

UNICORE Security

practised security in Grid Computing

Michael Rambadt , Achim Streit , Jules Wolfrat 

`m.rambadt@fz-juelich.de`

`a.streit@fz-juelich.de`

`wolfrat@sara.nl`

29. September 2005



Forschungszentrum Jülich
in der Helmholtz-Gesellschaft

Overview

- ▶ DEISA project
- ▶ Grid projects at Research Centre Jülich (FZJ)
- ▶ UNICORE – general aspects and architecture
- ▶ UNICORE meets DEISA
- ▶ UNICORE Security
 - ▶ Client
 - ▶ Gateway – Authentication
 - ▶ Network Job Supervisor (NJS) – Authorisation
- ▶ UNICORE @ Sourceforge
- ▶ Future Prospects



The DEISA Consortium



DEISA



EUGridPMA, Poznan, September 29, 2005

DEISA objectives



- *To enable Europe's terascale science by the integration of Europe's most powerful supercomputing systems.*
- *Enabling scientific discovery across a broad spectrum of science and technology is the only criterion for success*
- DEISA is an European Supercomputing Service built on top of existing national services.
- DEISA deploys and operates a persistent, production quality, distributed supercomputing environment with continental scope.

THE DEISA SUPERCOMPUTING GRID



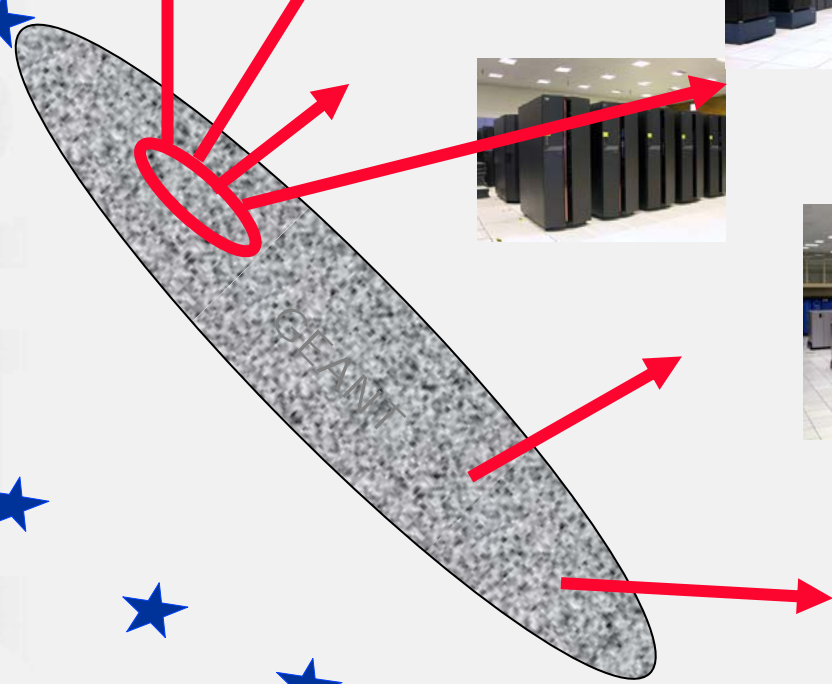
**AIX distributed
super-cluster**



**Vector systems
(NEC, ...)**



**Linux systems
(SGI, IBM, ...)**



The DEISA supercomputing Grid: a layered infrastructure

- Inner layer: a distributed super-cluster resulting from the deep integration of similar IBM AIX platforms at IDRIS, FZ-Julich, RZG-Garching and CINECA (phase 1) then CSC (phase 2). It looks to external users as a single supercomputing platform.
- Outer layer: a heterogeneous supercomputing Grid:
 - IBM AIX super-cluster (IDRIS, FZJ, RZG, CINECA, CSC) close to 24 Tf
 - BSC, IBM PowerPC Linux system, 40 Tf
 - LRZ, Linux cluster (2.7 Tf) moving to SGI ALTIX system (33 Tf in 2006, 70 Tf in 2007)
 - SARA, SGI ALTIX Linux cluster, 2.2 Tf
 - ECMWF, IBM AIX system, 32 Tf
 - HLRS, NEC SX8 vector system, close to 10 Tf

Technologies deployed

- Batch systems integrated between core sites (Loadleveler-MC)
- Transparent data access - *Global file system*
 - GPFS (MC) on IBM systems - high performance parallel filesystem, high throughput network needed between sites to achieve performance - dedicated network between sites, currently provided by GEANT and NRENs (1Gbps)
 - AFS (if GPFS not available)
- UNICORE for job submission in heterogeneous environment

