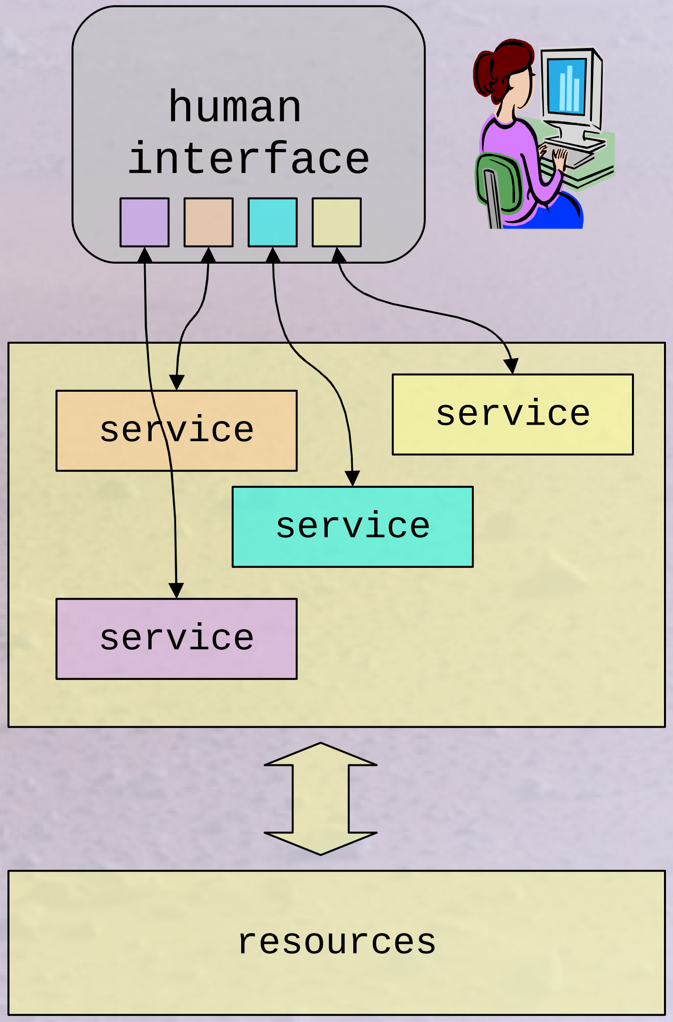
Grid Services

- We introduce Service Oriented Architecture to
  - ✓ Achieve resource virtualization
  - ✓ Enable users to access resources
  - ✓ Enable inter- application communication
  - ✓ Improve system maintenance and integration flexibility



Grid Presentation Layer

- Location independent
- Human-friendly interface to Grid services
- Implements end user security, and location specific GUIs
- Browser-accessible portals frequently used
  - ✓ Applicaction oriented portals – **the future!**
- Note: not all Grid systems need human interface



human interface

service

service

service

service

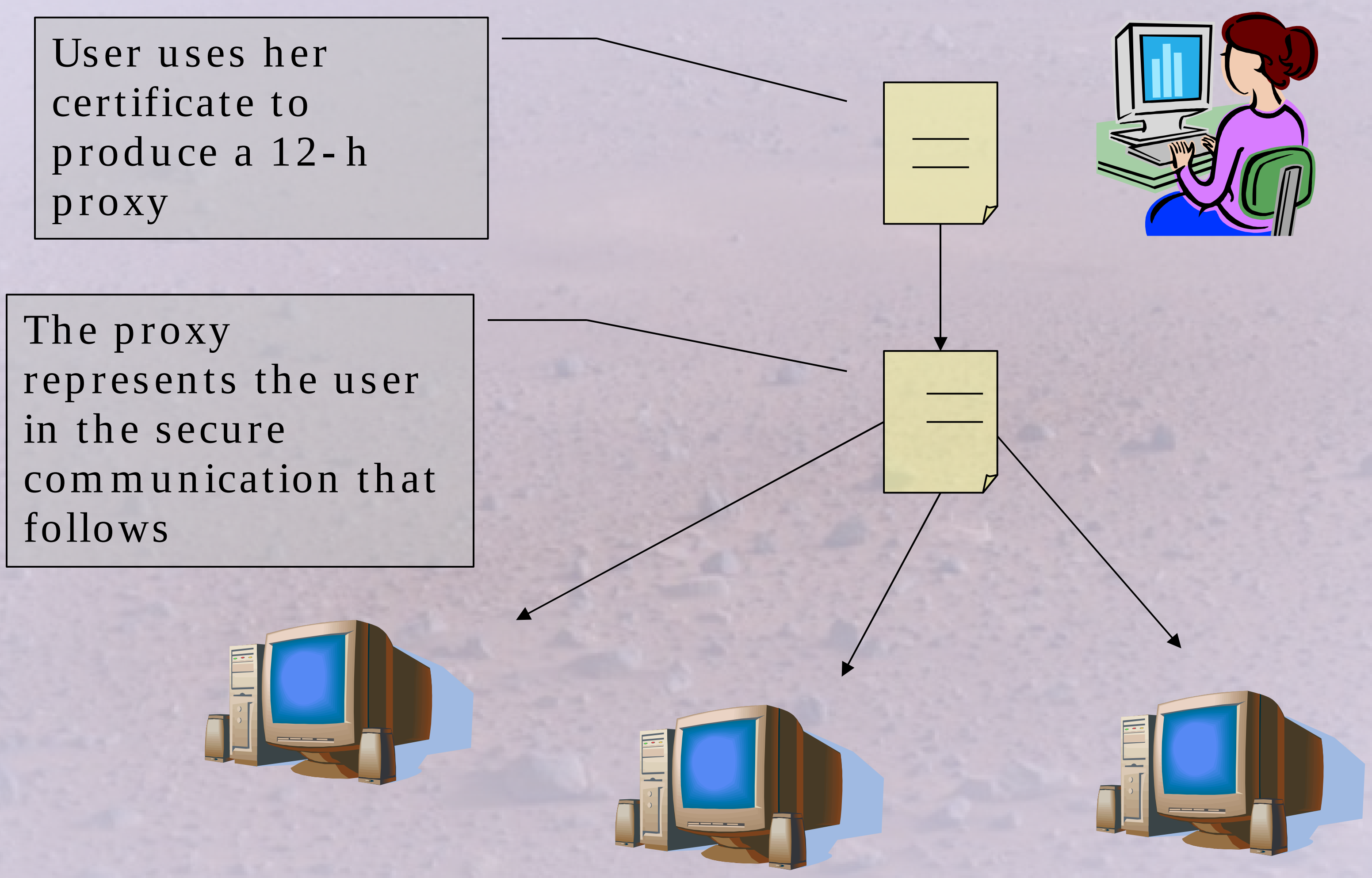
resources

gridwise tech

Grid Security: Requirements

- Single sign-on
- Mutual authentication
- Delegation (impersonation)
- Mutual trust domains
- Different users - different access permissions
- Support for multiple security mechanisms
- Dynamic establishment of trust domains

