HAMBURG • ZEUTHEN

DESY–Registry

an approach to implement an authorisation management system for the EPICS environment

matthias.clausen@desy.de
tobias.tempel@desy.de

Hamburg · Zeuthen

Purpose of the DESY Registry

HAMBURG • ZEUTHEN

- **cross platform user account management**
- **delegation of management tasks**
- **central support**

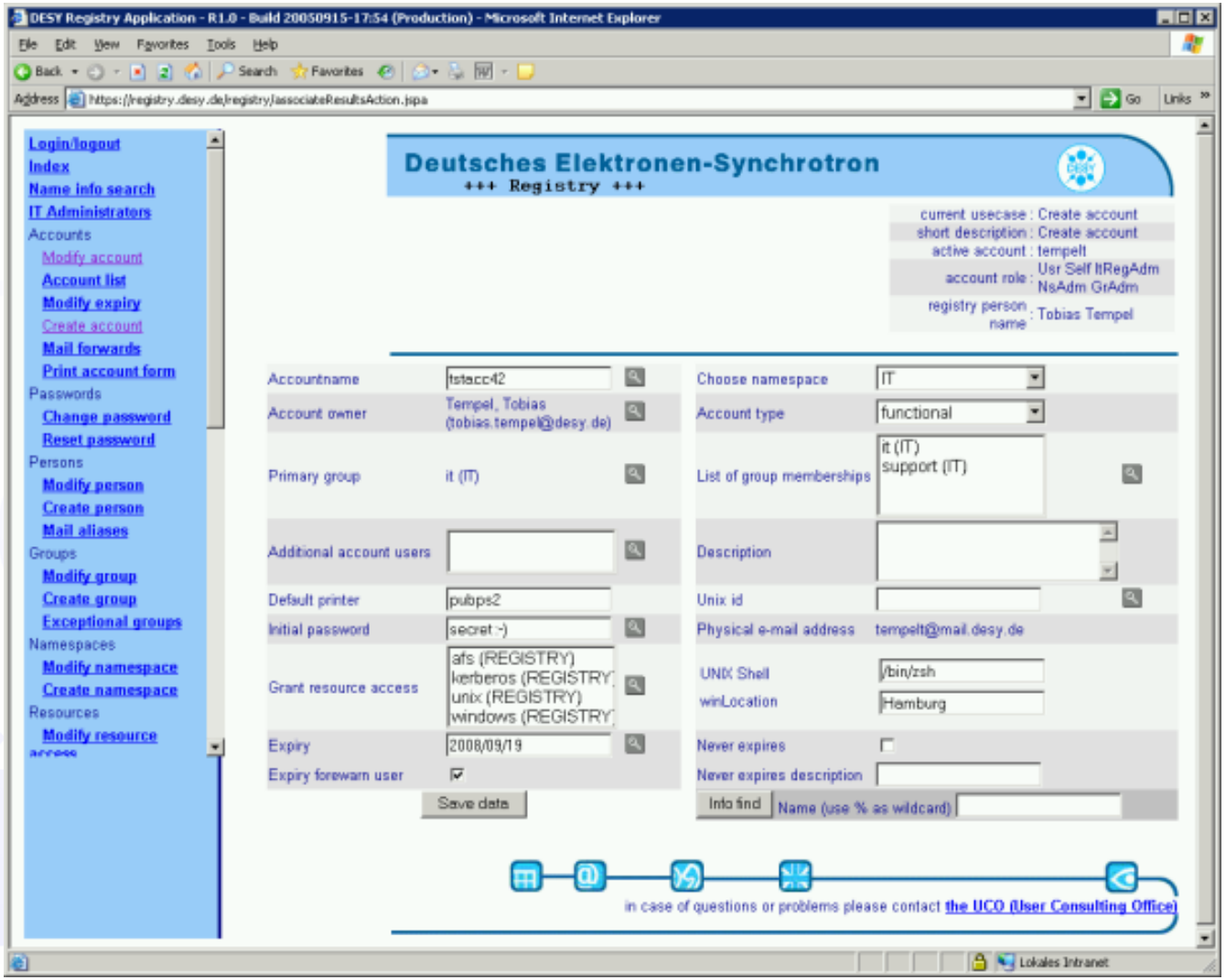
Purpose of the DESY Registry (cont.)

