www.prace-ri.eu

The PRACE Security model and eduGAIN interoperability

Walter de Jong (SURFsara)
Vincent Ribaillier (CNRS/IDRIS)
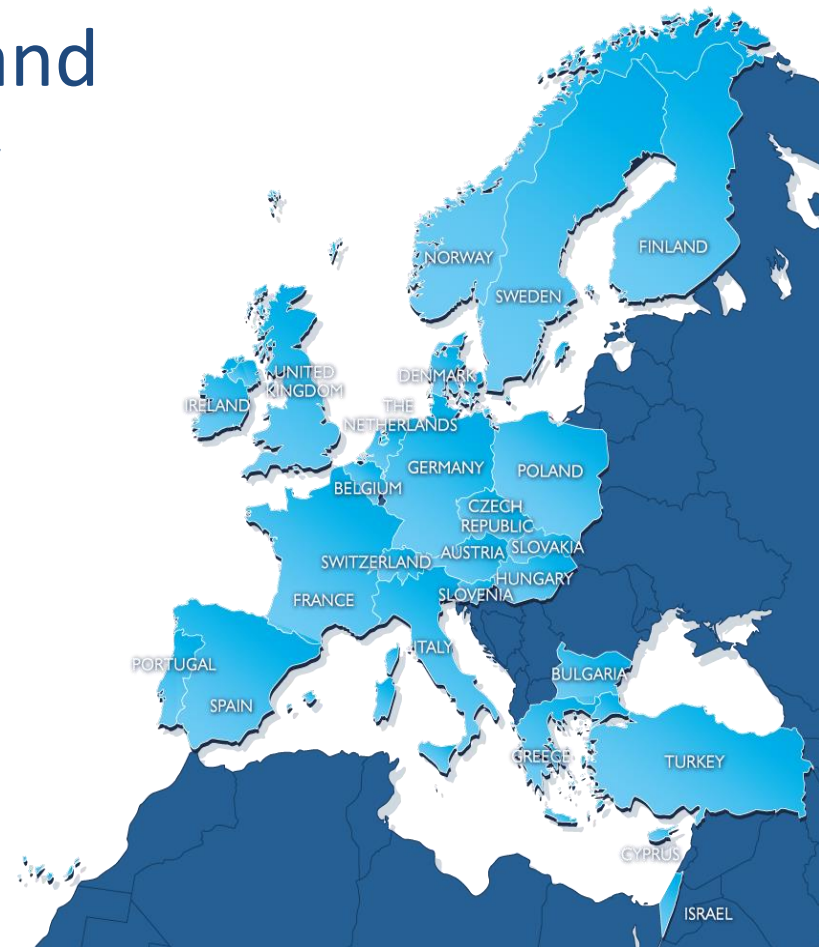
39th EUGridPMA meeting, January 30, 2017, Florence

Partnership for Advanced Computing in Europe

PRACE is an international not-for-profit association under Belgian law, with its seat in Brussels.

PRACE counts 25 members and 2 observers.

The **PRACE** Hosting Members are France, Germany, Italy, Spain, and Switzerland.

PRACE is governed by the **PRACE** Council in which each member has a seat. The daily management of the association is delegated to the Board of Directors.

PRACE is funded by its members as well as through a series of implementation projects supported by the European Commission.

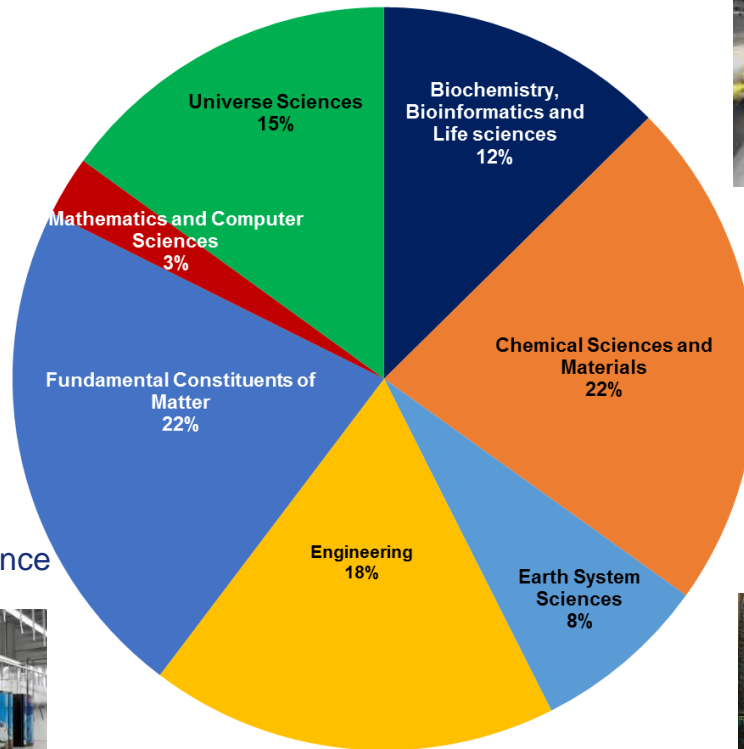# **5** Hosting Members offering core hours on **7** world-class machines

