Security and the Human Brain Project

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

DI4R Conference, Krakow, Poland
Sep. 29th 2016

Human Brain Project (HBP)

European Commission Future and Emerging Technologies Flagship

Coordinated 10 years effort to advance neuroscience, medicine and computer science

Building, developing and using a state of the art ICT infrastructure for brain science and cognitive computing.

The Project promotes collaboration across the globe

Started October 2013 and now in phase2 (year 3)

For further info see: www.humanbrainproject.eu

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

Co-funded by the European Union

More about HBP

- **Organized in thirteen subprojects, spanning strategic neuroscience data, cognitive architectures, theory, ethics and society, management**
- **develops six new informatics-based Platforms.**
- **The platforms will be accessible through the HBP Collaboratory – an Internet portal to HBP**

- **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

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**

HBP ICT Platforms

Neuroinformatics Platform

Provides tools to manage, navigate and annotate brain atlases

Brain Simulation Platform

Simulates unifying brain models integrating all available data

Medical Informatics Platform

Data mining on a large volume of federated clinical data

Neuromorphic Computing Platform

Develops and provides access to neuromorphic devices

Neurorobotics Platform

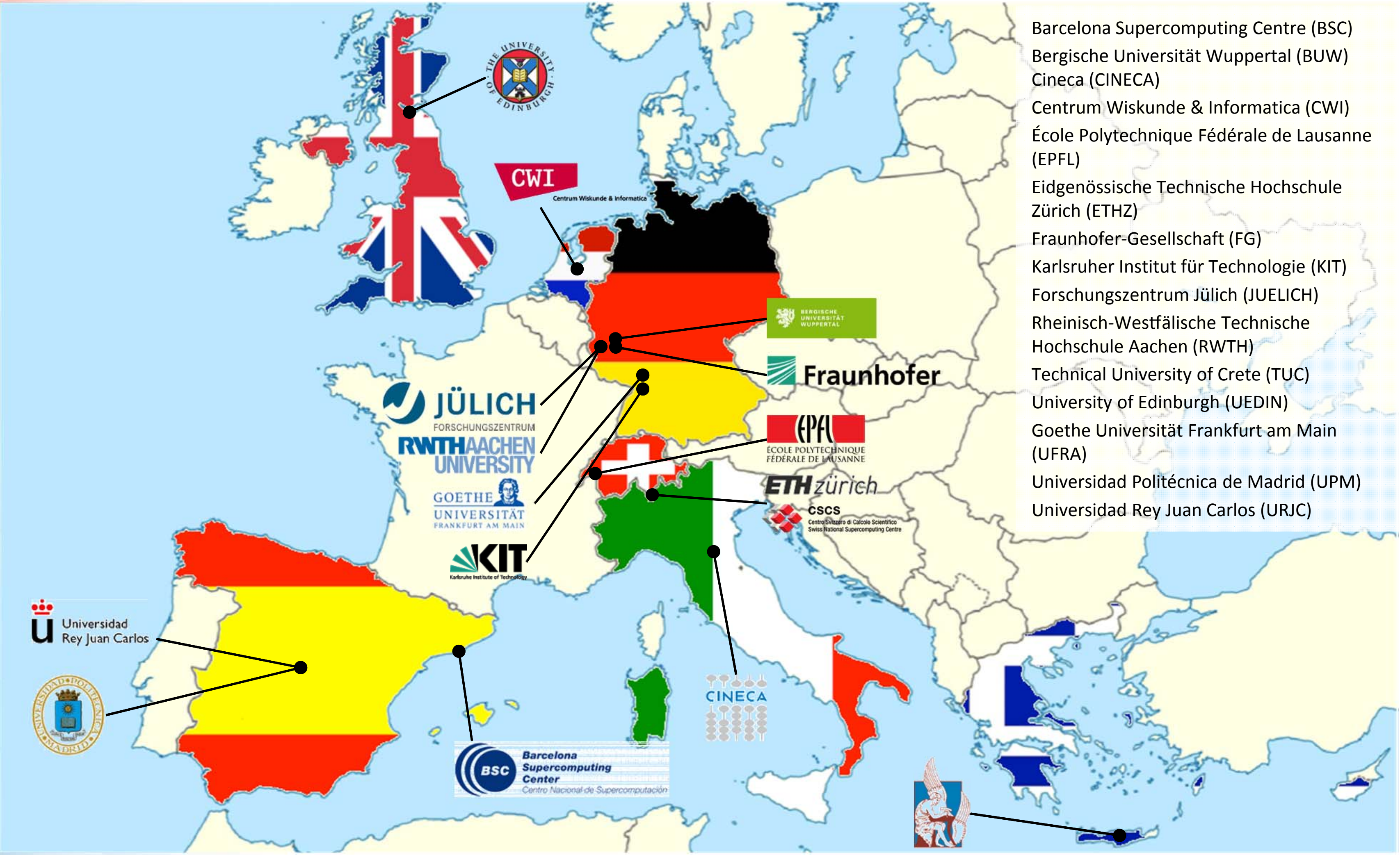
Interfaces a detailed brain model to a simulated body