HAMBURG • ZEUTHEN

administration front-end for administrators

- **create and manage accounts**
  - **define access rights for accounts**
    - **file access**
    - **resource access (computer, cluster, console …)**
- **organize accounts in groups**
- **reset passwords**
- **maintain user information**

Example web form “create account”

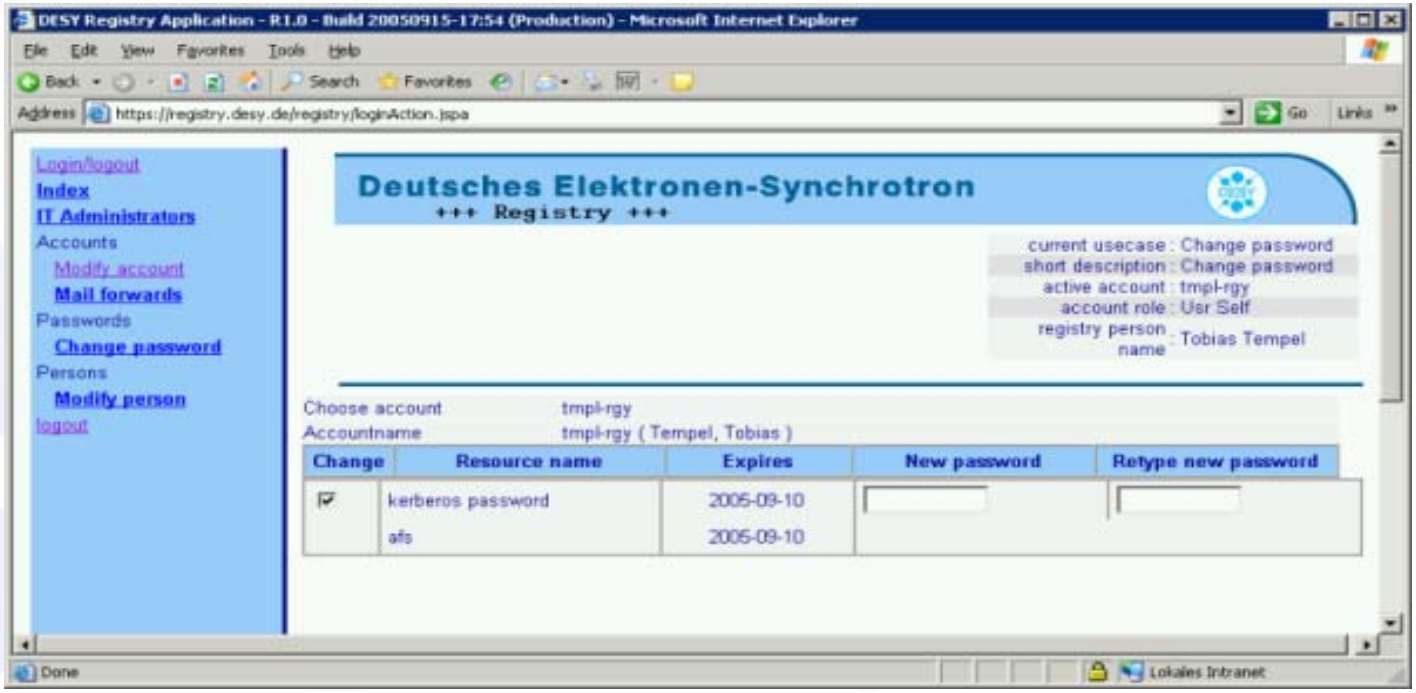


Purpose of the DESY Registry (cont.)

HAMBURG • ZEUTHEN

functionality for users

- **change passwords**
- **modify user and mail address attributes**



Purpose of the DESY Registry (cont.)

HAMBURG • ZEUTHEN

automatic control of object expirations

- **daily expiration scanner job**
- **checks account expiration**
- **expiration of passwords and access rights**
- **warning mails for users and administrators**

Delegation of administrative rights

HAMBURG • ZEUTHEN

- **organization of accounts and other managed objects in namespaces**
- **delegation of administration of namespaces - and objects within - to distinct administrators**
- **possibility to explicitly delegate administration of groups and resources**
- **role model to define administrative rights**

The Registry and the real world

HAMBURG • ZEUTHEN

- **propagation of user account data to platforms**
- **configurable registry event and platform job subsystem**
- **preferred communication between registry and platforms by SOAP webservices**