UNICORE

- ▶ UNICORE: **UN**iform Interface to **CO**mputer **RE**sources
- ▶ Development started in 1997
- ▶ UNICORE and UNICORE Plus projects were funded by the German Ministry for Education and Research (until December 2002)
- ▶ Partners: German Research Centres, Universities and one software company
- ▶ Further UNICORE developments in several EU funded projects



Grid Projects based on UNICORE at FZJ

- ▶ UNICORE 08/1997-12/1999
- ▶ UNICORE Plus 01/2000-12/2002
- ▶ EUROGRID 11/2000-01/2004

- ▶ GRIP 01/2002-02/2004
- ▶ OpenMolGRID 09/2002-02/2005
- ▶ VIOLA 05/2004-04/2007
- ▶ DEISA 05/2004-04/2008
- ▶ UniGrids 07/2004-06/2006



UNICORE



EUROGRID



UNICORE

- ▶ Seamless, secure, and intuitive access to distributed resources and data
- ▶ A vertically integrated Grid system used in production and projects
- ▶ is used in projects, testbeds and production
- ▶ is interoperable with other Grid software (e.g. GT2.4, CONDOR)
- ▶ is developed towards OGSA-based UNICORE/GS with WS-RF interoperability

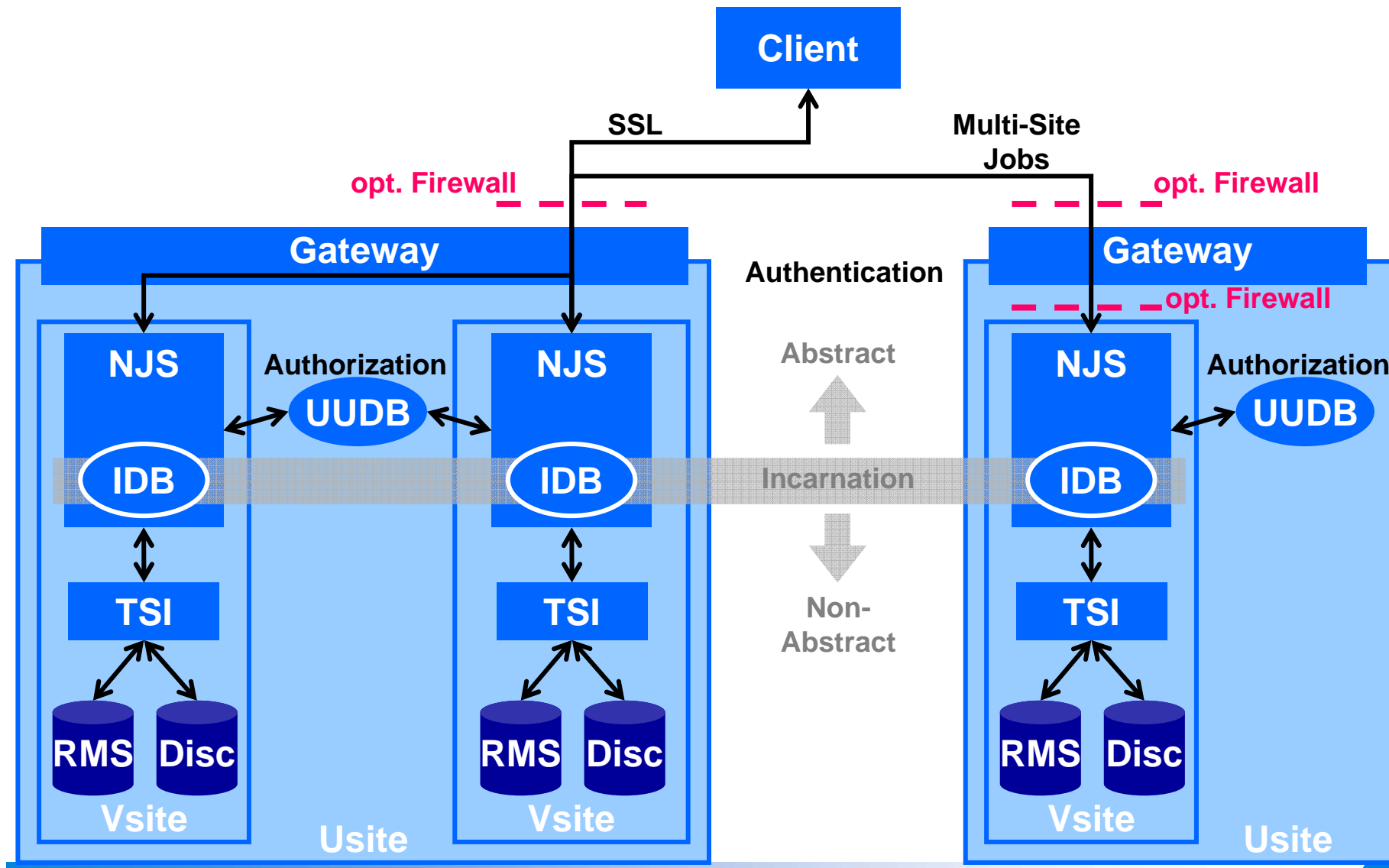




- ▶ Features
 - ▶ Intuitive GUI with single sign-on
 - ▶ X.509 certificates for AA and job/data signing
 - ▶ only one opened port in firewall required
 - ▶ workflow engine for
 - ▶ complex multi-site
 - ▶ multi-step workflows
 - ▶ job monitoring
 - ▶ extensible application support
 - ▶ secure data transfer integrated
 - ▶ resource management
 - ▶ easy installation and configuration of client and server components
 - ▶ full control of resources remains
 - ▶ production quality, ...



