JÜLICH
FORSCHUNGSZENTRUM

Security in PRACE & HBP

Ralph Niederberger
Jülich Supercomputing Center (FZJ)
r.niederberger@fz-juelich.de

Wise Workshop, Krakow, Poland
Sep. 27th 2016

Overview

- The PRACE Project
  - Security issues in PRACE
- The Human Brain Project
  - HBP security issues

The PRACE Project

Co-funded by the European Union

„This work was financially supported by the PRACE project funded in part by the EU's Horizon 2020 research and innovation programme (2014-2020) under grant agreement 653838."

PRACE → *the* European HPC Research Infrastructure

Enabling **world-class science** through large scale simulations

Providing **HPC services** on **leading edge capability** systems

Operating as a **single entity** to give access to **world-class supercomputers**

Attract, **train** and **retain** competences

Lead the **integration** of a highly effective **HPC ecosystem**

Offering its resources through a **single** and **fair** pan-European **peer review process to academia and** industry

PRACE

ESFRI

PRACE in numbers

25 members

€ 400 M total funding by hosting members for PRACE systems and operations

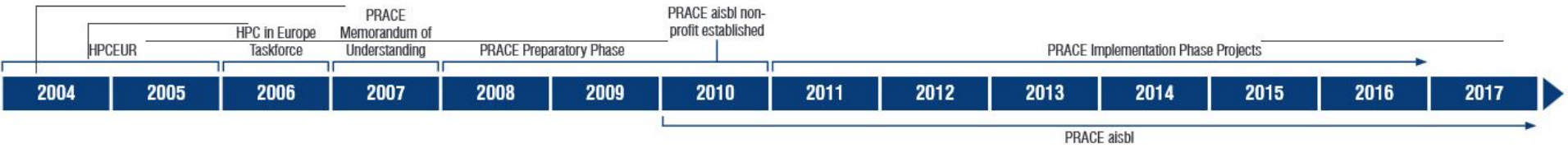
10.2 billion core hours awarded (Feb.2015) to 394 projects from 38 countries

25 prototypes of new architectures & technologies evaluated

100s of scientific applications enabled to exploit leading-edge HPC

50 companies have been supported since the inception of the Open R&D programme in 2012

16 Best Practice Guides and **200+** White Papers published



PRACE Security – Where is it handled?