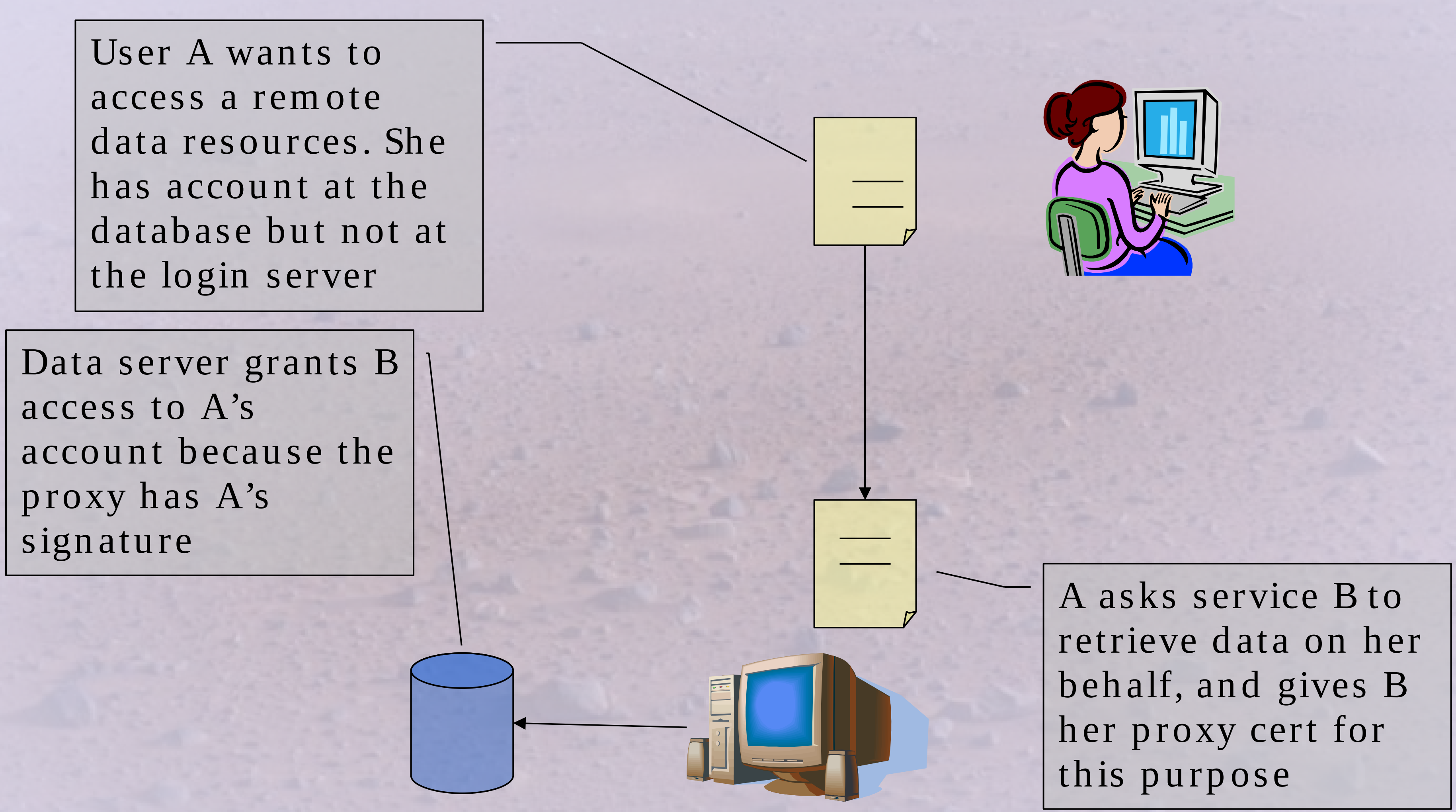
Single sign- on



User uses her certificate to produce a 12-h proxy

The proxy represents the user in the secure communication that follows

Delegation

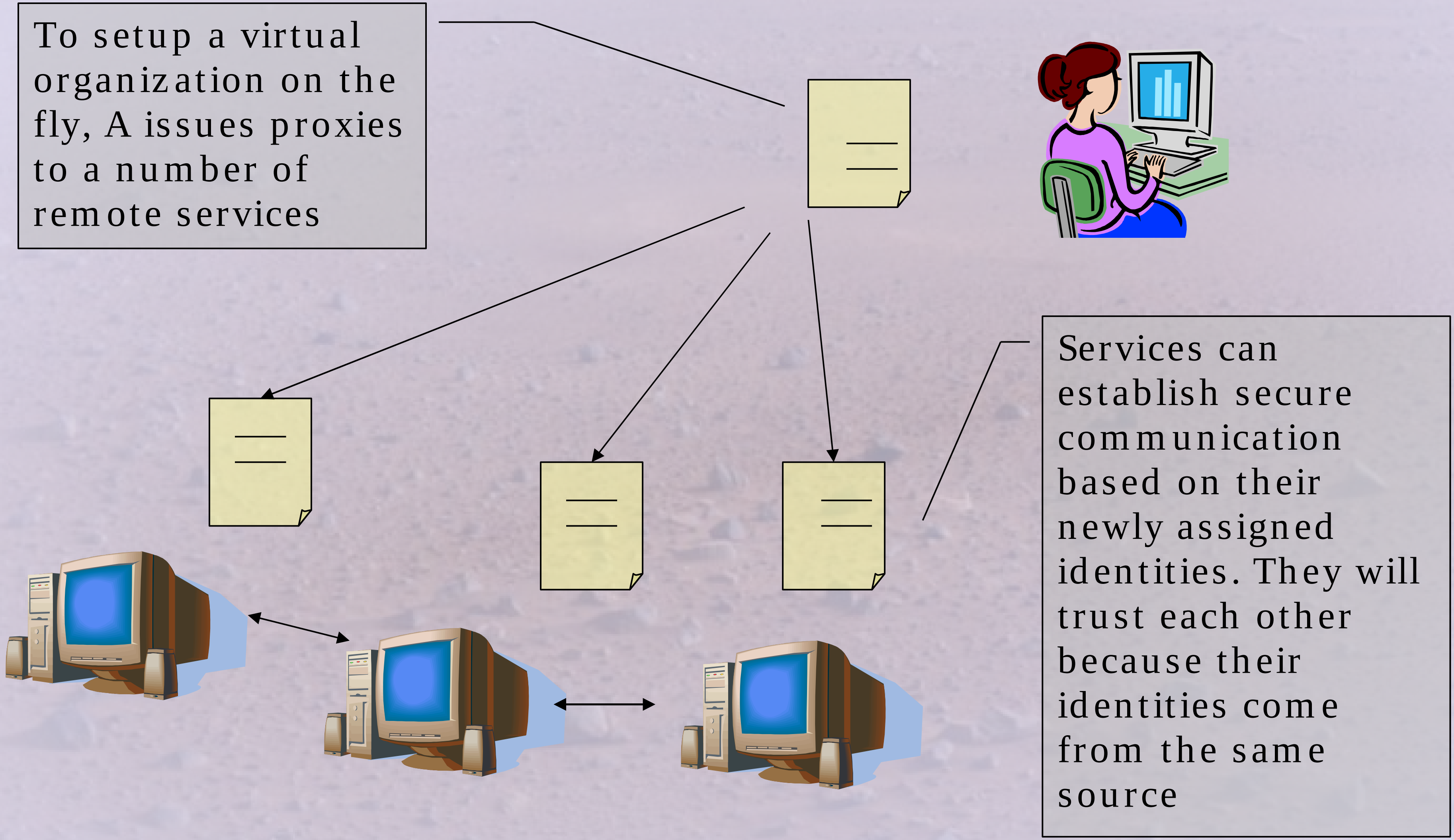


User A wants to access a remote data resources. She has account at the database but not at the login server