UNICORE Architecture

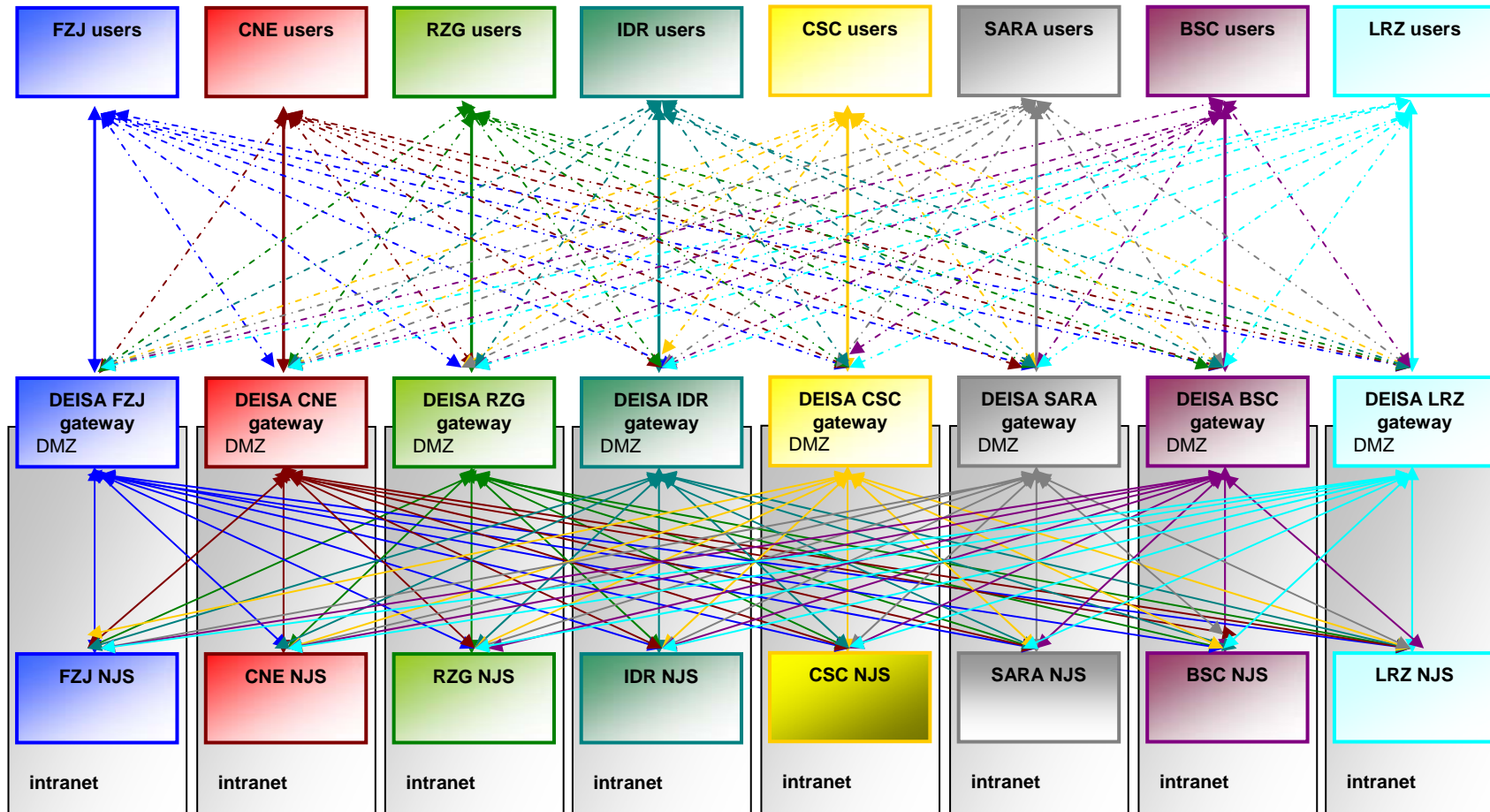


UNICORE Client

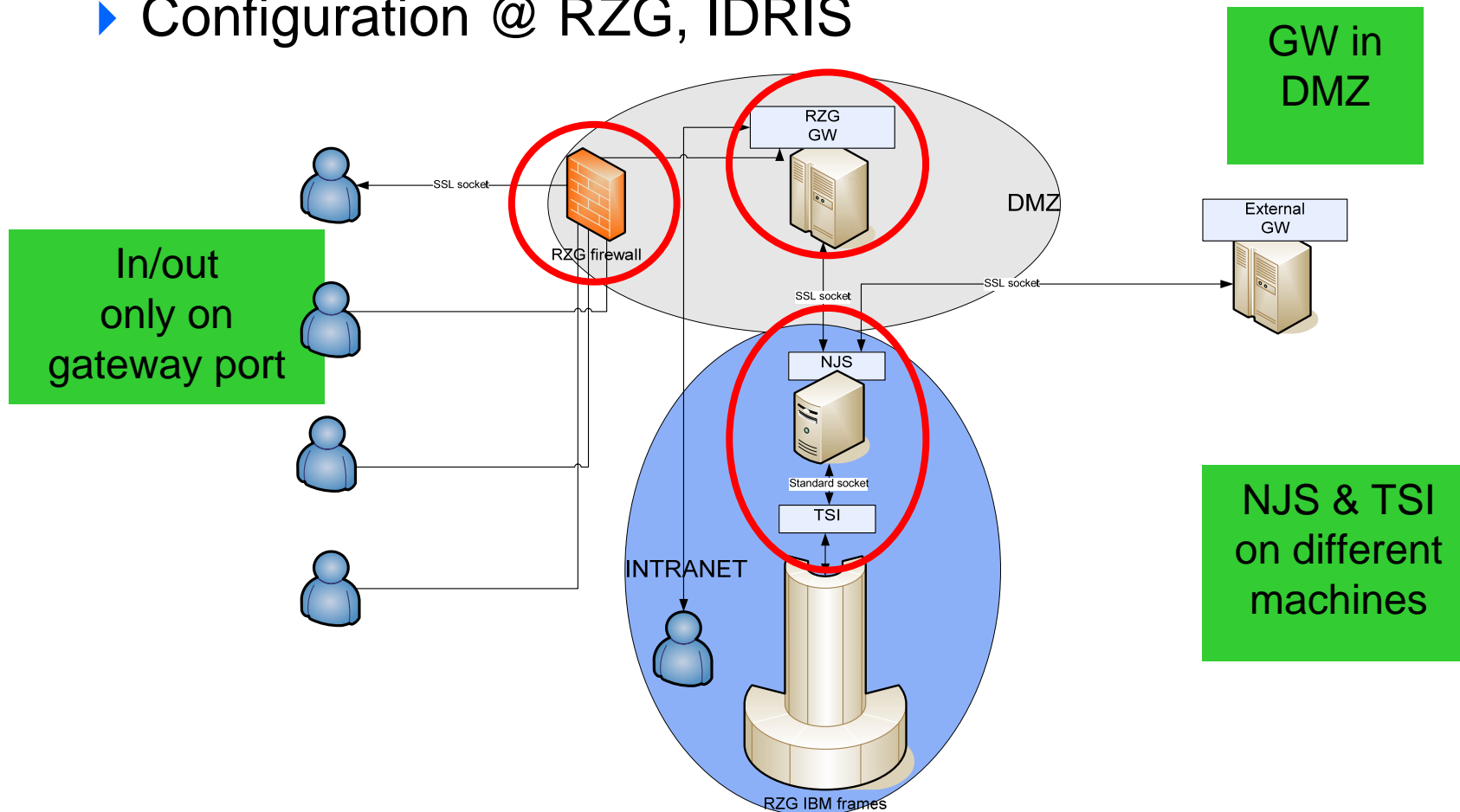
The screenshot shows the UNICORE Client interface with several callouts:

- Job Preparation:** A callout pointing to the 'Job Preparation' pane on the left, which shows a tree view of a job named 'New_DEISAJob' with sub-tasks 'New_DoN1', 'Loop1', and 'Pow_Ray'.
- Usites:** A callout pointing to the 'UNICORE Site' list in the middle pane, which includes sites like DEISA_BSC, DEISA_CSC, DEISA_Cineca, DEISA_FZJ, DEISA_Idris, DEISA_LRZ, DEISA_RZG, DEISA_Sara, FZ-Juelich, and VIOLA CAESAR.
- Workflow Management:** A callout pointing to the 'Task Dependencies' graph in the right pane, which shows a dependency between 'New_DoN1' and 'Pow_Ray'.
- Job Monitoring:** A callout pointing to the 'Job Monitoring' pane at the bottom left, which lists various sites like DEISA_BSC, DEISA_CSC, DEISA_Cineca, DEISA_FZJ, DEISA_Idris, DEISA_LRZ, DEISA_RZG, and DEISA_Sara.
- Vsites:** A callout pointing to the 'Virtual Site' list in the middle pane, which includes sites like BSC Marenostrum <NJS>, CINECA SP5 <NJS>, CSC <NJS>, FZJ JUMP <NJS>, IDRIS ZAHIR <NJS>, LRZ Altix <NJS>, RZG SP4 <Globus>, and SARA ASTER <NJS>.