High Performance Computing Platform

Exascale capability / Big Data /

Interactive Supercomputing / Future Computing (Hybrid)

Subproject 7
15 partners from 7 countries


THE UNIVERSITY OF EDINBURGH
CWI
Centrum Wiskunde & Informatica
BERGISCHE UNIVERSITÄT WUPPERTAL
Fraunhofer
JÜLICH
FORSCHUNGSZENTRUM
RWTHAACHEN UNIVERSITY
GOETHE UNIVERSITÄT FRANKFURT AM MAIN
KIT
Karlsruhe Institute of Technology
EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
ETH zürich
cscs
Centro Svizzero di Calcolo Scientifico
Swiss National Supercomputing Centre
Universidad Rey Juan Carlos
UNIVERSIDAD POLITÉCNICA MADRID
BSC
Barcelona Supercomputing Center
Centro Nacional de Supercomputación
CINECA

Barcelona Supercomputing Centre (BSC)

Bergische Universität Wuppertal (BUW)

Cineca (CINECA)

Centrum Wiskunde & Informatica (CWI)

École Polytechnique Fédérale de Lausanne (EPFL)

Eidgenössische Technische Hochschule Zürich (ETHZ)

Fraunhofer-Gesellschaft (FG)

Karlsruher Institut für Technologie (KIT)

Forschungszentrum Jülich (JUELICH)

Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)

Technical University of Crete (TUC)