Data server grants B access to A’s account because the proxy has A’s signature

A asks service B to retrieve data on her behalf, and gives B her proxy cert for this purpose

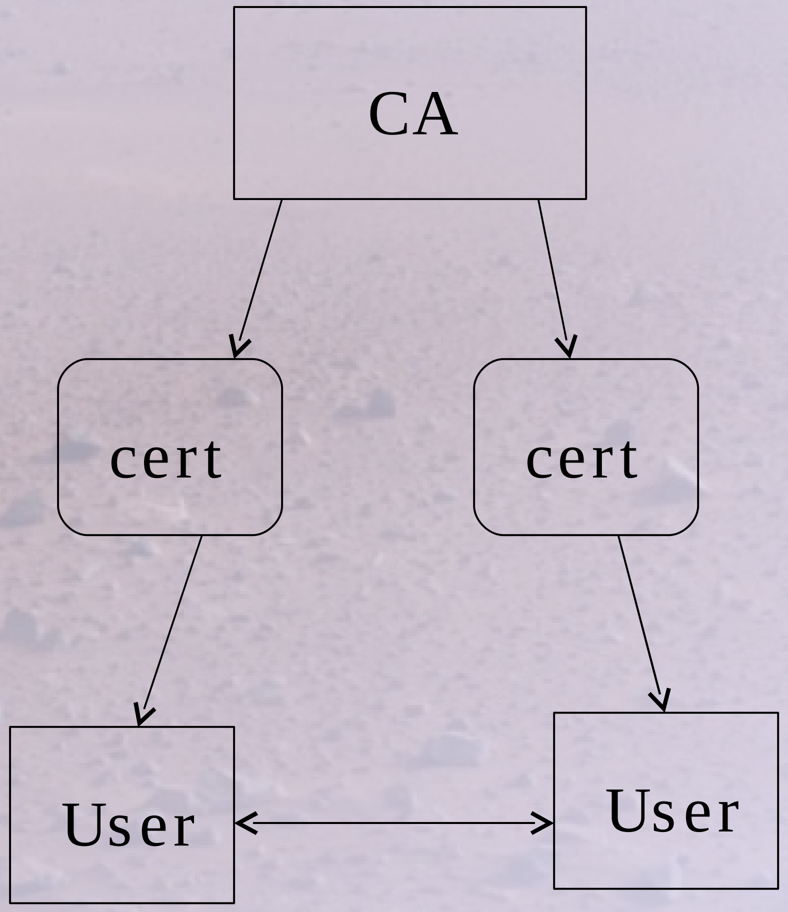
Mutual Trust Domains



To setup a virtual organization on the fly, A issues proxies to a number of remote services

Services can establish secure communication based on their newly assigned identities. They will trust each other because their identities come from the same source

Basic Facts about Grid Security Infrastructure



- Public Key Infrastructure (PKI)
- Certificate Authority (CA)
- TLS (SSL) / WS - Security

Virtual Organization

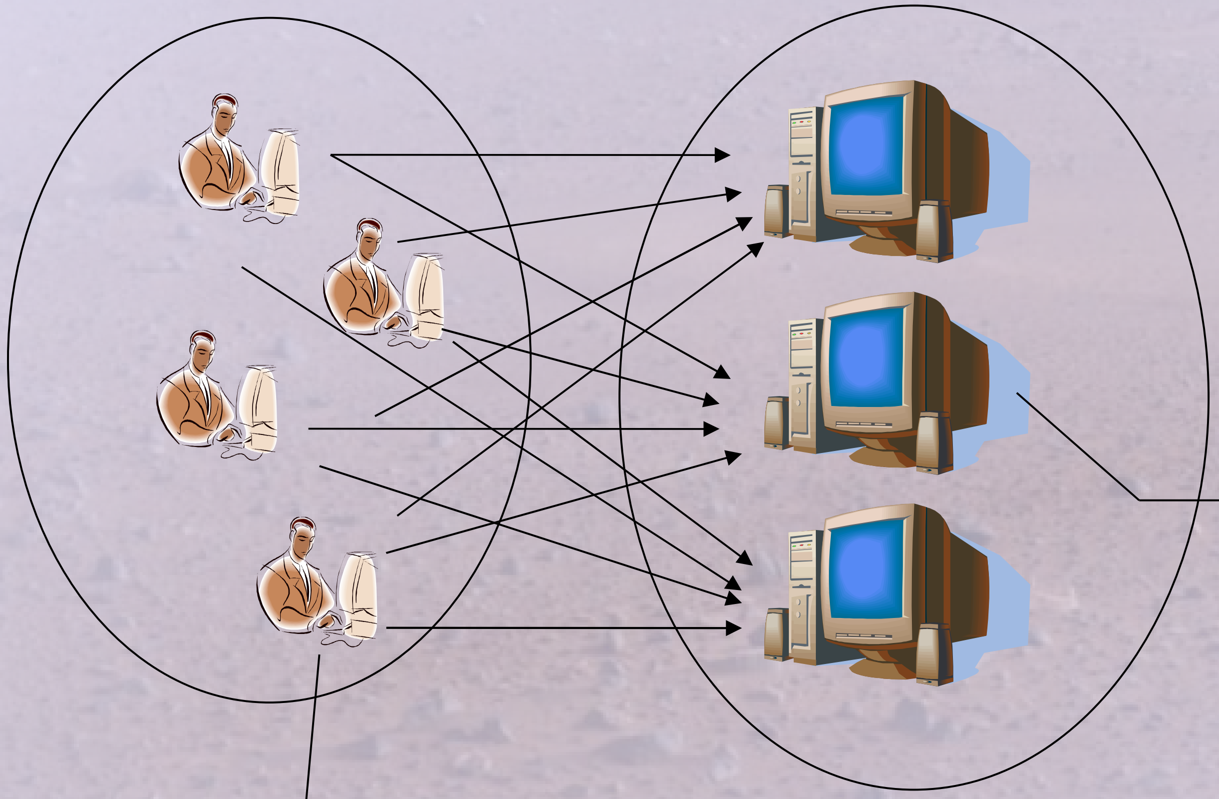
A Virtual Organization is a group of **individuals or institutions** who share the **computing resources** of a “grid” for a **common goal**.