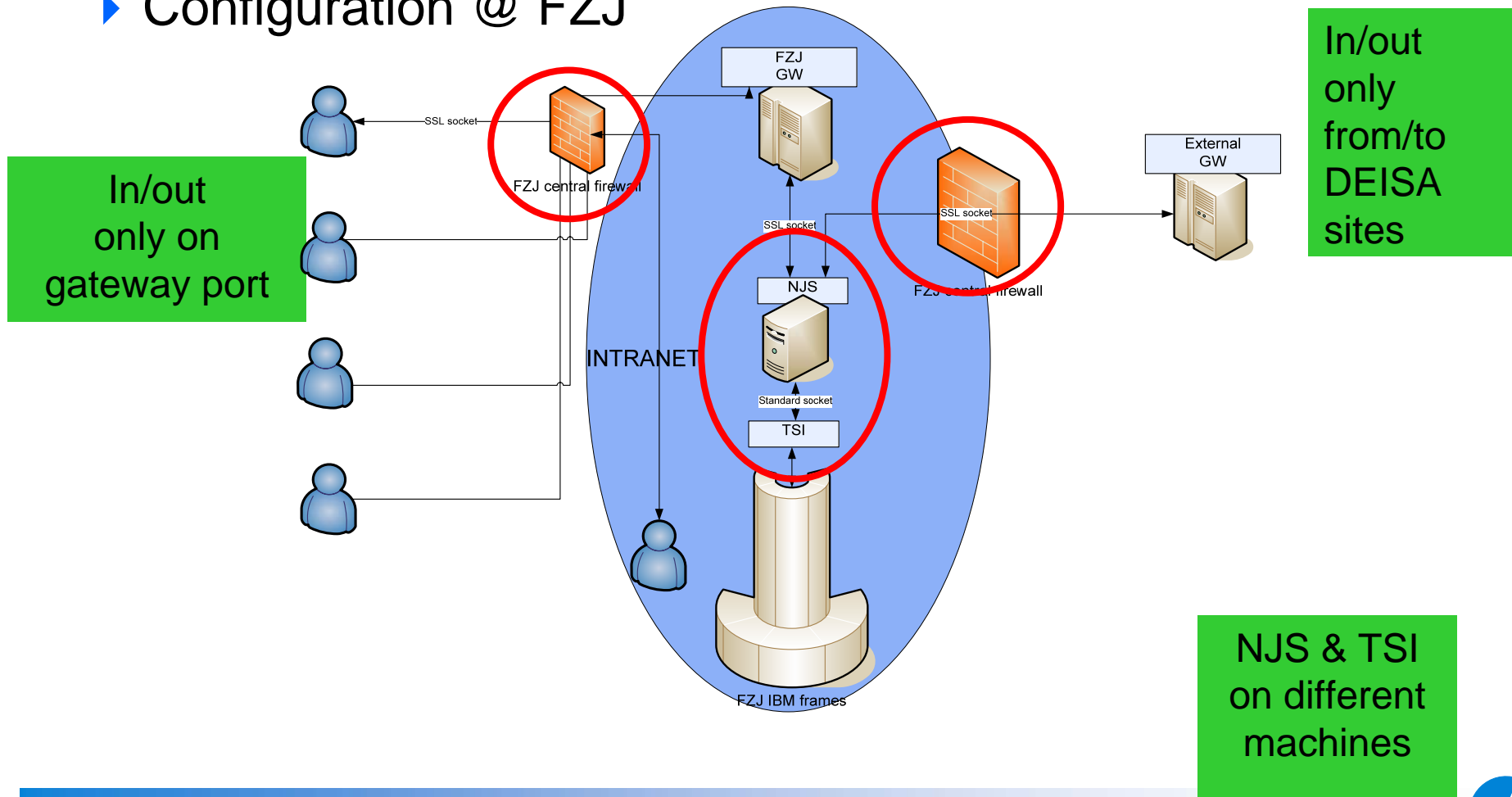




► Configuration @ RZG, IDRIS



► Configuration @ FZJ



UNICORE Security

- ▶ Security model based on X509 public key infrastructure
- ▶ Credential consists of a public and a private key
- ▶ No userid and password authentication
- ▶ Password protected keystore
- ▶ Single sign on
- ▶ UNICORE accepts following private key formats:
 - ▶ RSA (pkcs12)
 - ▶ E.g. Openssl 0.9.7x
 - ▶ Java keystore (jks)
 - ▶ SUN Java
- ▶ Certificates provided e.g. by DFN CA
- ▶ Two server site security entities:
 - ▶ Gateway – Authentication
 - ▶ NJS – Authorisation

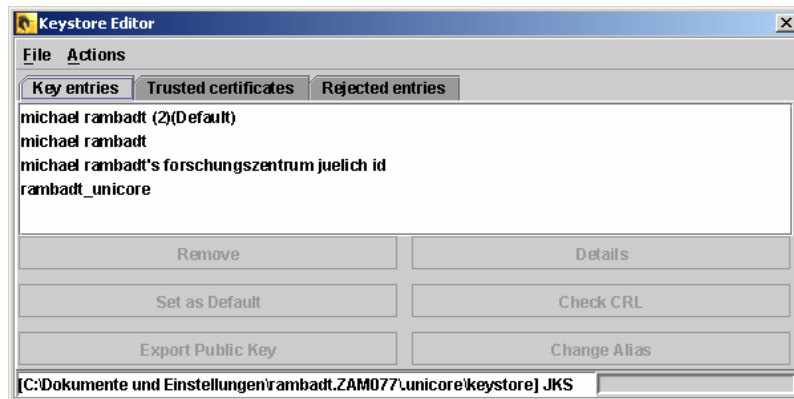