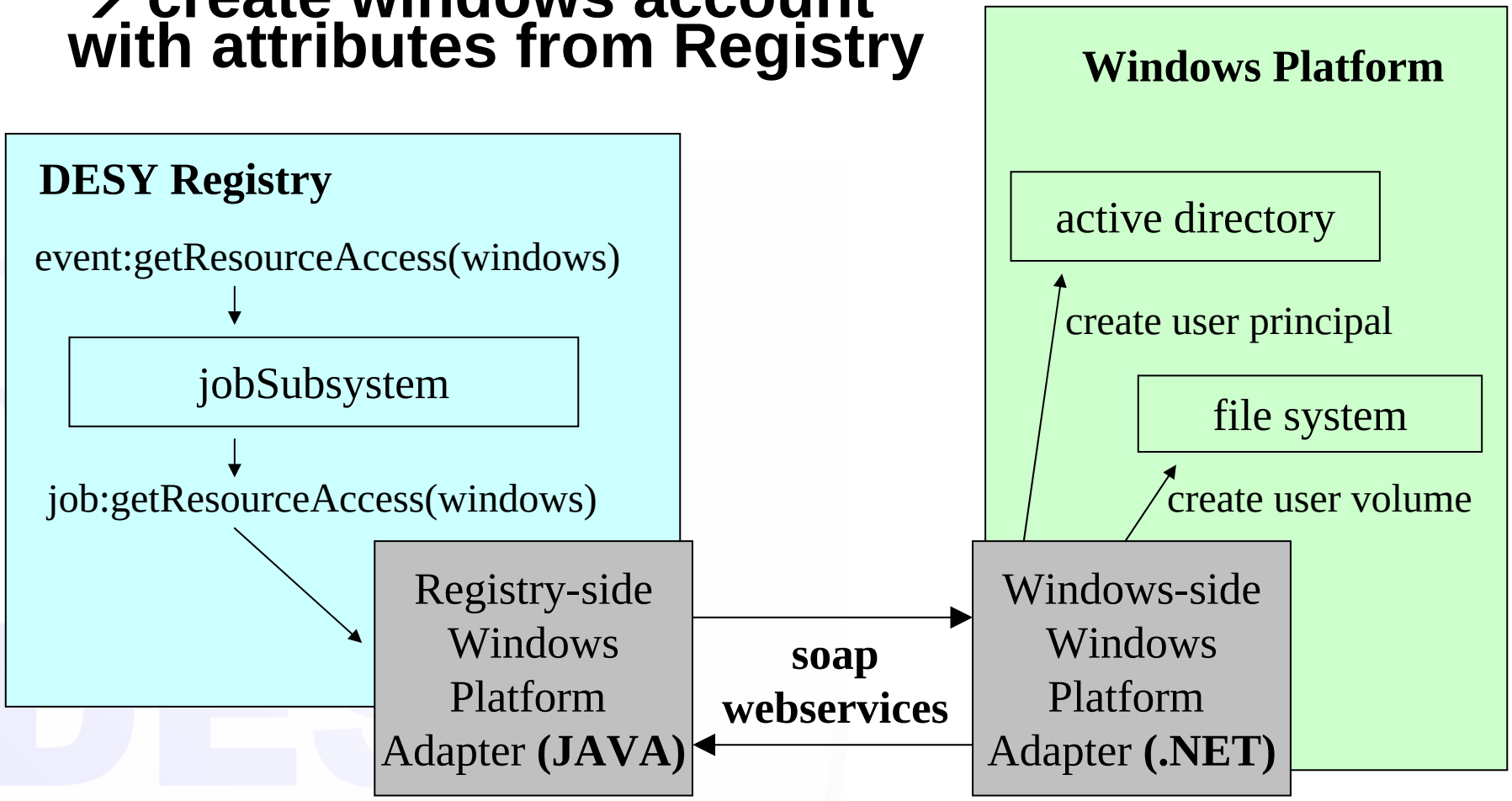
Registry platform adapter

HAMBURG • ZEUTHEN

- **connection to platforms via registry platform adapter architecture**
- **platform side adapters can be implemented with java, pearl, .NET, ...**
- **simple platform adapters with script-invocation or file transfer possible**

Registry platform adapter example

create account and give windows system access
→ create windows account
with attributes from Registry



High availability ?