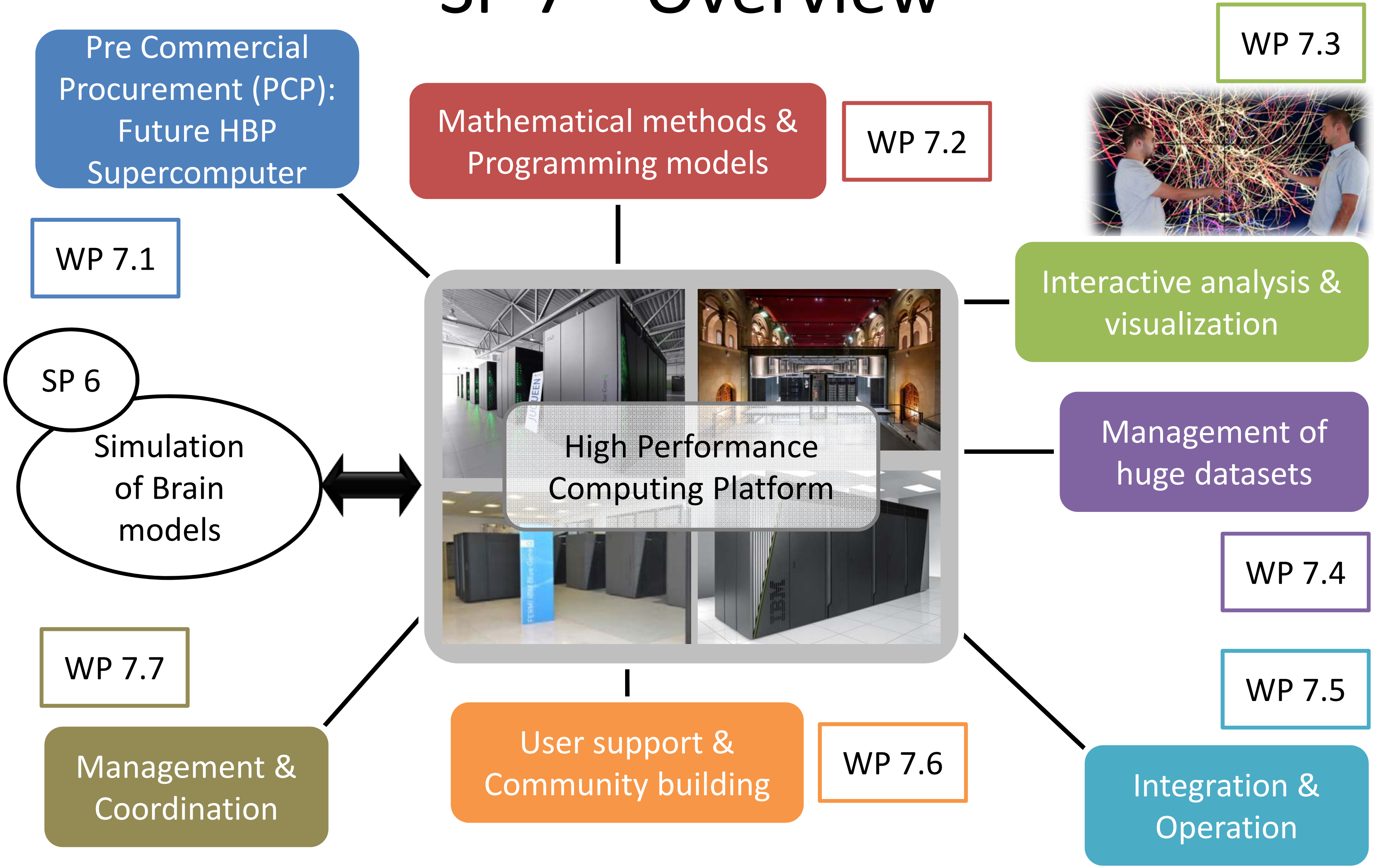
University of Edinburgh (UEDIN)

Goethe Universität Frankfurt am Main (UFRA)

Universidad Politécnica de Madrid (UPM)

Universidad Rey Juan Carlos (URJC)