UNICORE Security - Client

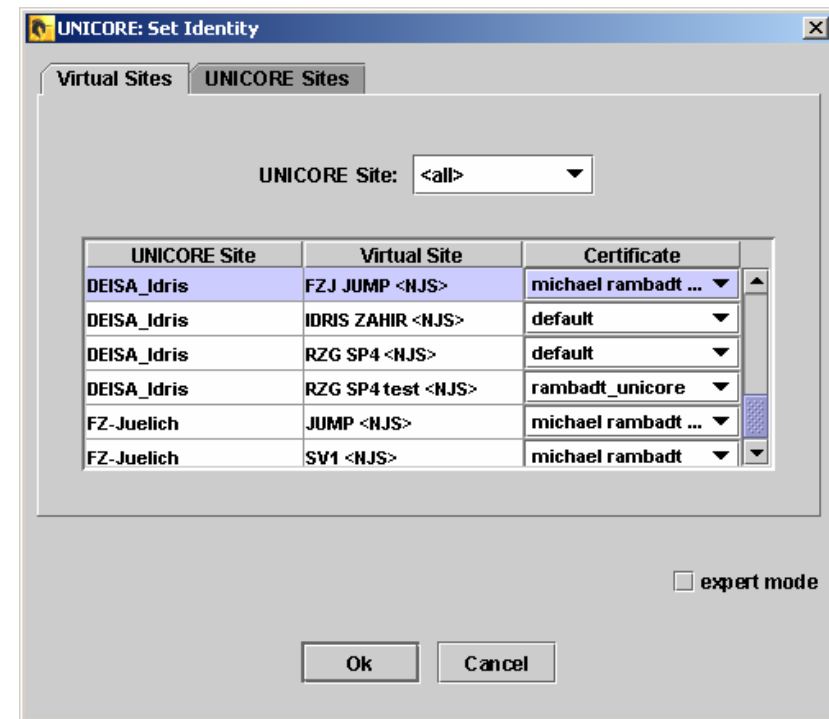
- ▶ Access to password protected keystore
- ▶ Encrypted Keystore contains all imported certificate(s) and the user's private key(s)
- ▶ UNICORE Keystore editor allows to
 - ▶ Generate a X509 certificate request
 - ▶ Import/export .p12 or .jks keystores
 - ▶ Import public keys
- ▶ The User has to import (at least) three certificates into the Client
 - ▶ Pluginsigner's certificate (public key)
 - ▶ Gateway signer's certificate (public key)
 - ▶ User's signed public key



Using Different Identities



Key entries: Who am I?