PRACE is structured into several tasks

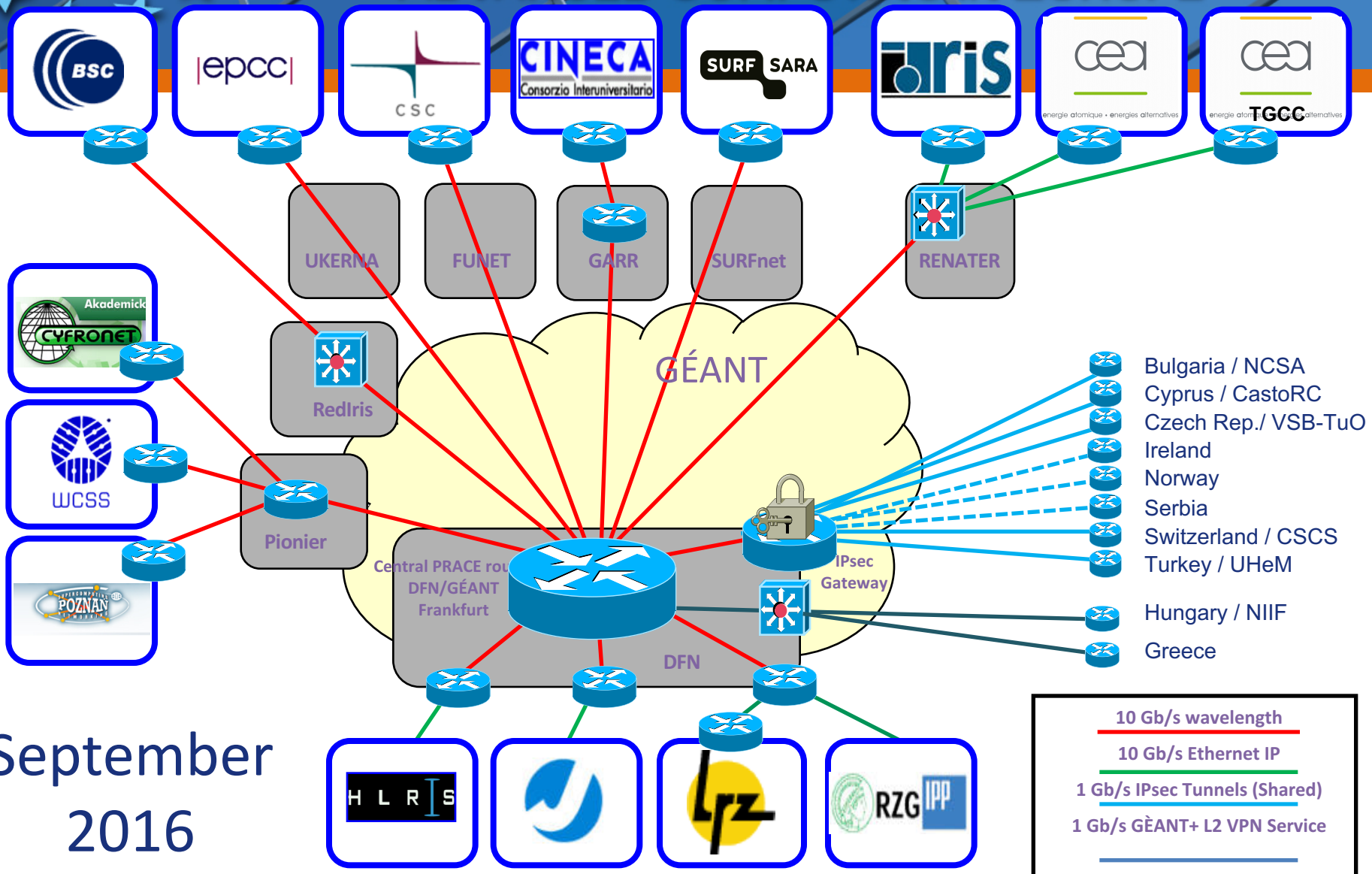
→ WP6 Operational services for the HPC Eco-system includes

- Operation and coordination of the comprehensive common PRACE operational services including PRACE **networking and security**
- Link with other e-infrastructures and CoEs
  - HBP and EUDAT, SCI → WISE and AARC

The PRACE dedicated network

The infrastructure consists of

- a central L2/L3 switch in Frankfurt connecting T0 & T1 systems of
- 15 partners via 10 Gb/s wavelength
- an IPSEC/GRE gateway in Frankfurt connecting
- 5 additional partners with 1 Gb/s IPSEC/GRE tunnels and
- two partners via 1 Gb/s GÉANT-L2VPN connections



September 2016

Why are network & security correlated

- A dedicated network allows to define different security policies to be used than public networks would allow
- No interfering traffic, no spying, no *hackers??*
- Requirement: "**Net of trust**"
- Here comes in: WISE Community work