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

Management of huge datasets

WP 7.4

WP 7.5

Integration & Operation

User support & Community building

WP 7.6

Management & Coordination

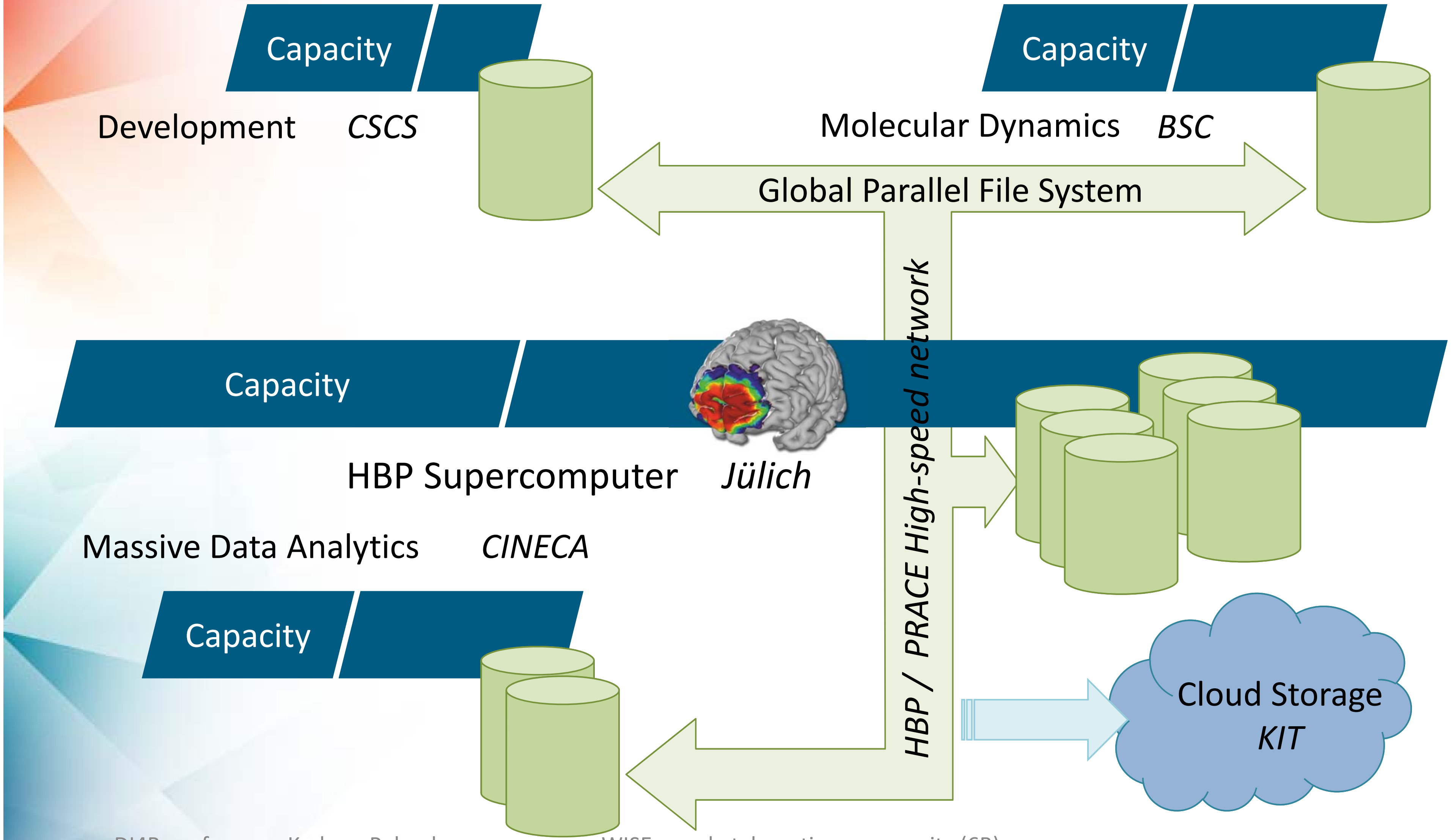
WP 7.7

SP 6

Simulation of Brain models

High Performance Computing Platform

The HBP HPC infrastructure



HBP Security of the HPC infrastructure Where is it handled?

Subtask 7.5.3 Low Level infrastructure services

- Task deals with the operation and maintenance of the low-level federated infrastructure, including the **network**, **AAI**, accounting, monitoring, and middleware.
- **Security aspects** relating to the infrastructure also form an important part of the work.
- Assistance and recommendations for the integration of new computing systems into the infrastructure are also undertaken in this Task.

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

HBP CSIRT Team

- Defines security related Policy and Procedures - to build “A trust model that allows interoperation of the distributed HBP services”;
- Undertakes 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”;
- Manages operational security – to coordinate “incident handling” (CSIRT team)

Security Policies and Procedures

Define:

- minimal security requirements, that HBP HPC 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 HBP HPC 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