Using different identities



UNICORE Security: Gateway

- ▶ Gateway authenticates the user
- ▶ Following checks are performed on certificates presented by a client
 - ▶ Certificate is issued by one of the trusted CA (e.g. DFN-CA)
 - ▶ Certificate is within its validity period
 - ▶ Certificate has not been revoked (if check for Certification Revocation Lists (CRL) is activated)
- ▶ Gateway accepts only SSL connections from Clients and other NJSs
 - ▶ SSL-Handshake
- ▶ Optional SSL connection between Gateway and NJS



Behind the scenes: Authentication



UNICORE Security: CRL

- ▶ All revoked certificates are stored in a Certification Revocation List (CRL)
- ▶ Gateway has access to the CRL
 - ▶ gateway.properties
 - ▶ gw.check_crls=true
- ▶ CRL URL has to be inside the certificate or in the gateway configuration file
- ▶ UNICORE client also has access to the CRL

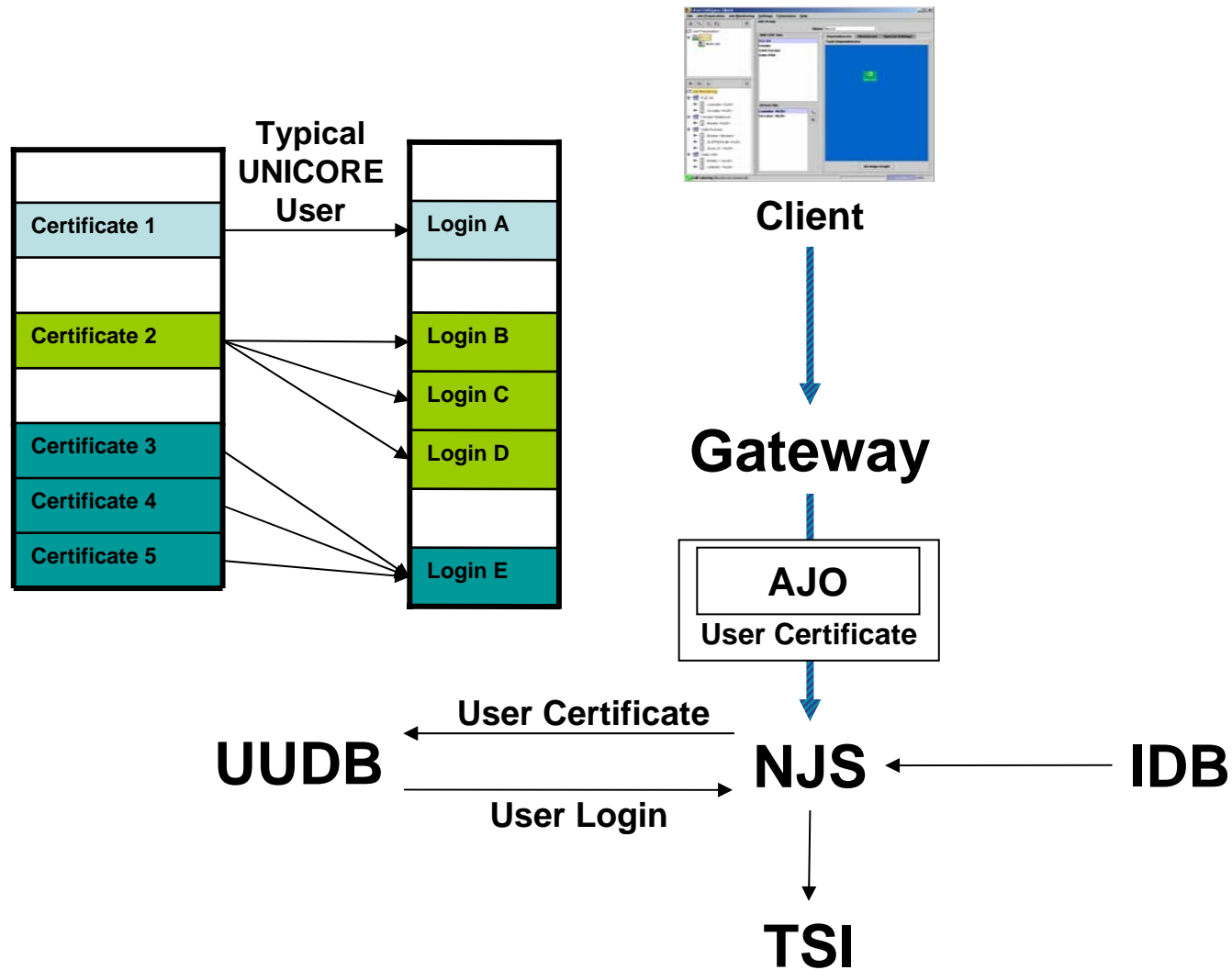


UNICORE Security: NJS

- ▶ NJS authorizes the user
- ▶ Access the UNICORE user Database (UUDB)
 - ▶ Maps the user's certificate to his xlogin on the target system
- ▶ Only users presenting certificates stored in the UUDB can connect to the target system
- ▶ NJS authorises other NJSs
 - ▶ Explicit UUDB entry



Behind the Scenes: Authorisation





- ▶ Open Source under BSD license
- ▶ Supported by FZJ
 - ▶ Integration of own results and from other projects
 - ▶ Release Management
 - ▶ Problem tracking
 - ▶ CVS, Mailing Lists
 - ▶ Documentation
 - ▶ Assistance
- ▶ Viable basis for many projects
 - ▶ DEISA, UniGrids, NaReGI, ...
- ▶ <http://unicore.sourceforge.net>



▼ UNICORE at SourceForge

- Project page
 - Download page
 - CORE
 - Client-side
 - Client
 - Server-side
 - Gateway
 - NJS
 - UUDB
 - TSI
 - Job Modeling
 - AJO
 - OPTIONAL
 - Client-side
 - Client library
 - Client plugins
 - Interactive Access
 - IADemo
 - List All Jobs (LAJ)
 - Plugin Loader
 - Broker
 - Unicore Broker
 - EXPERIMENTAL
 - Tracker page
 - Mailing list page
 - CVS page
 - Project Statistics
- ▷ Installation
- ▷ Documentation
- ▷ Links

UNICORE at SourceForge

The UNICORE Project page offers you the entry point to all features SourceForge provides for hosted projects. Selected pages which we think are most important in daily work are accessible via the menu to the left and briefly described below.

Selected pages

- Project page** The entry point to all SourceForge features available for the UNICORE project.
- Download page** The root download page. The quick links to single packages are described below.