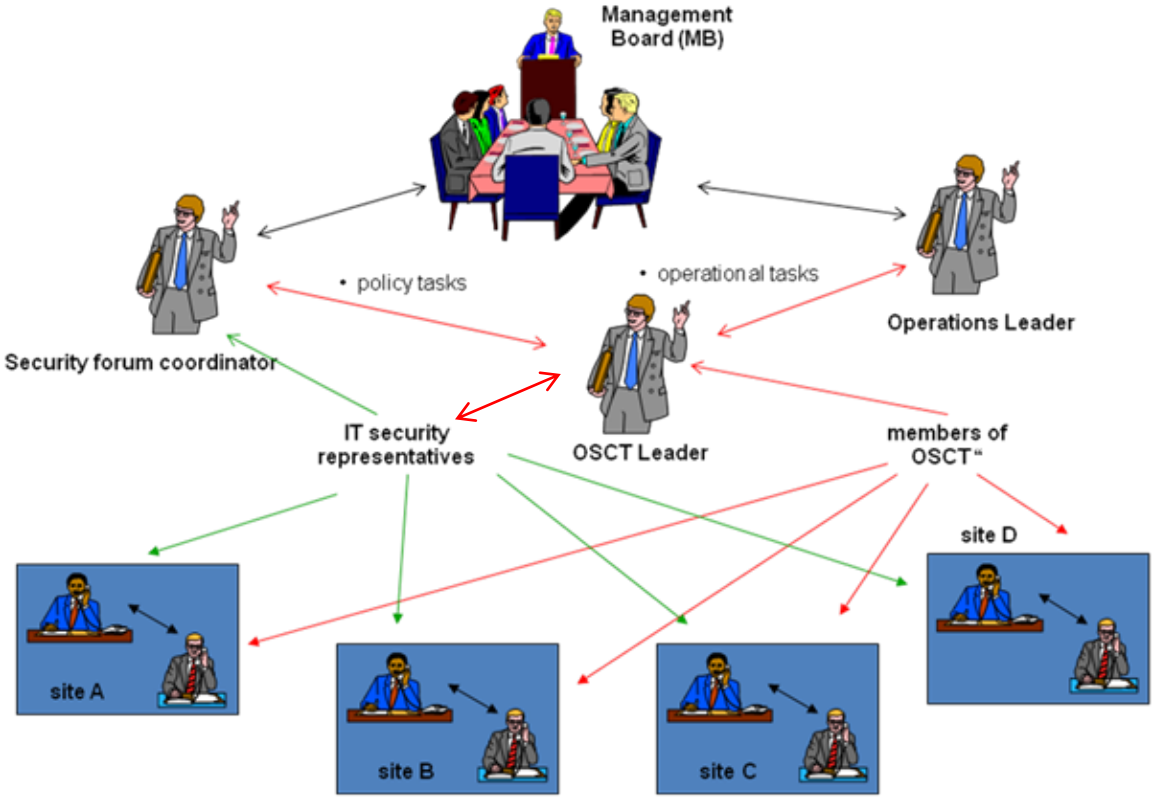
PRACE Security Forum

Tasks:

- Defining security related Policy and Procedures - to build “A trust model that allows interoperation of the distributed PRACE services”;
- The Risk Review of new services or service upgrades - to define and maintain “An agreed list of software and protocols that are considered robust and secure enough to fulfil the minimal security requirements”;
- The management of operational security – to coordinate “incident handling” (CSIRT team)

PRACE organisational chart (extract)

Networking of PRACE Security Forum



Security Policies and Procedures

Define:

- minimal security requirements, that all PRACE sites are expected to abide to;
- agreed list of software and protocols that are considered robust and secure enough to implement these requirements;
- trust model that allows smooth interop of the distributed PRACE services.
- The policies and procedures address:
    - The risk review of changes in the infrastructure
    - The handling of security incidents
    - The auditing of the security set-up
    - The roles and responsibilities of persons and teams

Risk reviews

- The Security Forum performs a risk assessment of new services or updates on existing services if changes in the security set-up come up.
- Rerequisites:
  - Provision of security policy documents by every site (Net of Trust model)
  - Possible self-assessment using a document published by SCI group

Operational security & Incident response

- All partners provide members to the PRACE CSIRT team
- Site incidents must be reported in case of possible impacts on sites
- Vulnerability reports have to be provided
  - No formal documents. Any available sources for information can be used (stored in PRACE Wiki)
- Sharing of emergency phone numbers and security mailing lists for all sites
- Although every partner is expected to have already information about vulnerabilities in general, it is helpful if specific information is also provided through internal channels.

Collaboration with other projects & activities

Collaboration with EGI, HBP and EUDAT CSIRTs on sharing of information on incidents and vulnerabilities

- enables exchange of information about incidents if there may be cross domain impacts and also exchange of vulnerability information
- Several PRACE colleagues are on the EGI, EUDAT and HBP security alert list and vice versa

Accreditation of PRACE CSIRT team

- Trusted Introducer service from GEANT
  https://www.trusted-introducer.org/processes/registration.html
- Teams may be
  - *listed*, which provides basic information about the team itself as well as shows endorsement of the team by the TI community;
  - ***accredited***, which ensures a defined level of best practices and acceptance of the established TI policies for such teams;
  - *certified*, if they have been accredited before and prove a confirmed level of maturity as defined by the TI SIM framework.