Source: http://en.wikipedia.org/

- VOs are scalable, dynamic, distributed
- VOs dynamically create entities (services)
- VOs need to obey policies of local organizations

gridwise tech

Without VO

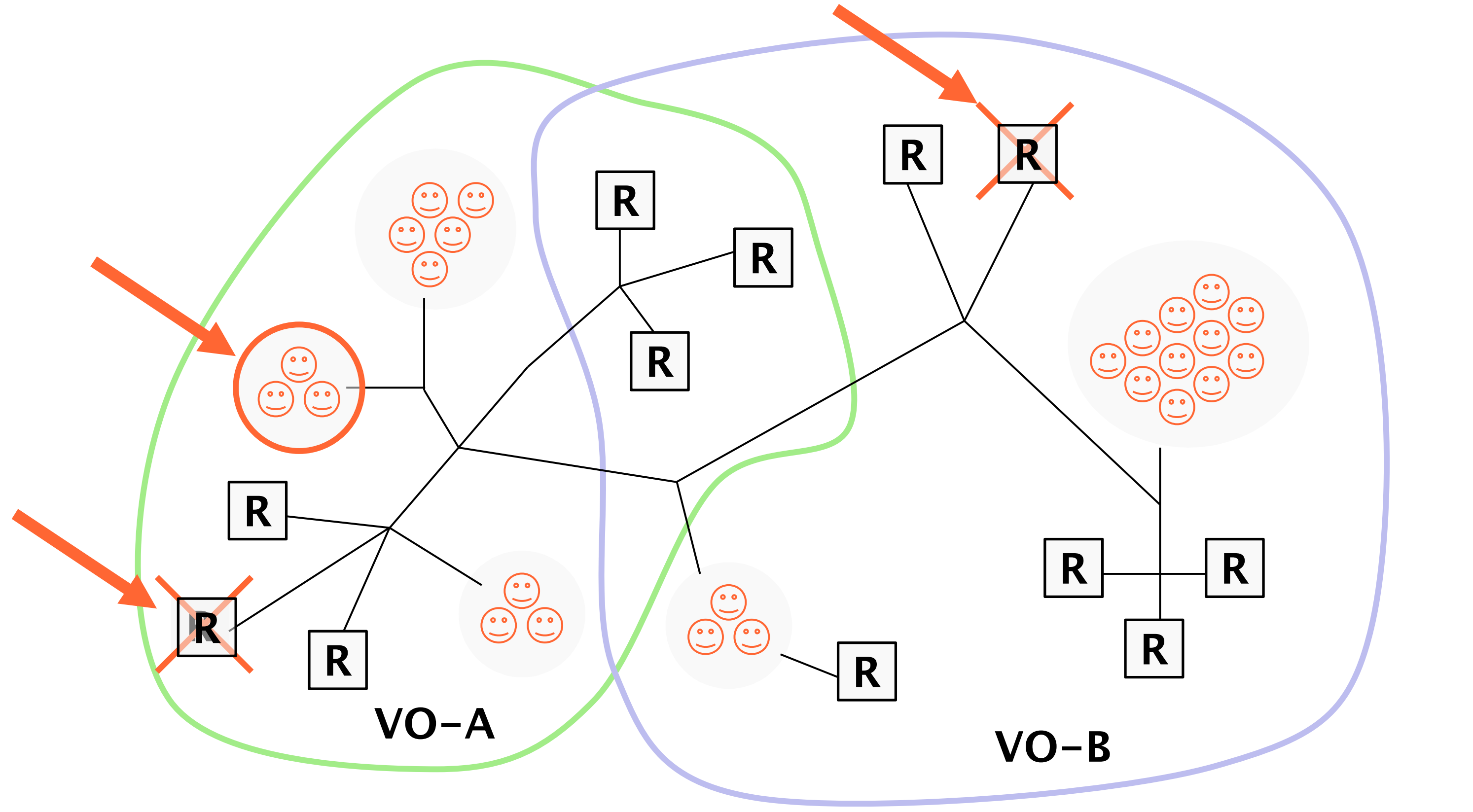


Resource maintains one account for each user

User accesses resource directly

gridwise tech

VO in action



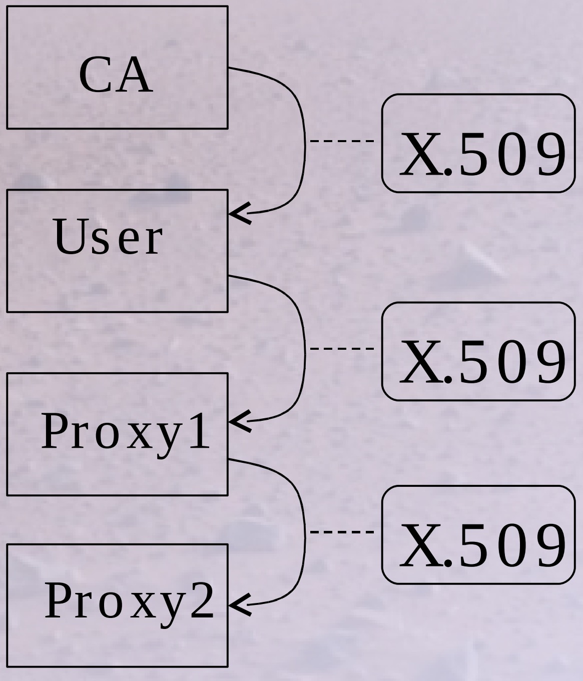
Source: Ian Foster, Globus Tutorial at e-Science

Some Interesting Solutions

- Community Authorization Service
- Grid Account Management Architecture
- Grid Authorization Service
- Higgins
- MyProxy
- PERMIS
- Shibboleth
- VOMS

MyProxy

- Credetial Management Service
  - do not store your credentials on your each client machine
  - store them in repository
  - retrieve a proxy credential
- Perfect solution for Grid portals
- Open Source