HAMBURG • ZEUTHEN

what the Registry is

- **a cross platform administration tool for accounts**

what the Registry is not

- **an authentication system for platforms**
- **an online information service for platforms**
- **high availability system**
- **a systems management tool**
- **a monitoring tool**

There is no need for high availability of the Registry application.

Used technologies

- **J2EE - Java 2 enterprise edition**
- **JBoss J2EE application server**
- **Oracle database server**
- **Struts based web application**
- **SOAP webservices communication**

Implemented platform adapters

HAMBURG • ZEUTHEN

- **AFS**
- **Kerberos**
- **Unix / NIS / netgroups**
- **Zeuthen location account administration**
- **Windows active directory**
- **LDAP**
- **Unix mail server / Windows Exchange**

DESY-Registry and EPICS

HAMBURG • ZEUTHEN

Scenario for using the DESY Registry for EPICS

- account and user management for control systems
- expiration of access rights
- authorization management for:
  - access to console workstations (groups of console workstations)
  - access to (generic) EPICS IOC access specified by text attributes

DESY Registry and EPICS adapter

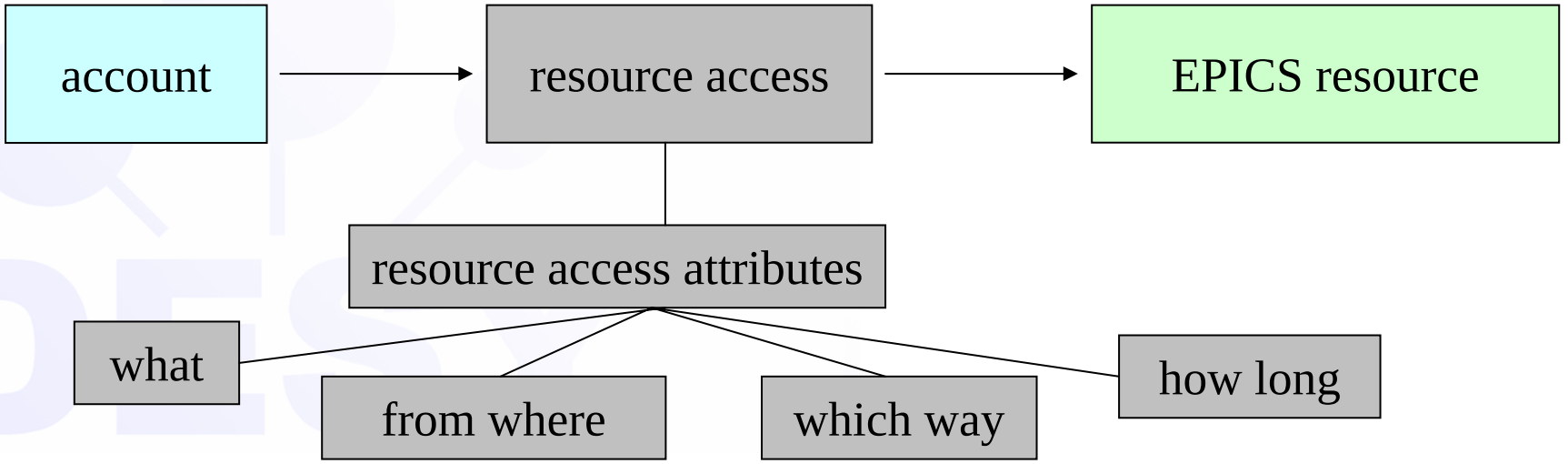
HAMBURG • ZEUTHEN

Connecting the Registry to EPICS

- Registry connects to EPICS platform adapter at EPICS boot application server
- script- and file-transfer-based platform adapter generates text file for IOC
- EPICS platform adapter writes authorization info for operator workstation access to local group and passwd files
- Windows platform adapter writes group membership info for console workstation access to active directory