EUGridPMA

- PRACE trusts the CAs accredited by EUGridPMA or the other two PMAs federated in the IGTF (Interoperable Global Trust Federation)
- PRACE is Relying Party of EUGridPMA
- Three times a year F2F meetings, attended regularly by PRACE representatives

AARC

- AARC = Authentication and Authorisation for Research and Collaboration

  https://aarc-project.eu
- Two year H2020 project
- Followup project in the pipeline
- Jülich and SURFsara are partners

WISE Community

WISE Information Security for Collaborating E-Infrastructures (https://wise-community.org/)

A trusted global framework where security experts can share information on different topics like risk management, experiences about certification process and threat intelligence

Joint effort of GEANT SIG-ISM (Special Interest Group on Information Security Management) and SCI (Security for Collaboration among Infrastructures) (EGI, EUDAT, HBP, PRACE, WLCG, XSEDE)

The Human Brain Project

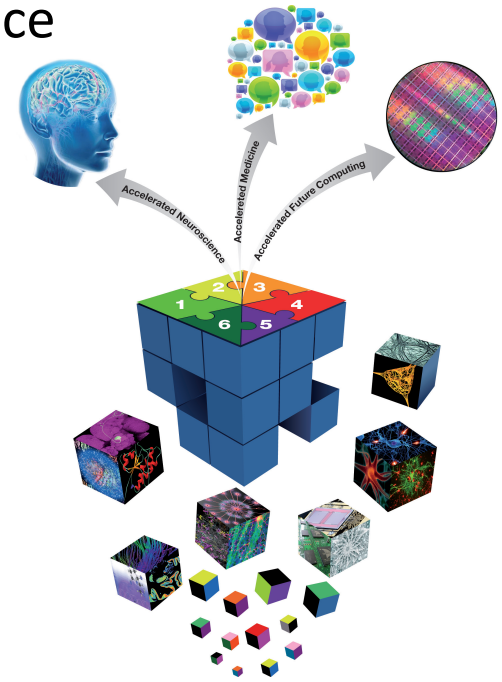
HBP

Co-funded by the European Union

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 720270 (HBP SGA1)".

The Human Brain Project (HBP)

Is a European Commission Future and Emerging Technologies Flagship.
It aims to put in place a cutting-edge, ICT-based scientific research infrastructure for brain research, cognitive neuroscience and brain-inspired computing.
The Project promotes collaboration across the globe.
It is organized in thirteen subprojects, spanning strategic neuroscience data, cognitive architectures, theory, ethics and society, management and the development of six new informatics-based Platforms.
The platforms will be accessible through the HBP Collaboratory – an Internet portal to HBP



HBP Partners, countries and more

- **More than 100 partners in 24 countries in Europe and around the world**

  Austria, Belgium, Canada, China, Cyprus, Denmark, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States of America

  For details see:

  https://www.humanbrainproject.eu/

HBP subprojects

SP1 **Strategic Mouse Brain Data**

SP2 **Strategic Human Brain Data**

SP3 **Cognitive Architectures**

SP4 **Theoretical Neuroscience**

SP5 **Neuroinformatics**

SP6 **Brain Simulation**

SP7 **High Performance Computing**

The High Performance Computing platform will provide the supercomputing, data and visualization hard and software capabilities required for multi-scale brain modelling, simulation and data analyses accessible via the HBP Collaboratory

SP8 **Medical Informatics**

SP9 **Neuromorphic Computing**

SP10 **Neurorobotics**

SP11 **Applications**

SP12 **Ethics and Society**

SP13 **Management**

Subproject 7
15 partners from 7 countries

SP 7 – Overview

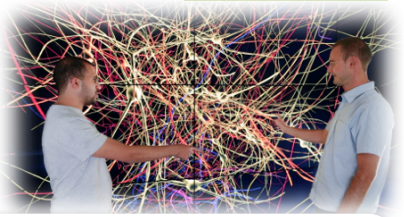
Pre Commercial Procurement (PCP): Future HBP Supercomputer

WP 7.1

Mathematical methods & Programming models

WP 7.2

WP 7.3



Interactive analysis & visualization

SP 6

Simulation of Brain models

Management of huge datasets

WP 7.4

WP 7.5

Integration & Operation

WP 7.6

User support & Community building

WP 7.7

Management & Coordination

High Performance Computing Platform

Technology evaluation for HBP HPC systems

- Requirements analysis for pre-commercial procurement
- Evaluation of designs & technologies for HBP Supercomputer

Numerical methods, programming models and tools

- Software specific for brain research but based on and aligned with European and international strategies and roadmaps