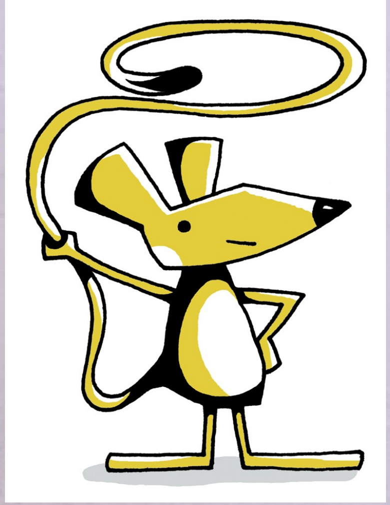
gridwise tech

Higgins

Software framework that integrates

- **identity** data
- **profile** data
- **relationship** data

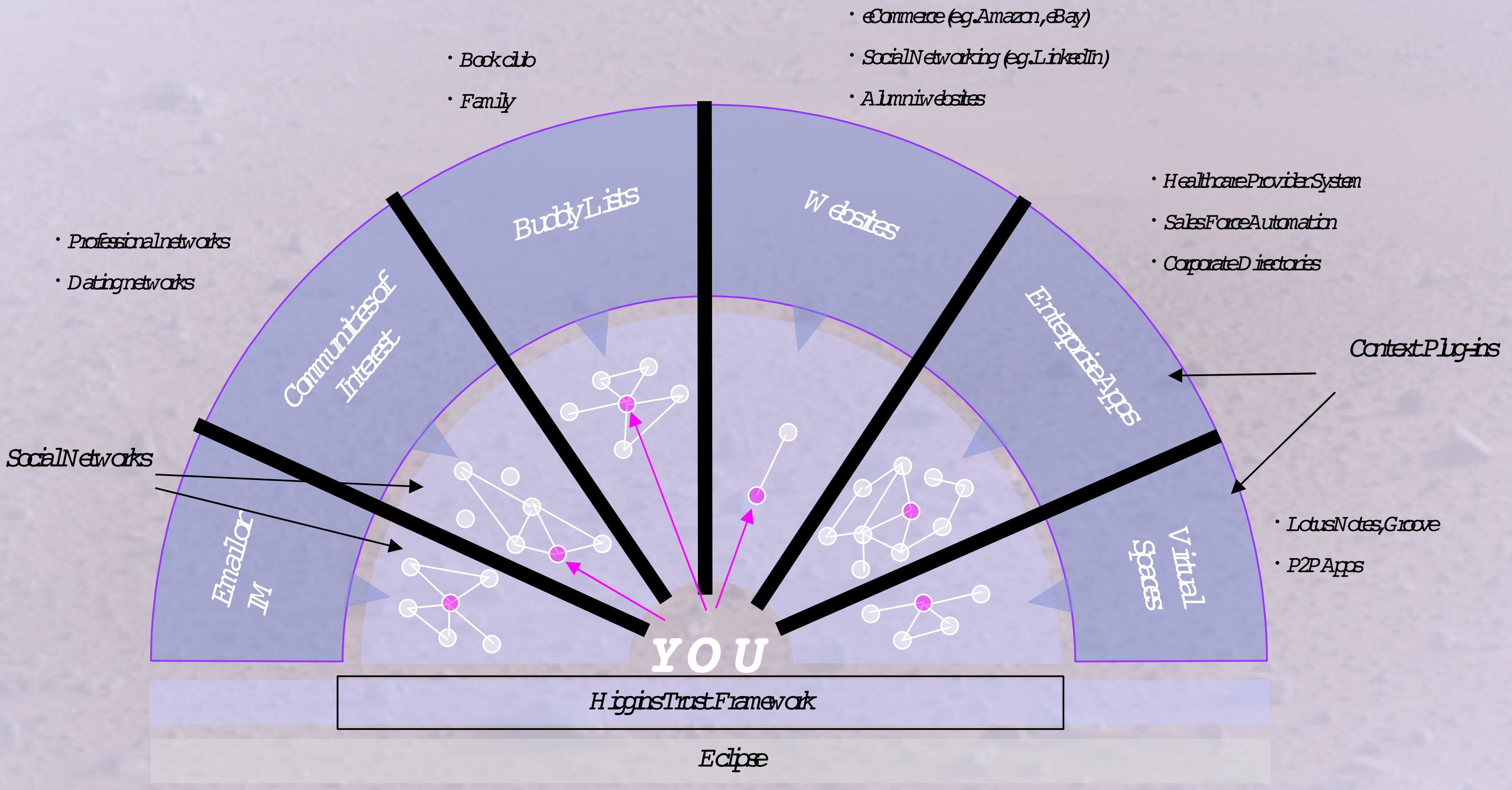
within and across multiple systems



- Eclipse: IBM, Novell, Parity Communications
- Open Source
- Java Reference Implementation (in the future)
- Extensible (plug-ins)

gridwise tech

Higgins: Why it is important?



- eCommerce (e.g. Amazon, eBay)
- Social Networking (e.g. LinkedIn)
- Alumni websites

- Book club
- Family

- Professional networks
- Dating networks

- Healthcare Provider System
- Sales Force Automation
- Corporate Directories

Context Plug-ins

Social Networks

- Lotus Notes, Groove
- P2P Apps

Buddy Lists

Websites

Communities of Interest

Enterprise Apps

Email or IM

Virtual Spaces

YOU

Higgins Trust Framework

Eclipse

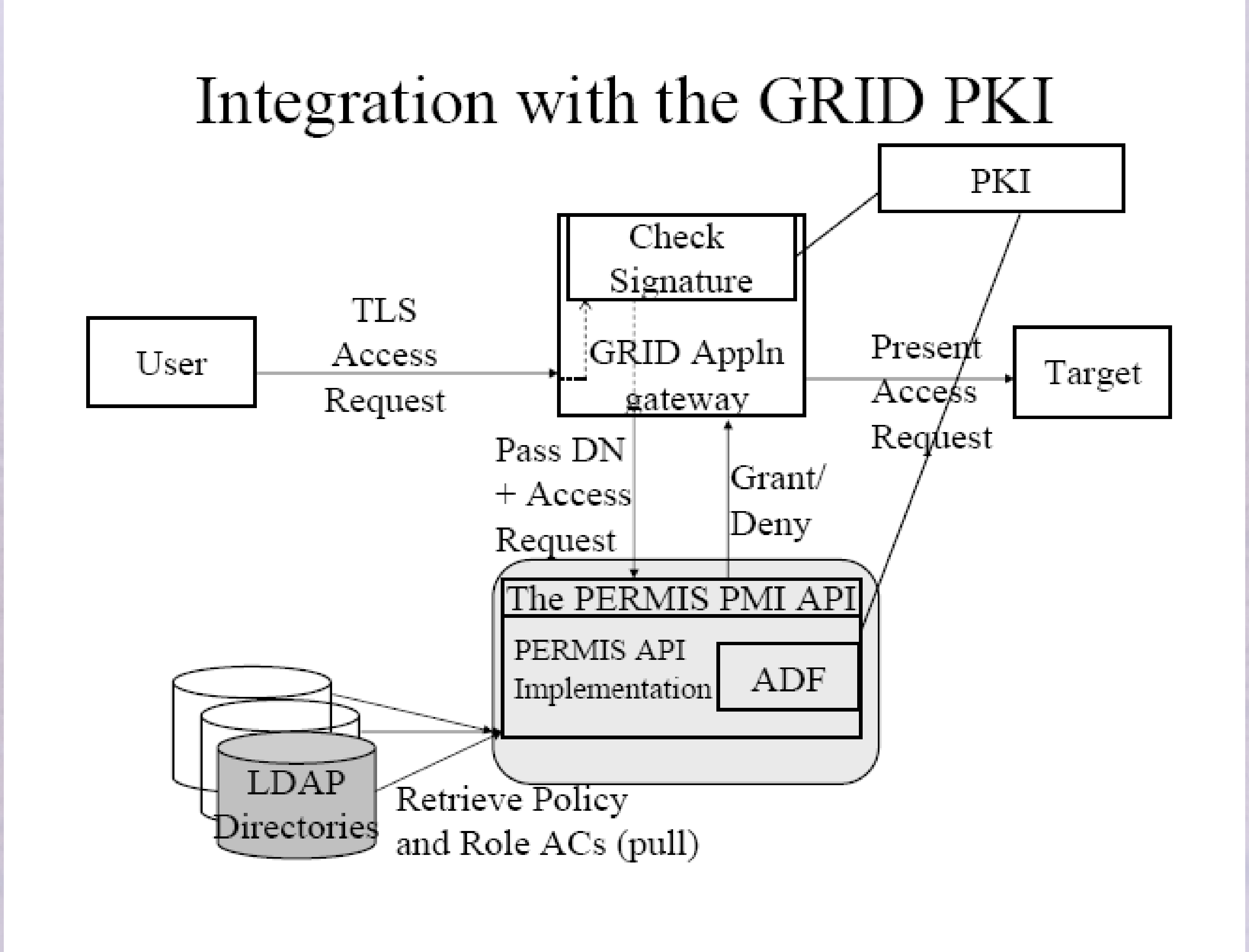
Source: Higgins Trust Framework, {mary,paul}@socialphysics.org