MareNostrum: IBM
BSC, Barcelona, Spain

CURIE: Bull Bullx
GENCI/CEA,
Bruyères-le-Châtel, France

Piz Daint: Cray XC30 system,
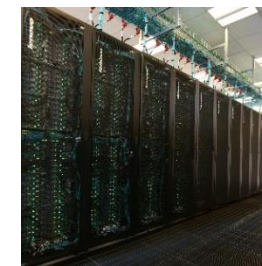CSCS, Lugano, Switzerland

JUQUEEN: IBM
BlueGene/Q,GAUSS/
FZJ, Jülich, Germany

SuperMUC: IBM
GAUSS/LRZ
Garching, Germany

Hazel Hen: Cray
GAUSS/HLRS,
Stuttgart, Germany

MARCONI: Lenovo
CINECA, Bologna, Italy

Universe Sciences
15%

Biochemistry,
Bioinformatics and
Life sciences
12%

Mathematics and Computer
Sciences
3%

Chemical Sciences and
Materials
22%

Fundamental Constituents of
Matter
22%

Engineering
18%

Earth System
Sciences
8%

Research Domain Pie Chart up to and including Call 13

465 scientific projects **enabled**

12.2 thousand million core hours awarded since 2010 with peer review, main criterion is **scientific excellence**. **Open R&D** access for **industrial users** with **>50 companies** supported

>7 350 people trained by **6 PRACE Advanced Training Centers** and others events

40 Petaflops of peak performance on **7 world-class systems**

530 M€ of funding for **2010-2015**, access **free at the point of usage**

25 members, including **5 Hosting Members** (France, Germany, Italy, Spain and Switzerland)

Criterion: Scientific Excellence

Access through PRACE Peer Review

Free-of-charge required to publish results at the end of the award period
Open to **international** projects

Project Access (*every 6 months*) **award period 1 to 3 years**
Individual researchers and groups
No restriction on nationality for both researcher and centre
Required to demonstrate technical feasibility of project

Preparatory Access (*cut-off date every 3 months*)
Optional support from PRACE experts
Prepare proposals for Project Access

Project Access

Open Call for Proposals	Technical Review	Scientific Peer Review	Right to reply	Priorisation + Resource Allocation	Project + Final Report

~ 2 Months   ~ 3 Months   Up to 3 years

Technical experts in PRACE systems and software

Researchers with expertise in scientific field of proposal

Access Committee

Researcher

www.prace-ri.eu/call-announcements/

PARTNERSHIP FOR ADVANCED COMPUTING IN EUROPE
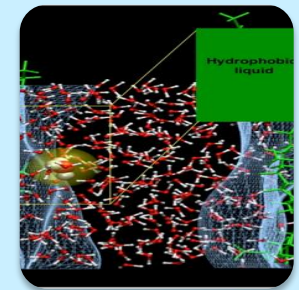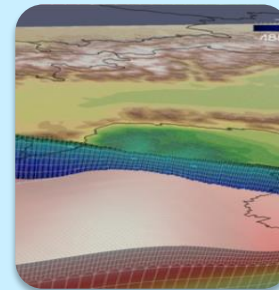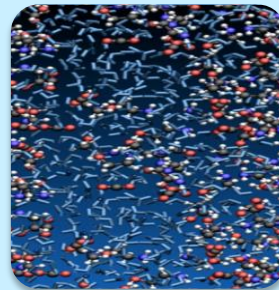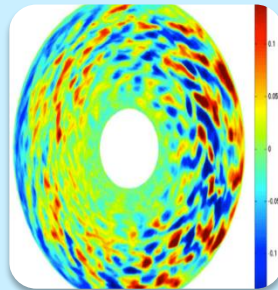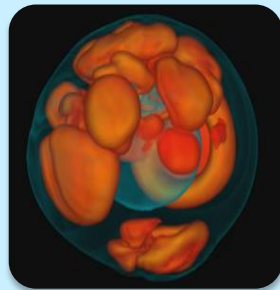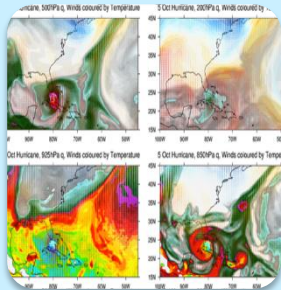
Climate
144 million core hrs on Hermit (DE) **for UK - UB**

PRACE will give to UK Met a 3 years advance in the development of their models (high resolution global weather & climate models).

Astrophysics
million core hrs: 98 on CURIE (FR) + 49 on SuperMUC (DE) **for Germany**

This PRACE grant is one of the biggest worldwide allocation in this domain. Without this huge computational resources this project would not have been carried out in a decent time.

Energy
30 million core hrs on SuperMUC (DE) **for Finland**

PRACE resources enable the first European direct comparison of first-principles simulations to multi-scale experimental data for fusion energy (Link ITER).