Interactive visualization, analysis and control

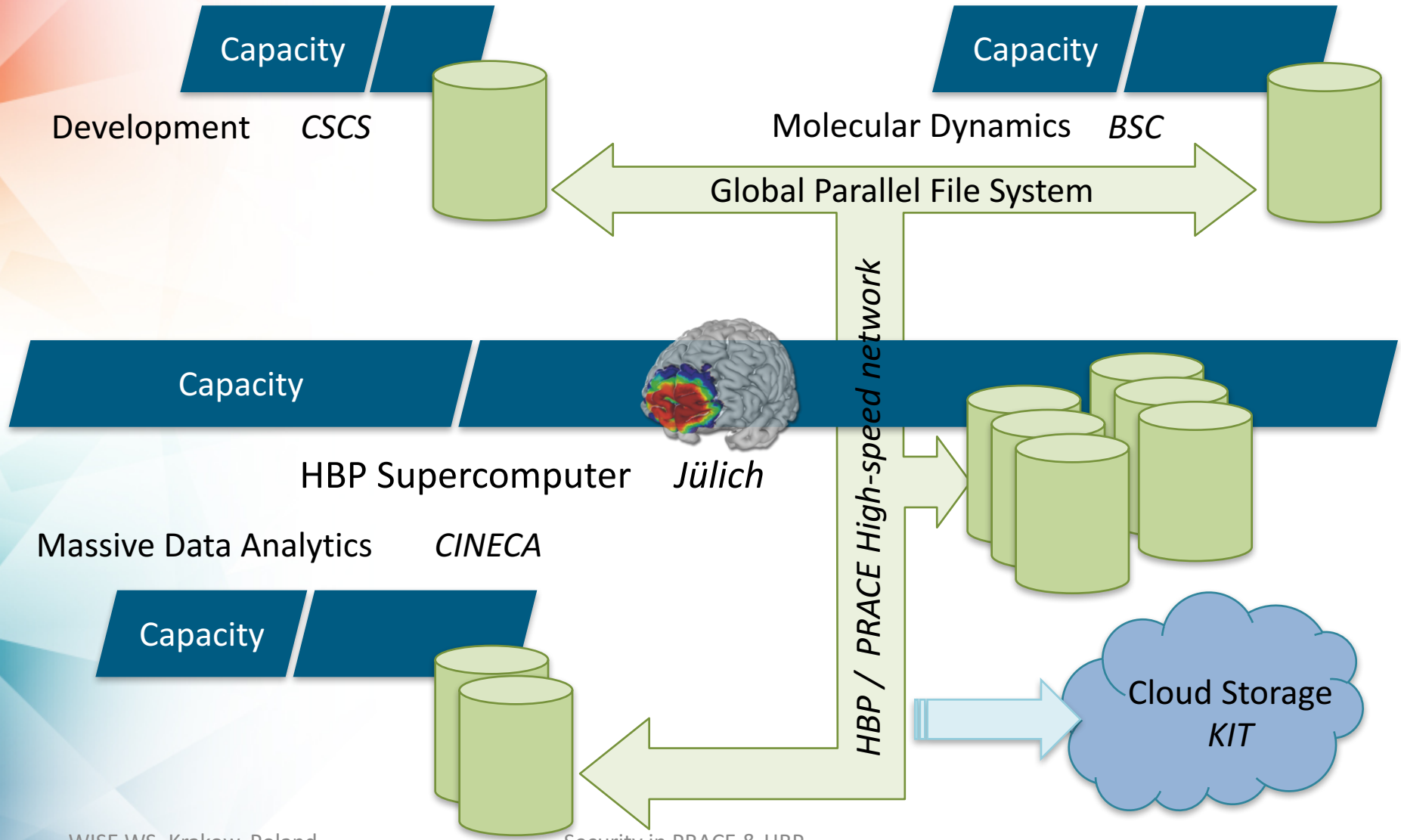
- In situ visualization and interactive steering of simulations