gridwise tech

PERMIS

- policy based authorization system (RBAC)
- uses X.509 attribute certificates to hold roles/ attributes
- PMI + PKI
- University of Salford (?), sponsored by EC (?)
- Standards based, flexible (X.509, LDAP)
- Open Source (but watch out!)

PERMIS: Usage Scenario



Integration with the GRID PKI

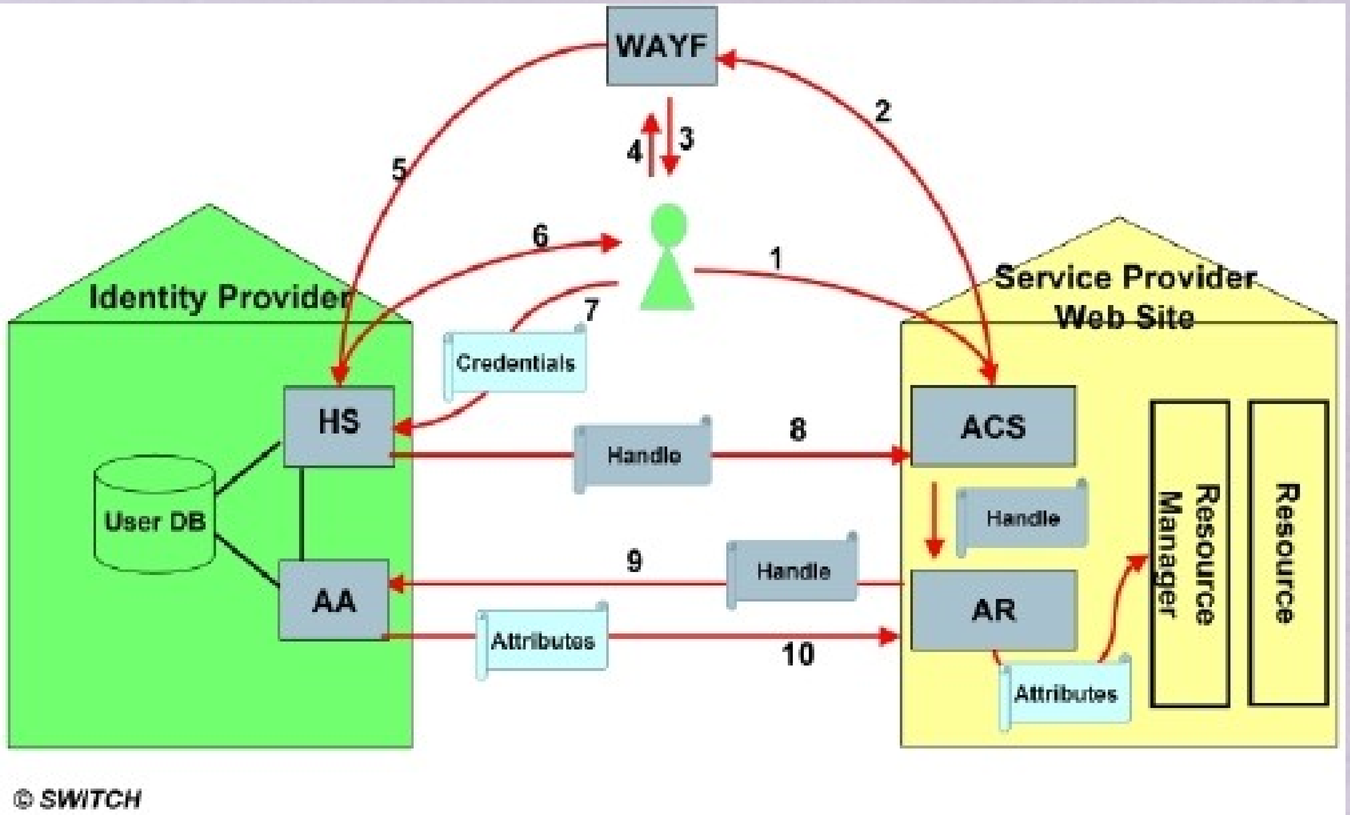
Source: David Chadwick, The EC PERMIS Project

Shibboleth

- Internet2 consortium (universities, industry, gov)
- Standards based, but flexible
- Open Source
- Large set of Shibboleth- enabled products
- Attribute - based Authorization
- **SSO, decent user privacy**
- **Simple trust model, no support for RBAC**