Chemistry
59,8 million core hrs on JUQUEEN (DE) **for Switzerland**

Simplified models would not give reliable or meaningful results: Only PRACE systems are large enough to allow these computational models to be calculated.

Seismology
53.4 million core hrs on SuperMUC (DE) **for Italy**

The massive allocation of computing resources awarded via PRACE can be used to explore the non-linearity involved in the dependence of local ground shaking on geological structure.

Life Science
40 million core hrs on JUQUEEN (DE) **for Germany**

A single standard PC would need 5.000 years to do what JUGENE did in 100 days (40 million core hours) Only a PRACE system can offer enough resources to accomplish such a computationally intensive project.

The PRACE Security Model

39th EUGridPMA meeting, January 30, 2017, Florence

WISE (i.e. SCI) activity
WISE (i.e. SCI) activity
WISE (i.e. SCI) activity
WISE (i.e. SCI) activity

PARTNERSHIP FOR
ADVANCED COMPUTING IN EUROPE

General Principles

- Each PRACE site committing resources is responsible for the management of its users.

- User registration and authentication methods may differ (slightly) from one site to another.

- The PRACE Acceptable Use Policy applies to all Users of the PRACE infrastructure. Some sites have also specific regulations related to security (cf. WISE SCIV2-WG).

Authentication

- X.509 is the preferred authentication method (EUGridPMA, IGTF).
- SSO is implemented via two MyProxy servers.
- Examples of services using X.509 authentication :
  - GSI SSH, UNICORE, GridFTP, Web services

Authorization

- Each site generates authorizations for its users.
- Authorizations are based on attributes published in a distributed LDAP directory.
- LDAP allows a fine grain management of attributes :
  - Attributes associated to projects
  - Attributes associated to accounts
  - Examples of attributes stored in LDAP:
    - Home site, logins, group membership, roles, budgets
- LDAP has been chosen for:
  - its distributed design (each site administers its own branch),
  - its security (fine grained ACL, X.509 authentication, TLS).

Accounting

- Accounting is published in a distributed database (DART).
- Accounting records are compliant to the OGF usage record format.
- The accounting database can be queried by sites and users (X.509 authentication).

Use cases related to Identity Federations

Main objectives

- The PRACE security model has been in production for now more than 10 years and has proven to fully fulfill the security objectives related to the PRACE core services.

- PRACE is following closely the identity federation initiatives.

- **Interoperability** is the main goal :
  - Interoperability with other European and international projects
    - PRACE has a long history of collaboration with other projects : EGI, EUGridPMA, EUDAT…
  - Interoperability with scientific communities
  - Interoperability with industrial partners

So, what could be the use cases ?

Use cases

- Use case 1 : PRACE as an Identity Federation consumer

- Use case 2 : PRACE as an Identity Provider

PRACE as an Identity Federation consumer (1)

- In this scenario, PRACE would rely on an Identity Federation to allow its users to access its resources.

- The main problem with this approach is that each PRACE site would have to accept to delegate the authentication process to the organizations members of the identity federation :

  - **All sites participating to the federation need to be trusted.**

  - What **Levels of Assurance** can be provided by the Identity Federation ?

    - How can a PRACE site be sure that the authentication method is based on X.509 certificates and not based on a simple login/password method ?

    - How can a PRACE site be sure that the best practices are respected by each member of the Identity Federation ?

PRACE as an Identity Federation consumer (2)

- Is it technically possible to :
    - mention the details of the authentication method in the SAML assertions delivered by the Identity Federation ?
    - make sure that SAML assertions are compliant to the PRACE policy ?
    - produce SAML assertions "certified" by EUGridPMA (Such assertions would be assertions delivered after a successful X.509 authentication based on a X.509 certificate delivered by a CA accredited by EUGridPMA) ?

PRACE as an Identity provider (1)

- In this scenario, PRACE would maintain its own Identity Provider(s).
- Attribute enrichment could be performed based on LDAP information.
  - LDAP schema modification may be required.
- A Token Translation Service could be also deployed.
- A SPIdP proxy could also be deployed to aggregate attributes.
  - E.g : persistent unique Identifier (cf. eduPersonUniqueId attribute defined in the eduPerson schema)

PRACE as an Identity provider (2)

- Added value for the PRACE users :
  - Once authenticated, interoperability becomes possible :
    - The assertions delivered by the authentication process could be used to access resources managed by other partners or projects (large data set, web services, …).

PRACE as an Identity provider (3)

- Middleware used in this scenario must support the SAML assertions delivered by the Identity Provider(s).

- Currently, SAML seems to be adapted mainly to Web SSO (cf. SAML2int), which is not necessarily the preferred access method of PRACE users.

39th EUGridPMA meeting, January 30, 2017, Florence

Conclusion

- X.509 certificate model is currently acceptable for PRACE.

- It is part of PRACE technology evaluation program to follow what is going on in the identity federation field.

- Interoperability is the key word.

- PRACE is interested in open standards for the exchange of authentication and authorization information (SAML).

- But interoperability is not always easy to achieve :

  - Use cases must be defined.

  - Middleware used in PRACE must support these standards.