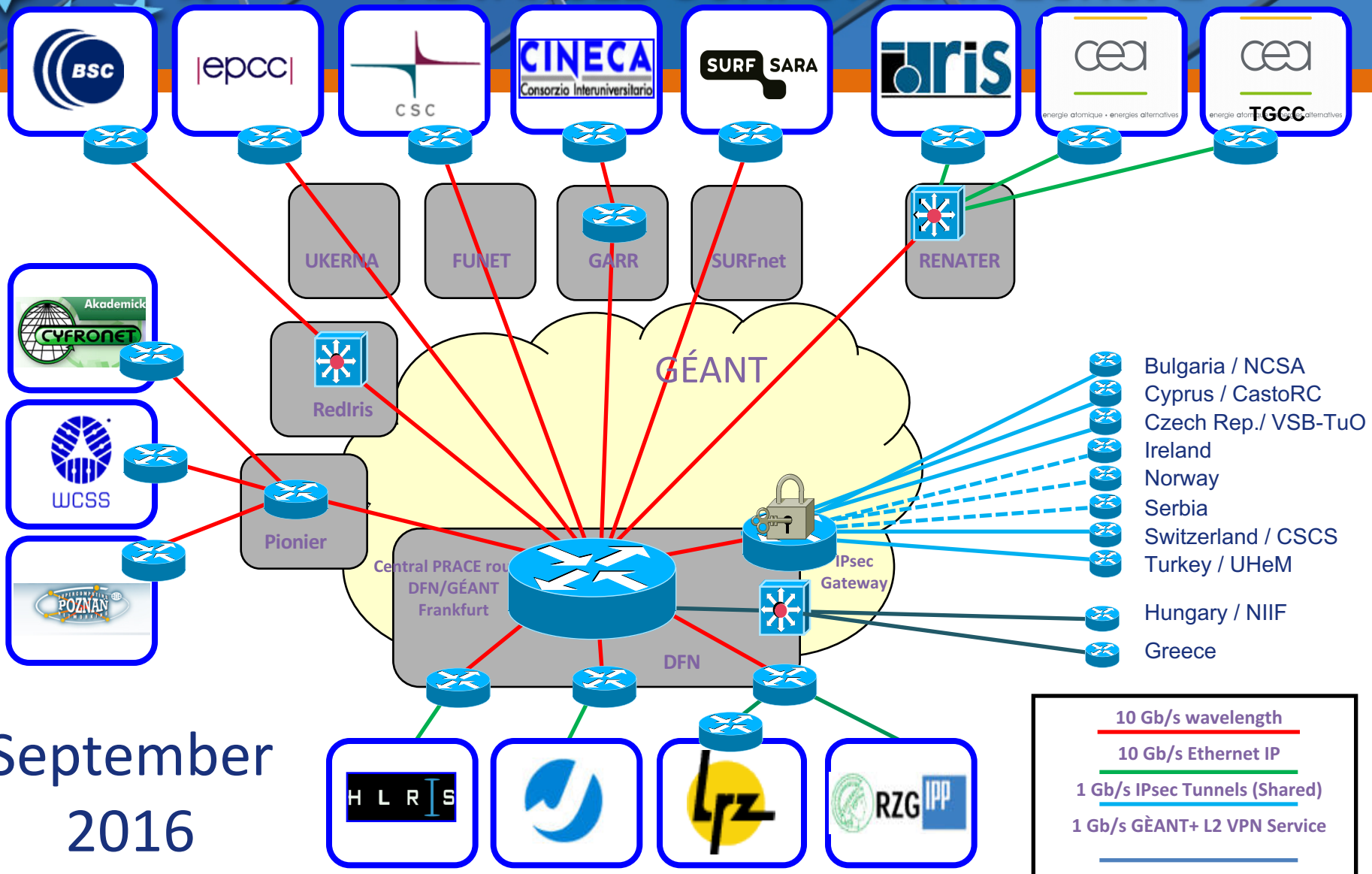
Exascale data management

- Big Data for brain research

High Performance Computing Platform

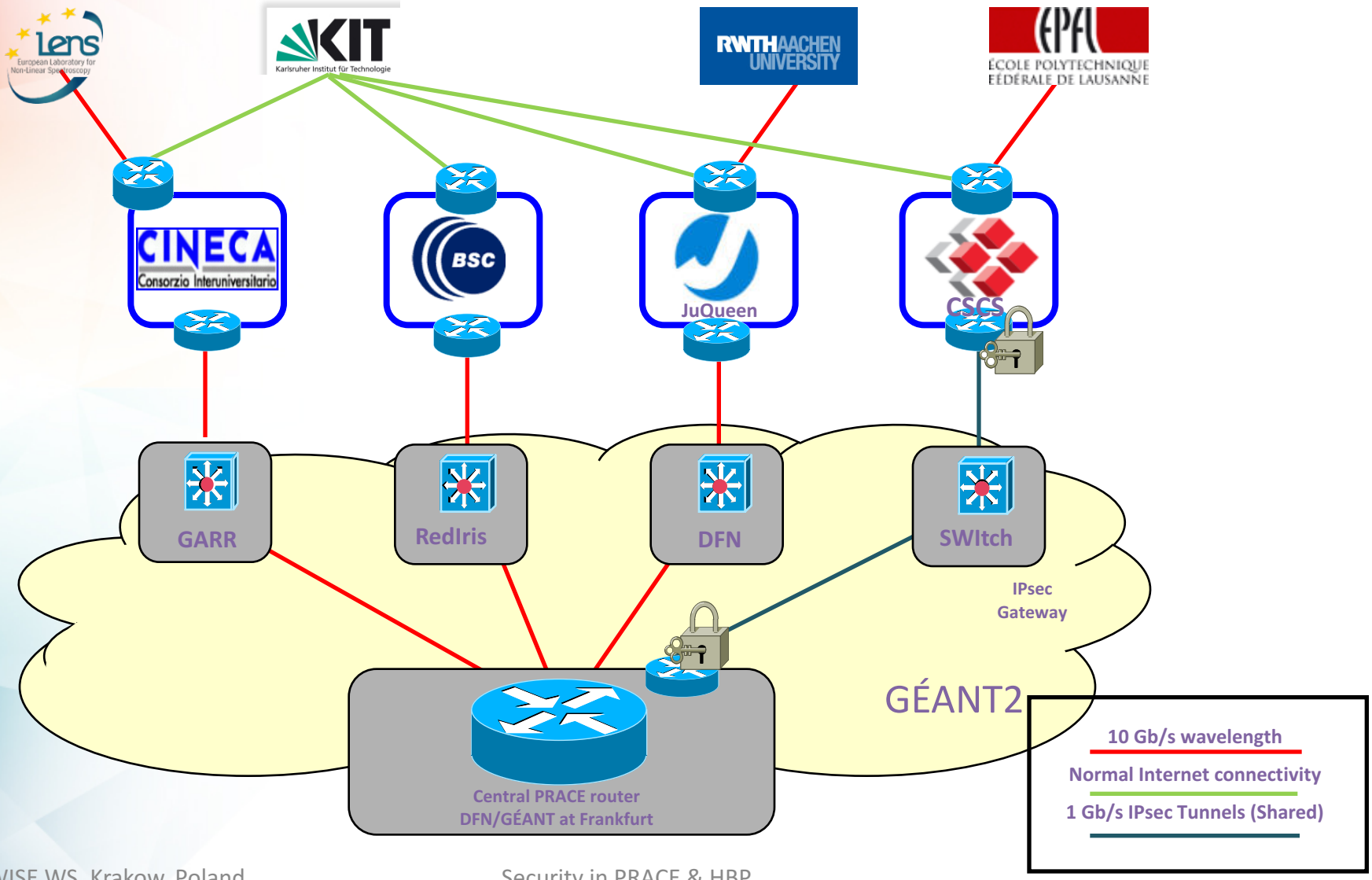
The HBP HPC infrastructure





September 2016

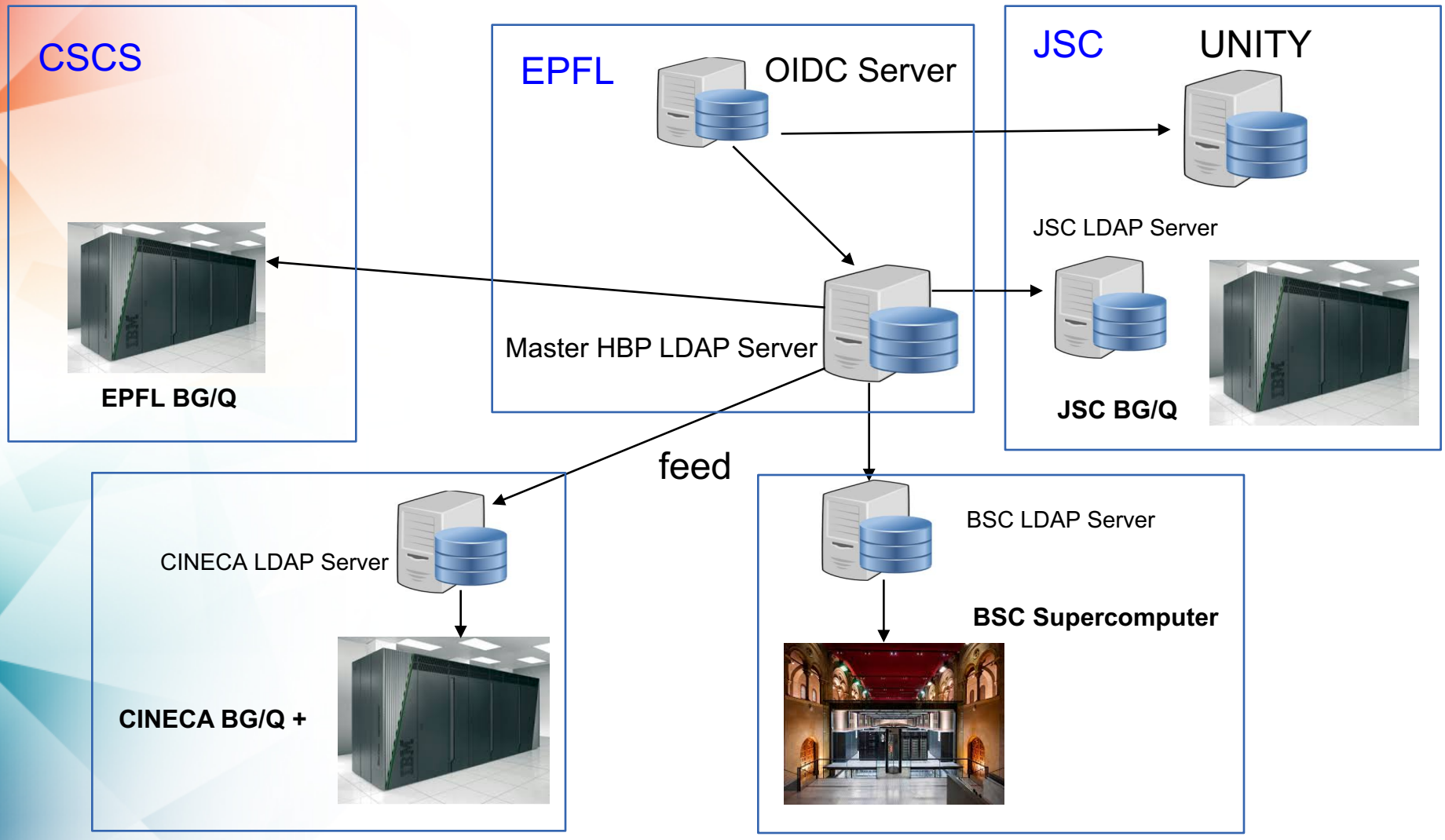
The HBP HPC infrastructure



Overall HBP HPC security setup

- Nearly identical to PRACE security
- Speciality can be found in different access strategies
- PRACE -> direct access to computing resources
- HBP -> access mostly via a specialiced HBP portal and predefind applications, but also direct access possible

Centralized LDAP infrastructure



User Access to the HBP Portal

User

1. Login with {username, password} to get OIDC token

EPFL

OIDC Server

JSC

UNITY

2. use OIDC token to access UNICORE services

4. validate OIDC tokens

3. pass OIDC token, gets user DN

UNICORE

5. user DN

user uid, gids

UNICORE XUUDB

Master HBP LDAP Server

6. access HPC resources with correct user uid, gids

(periodically) update user info: {DN, uid, gids}

Local LDAP

(periodically) sync user records {DN, uid, gids}

(periodically) manage users' uids & gids

HPC site (JSC, CSCS, BSC, CINECA, KIT, ...)

Summary

- Both PRACE as well as HBP are collaborating e-infrastructures where security risks are dependent not only on the security policies of the own infrastructure
- Security policies and procedures have to be setup globally, which help to circumvent those additional risks.
- These activities are exactly the ones WISE community is undertaking
- so contributing to this work will make future e-infrastructures more secure

Questions