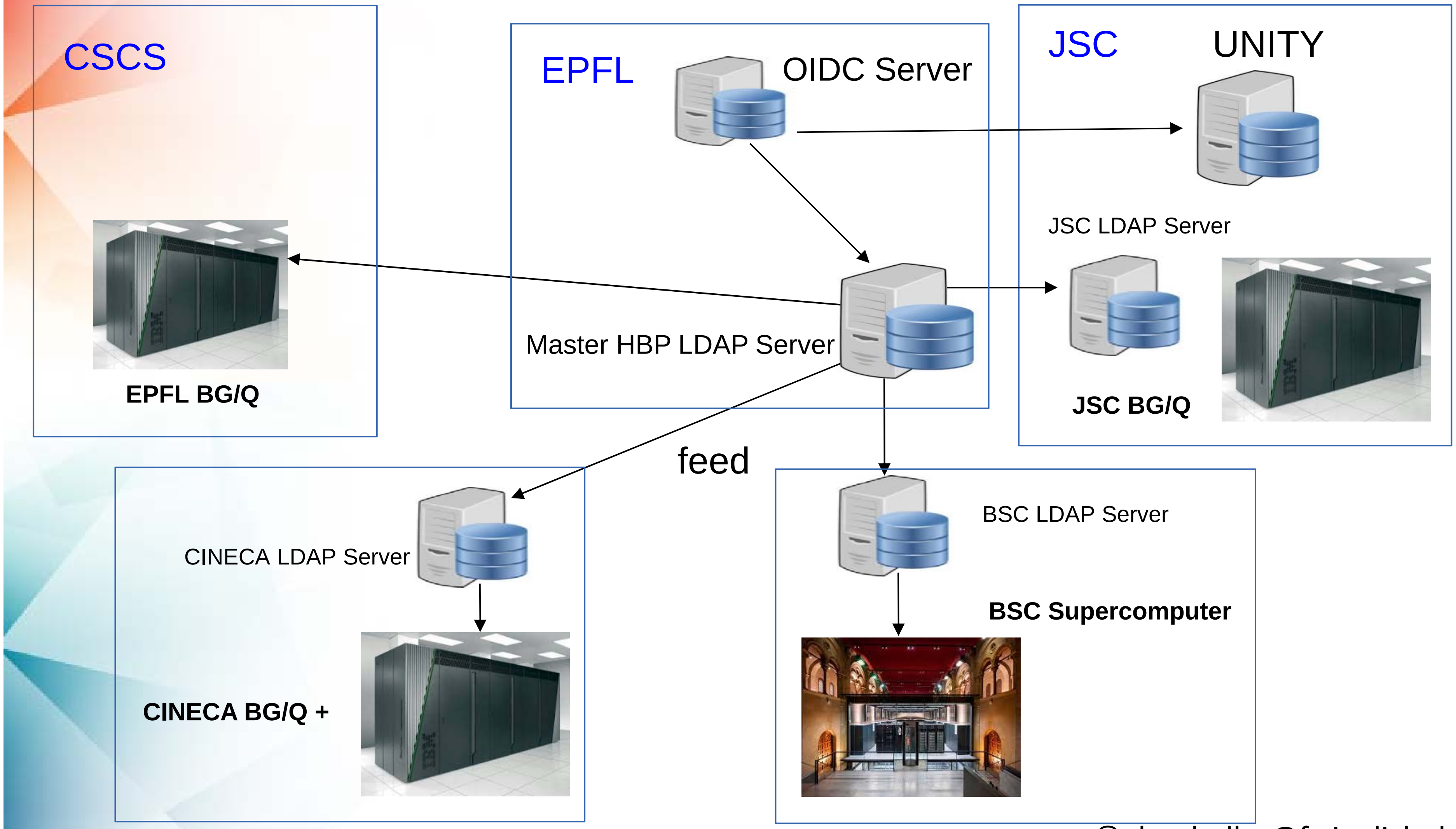
Risk reviews

- The Security Team performs a risk assessment of new services or updates on existing services if changes in the security set-up come up.
- Prerequisites:
  - Provision of security policy documents by every site (Net of Trust model)
  - Possible self-assessment using a document published by SCI group (now WISE SCIV2-WG)

Operational security & Incident response

- All partners provide members to the HBP 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 may be used
- 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.