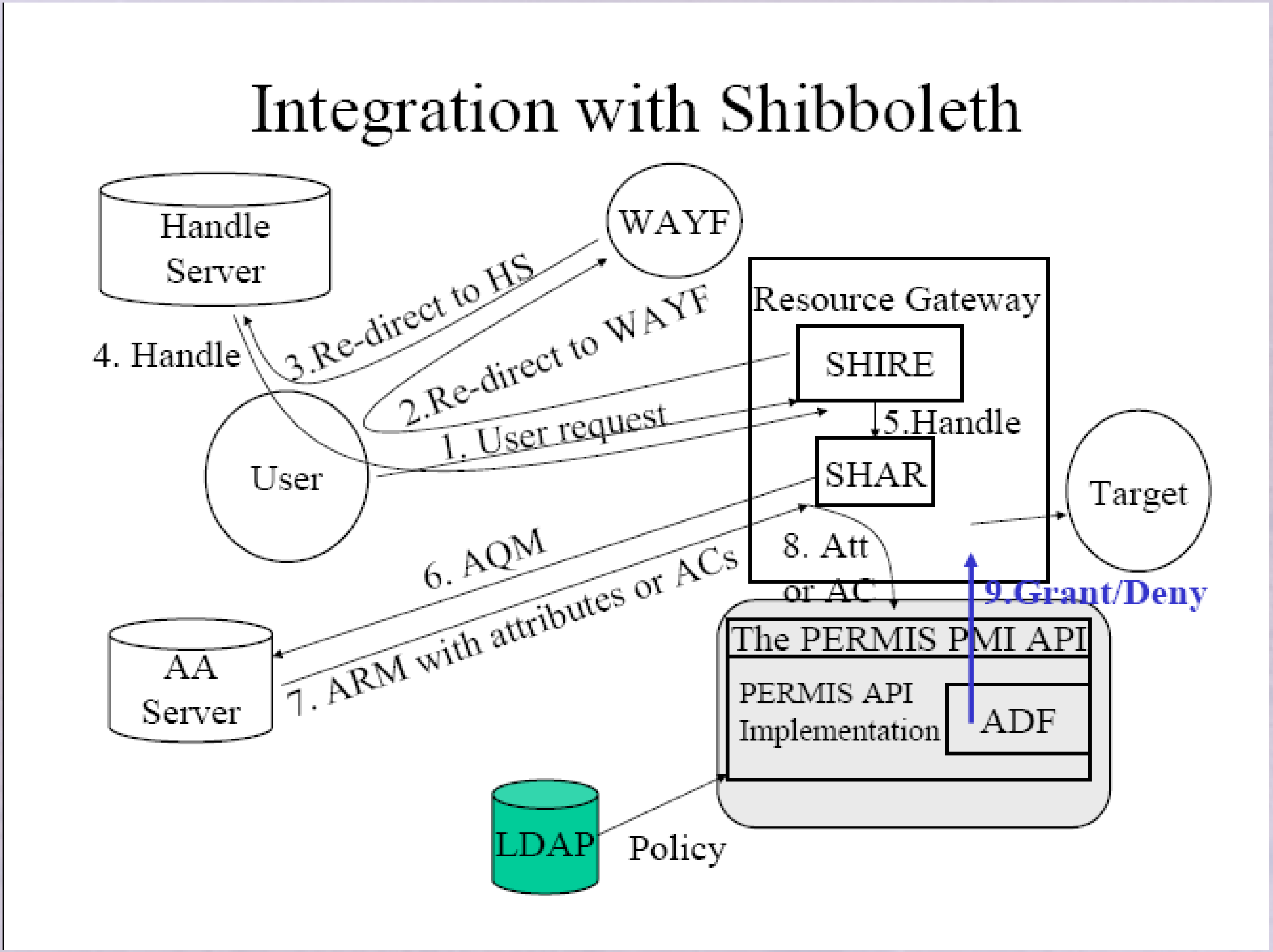
gridwise tech

Shibboleth: Usage Scenario



Source: http://www.switch.ch/

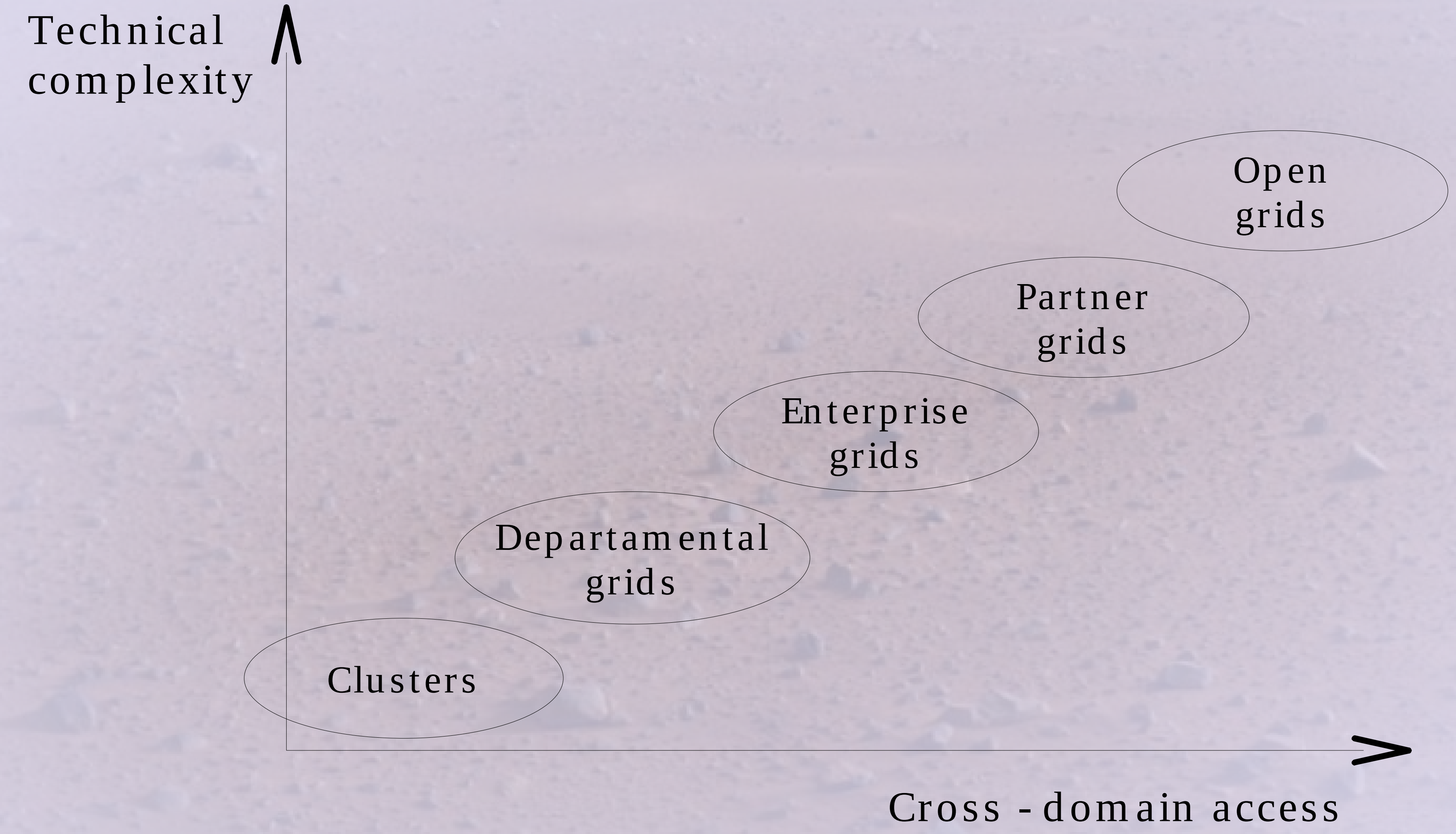
PERMIS + Shibboleth



Integration with Shibboleth

Source: David Chadwick, The EC PERMIS Project

Taxonomy once again



Technical complexity

Open grids

Partner grids

Enterprise grids

Departamental grids

Clusters

Cross-domain access

The Challenge

- which services are available?
- what capabilities do they have?
- which resources may authorize me?
- where my tasks may be executed correctly?