- Tracker page** Trackers are used to submit and discuss bugs, support requests, patches and feature requests related to the UNICORE project. A separate page for each tracker category is accessible via this link. **We encourage you to use trackers for comments, requests, etc. concerning this web site, too.**
- Mailing list page** All mailing lists linked to this project including archives can be found here.
- CVS page** You want to get the latest development version of the source code? Then check the CVS page out.

Quick links to software packages

Every single component which is downloadable via a quick link to the left is briefly described and, if existent, a link points to an in-depth description of the respective component.

Client	UNICORE's client-side entry point providing a graphical interface to a UNICORE Grid (see detailed description).
Gateway	The Gateway is the single entry point for all UNICORE connections into the USite.
NJS	The Network Job Supervisor manages all jobs submitted to a UNICORE Vsite. The NJS package contains UNICORE's information service, the Incarnation Database (IDB).
UUDB	User authorization is the job of the UNICORE User Database.
TSI	The Target System Interface accepts incarnated job components from the NJS and passes them to the local resource management system for execution.
AJO	The Abstract Job Object class library provides the foundation for job and workflow modeling and for the protocol between UNICORE clients and servers.
Client library	The Arcon Java client library provides the means to integrate UNICORE client services in portals, applications, etc.
Client plugins	The Client's plugin concept provides the means to integrate applications into a UNICORE Grid without source code modifications to the application. A large variety of plugins is already available.
Unicore Broker	Maintained as a separate project, please visit http://uombroker.sourceforge.net/



Future of UNICORE (GRID) Security?

- ▶ Explicit trusted delegation (developed for the Naregi Project)
- ▶ Many grid application require dynamically opened ports in a firewall
 - ▶ =>Dynamic Grid Firewalls?



Conclusion

- ▶ Questions
- ▶ Comments
- ▶ Discussion

Thank You!





October 11–12, 2005
ETSI Headquarters, Sophia Antipolis, France
<http://summit.unicore.org/2005>

In conjunction with
Grids@work: Middleware, Components, Users, Contest and Plugtests
<http://www.etsi.org/plugtests/GRID.htm>

Supported by

UNICORE
F O R U M