Centralized LDAP infrastructure



CSCS

EPFL BG/Q

EPFL

OIDC Server

Master HBP LDAP Server

JSC

UNITY

JSC LDAP Server

JSC BG/Q

feed

CINECA LDAP Server

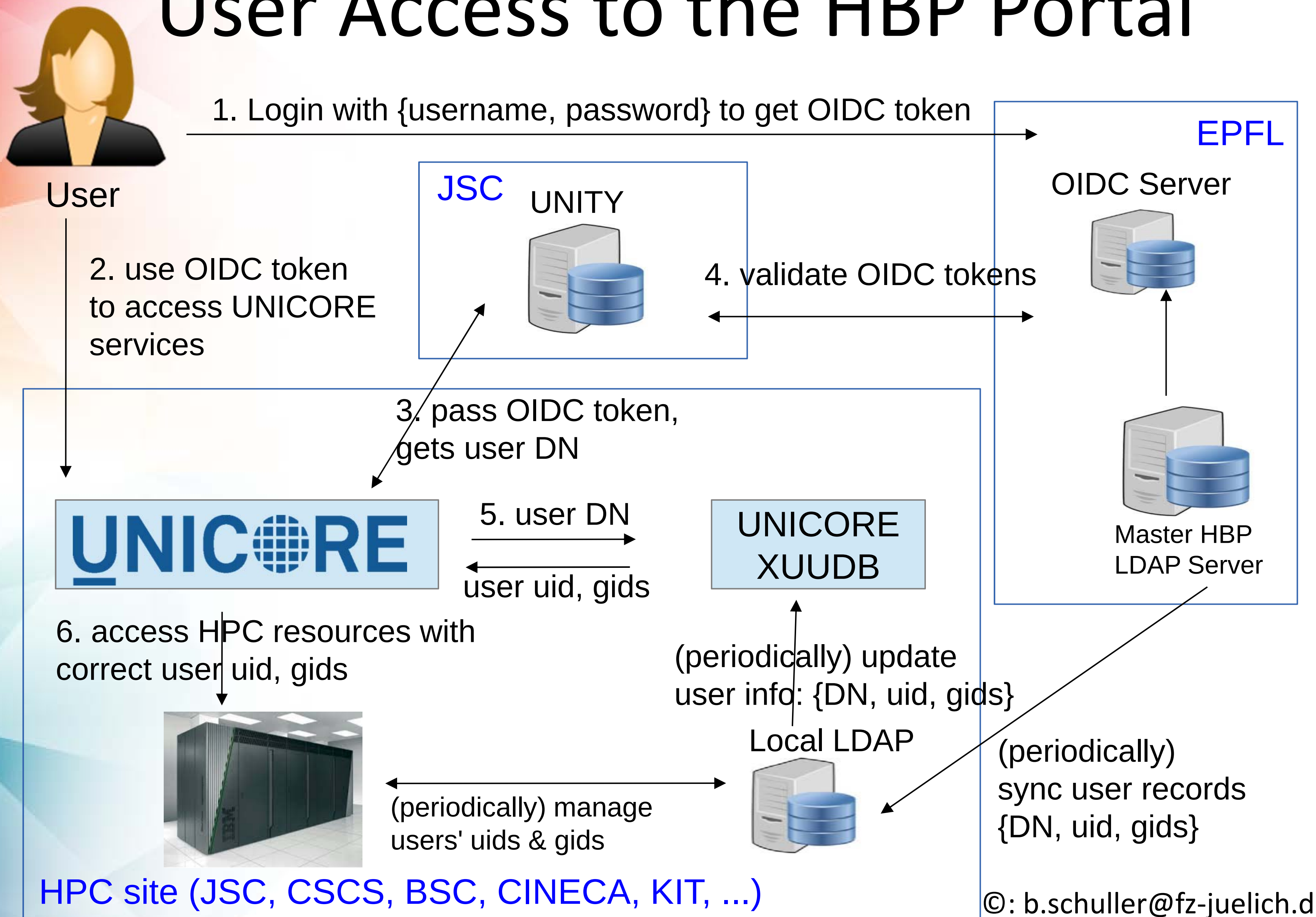
CINECA BG/Q +

BSC LDAP Server

BSC Supercomputer

©: b.schuller@fz-juelich.de

User Access to the HBP Portal



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

2. use OIDC token to access UNICORE services

3. pass OIDC token, gets user DN

4. validate OIDC tokens

5. user DN

user uid, gids

6. access HPC resources with correct user uid, gids

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

(periodically) manage users' uids & gids

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

©: b.schuller@fz-juelich.de

Security collaboration with other projects & activities

Collaboration with

- PRACE and EUDAT CSIRTs on sharing of information on incidents and vulnerabilities
  - exchange of information about incidents if there may be cross domain impacts and also exchange of vulnerability information
  - HBP HPC partners are mostly partners of PRACE and EUDAT also, i.e. are registered at those security alert lists

and active participation within the WISE community

Summary

- HBP is a very huge collaborating e-infrastructure 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