- should I allow this user to run this computations?
- how important her tasks are?

gridwise tech

Trust

- French hard rock band?

- Allow without fear? (WordNet)

Source: http://en.wikipedia.org/

Trust in sociology is a **relationship between people**. It involves the suspension of disbelief that one person will have towards another person or idea. It especially involves having one person thinking that **the other person or idea is benevolent**, competent / good, or honest / true.

Source: http://en.wikipedia.org/

Reputation

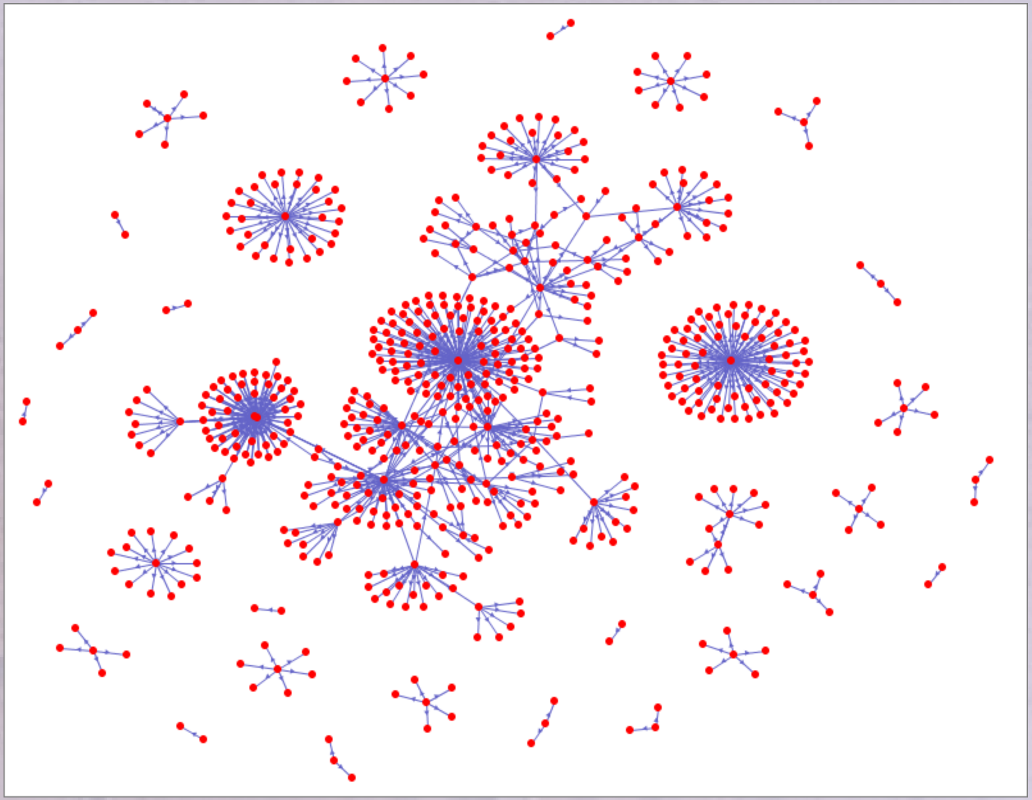
Reputation is the **general opinion** of the **public** towards a person, a group of people, or an organization. It is an important factor in many fields, such as business, **online communities** or social status.

Source: http://en.wikipedia.org/

gridwise tech

Online Reputation

- eBay / Allegro
- LinkedIn / grono
- Amazon / Merlin
- Forums
- Google
- Wikipedia?
- Grid computing?



Source: http://trust.mindswap.org/

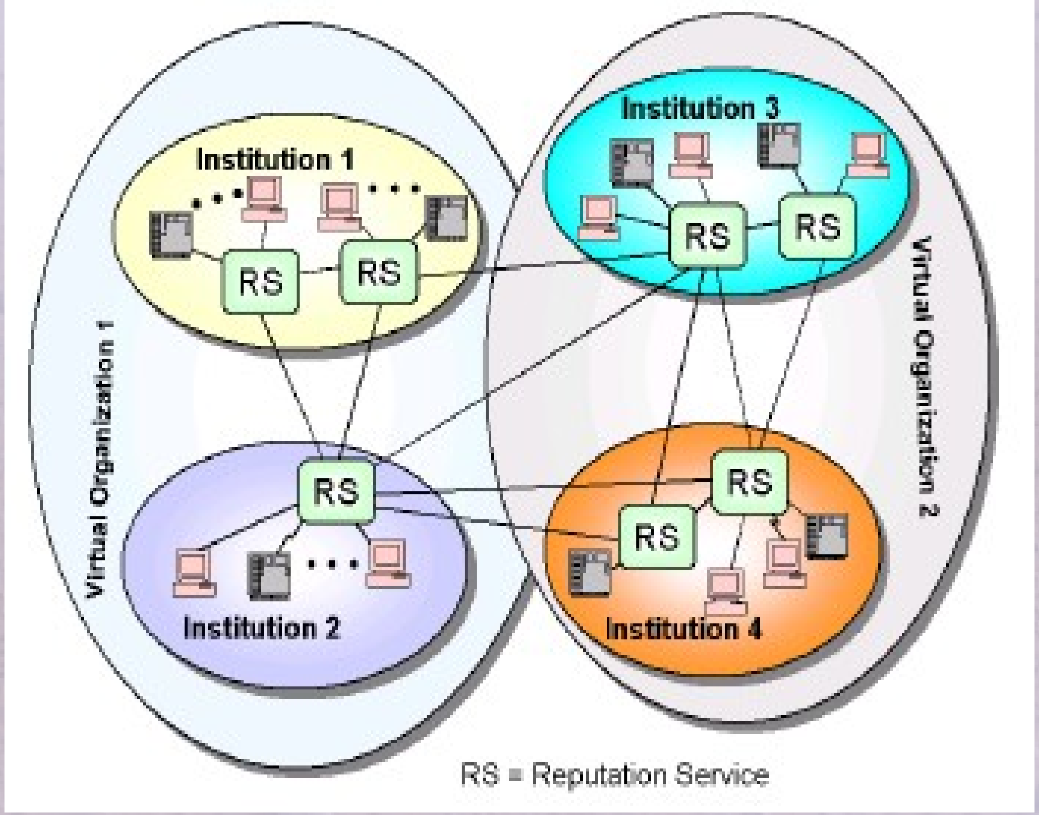
gridwise tech

Reputation Metrics Features

- No authority given *a priori*
- Feedback and responsibility
- Decentralization
- Considering both direct experience and recommendation

gridwise tech

Reputation Based Authorization



Source: Reputation-Based Grid Resource Selection

Summary

- Grid technologies **are secure**
  - They provide the same security level as other network technologies
- Grid technologies provide many mechanisms supporting **cross- domain collaboration**
- Grid technologies are not yet ready for a truly **open environment**

gridwise tech

Thank you!

- Questions?
- Continue on **http://jakub.dziwisz.org/**

gridwise tech