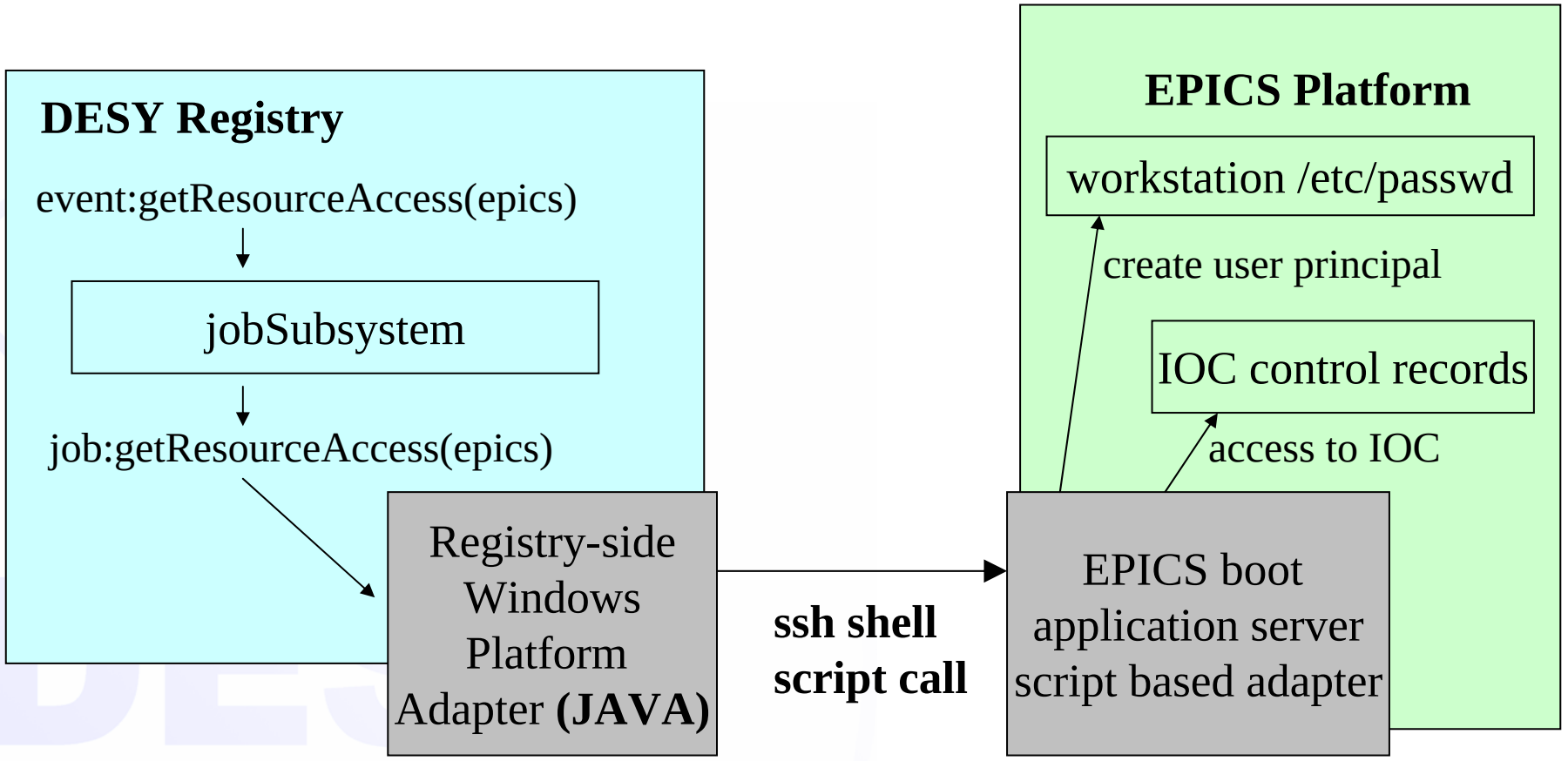
Example EPICS access authorization

- **define an EPICS-IOC resource in Registry**
- **example attributes of EPICS-IOC resource**
  - **which IOC(s) read/write access is granted to**
  - **from which workstation IOC(s) can be accessed**
  - **which access control records are visible**
  - **other right / restrictions / expiration of access**



Example EPICS prototype adapter

- **prototypical script based EPICS platform adapter distributes access control records to IOC(s)**



Restrictions

HAMBURG • ZEUTHEN

- **for now the GUI does not support to manage very large amounts of Resources (systems that access rights can be granted to)**
  - should be not more than 100

- **GUI also does not support to manage large amounts of Resource attributes per resource**
  - should be not more than 10

- **restriction must be kept in mind when modeling connection to EPICS with many ‘IO Controllers’ and many ‘Control Blocks’**

Outlook

HAMBURG • ZEUTHEN

- **prototypically implementation at the DESY site with existing Registry instance**
- **implementing a simple EPICS platform adapter as rapid prototyping approach**
- **setting up Registry instances at other sites**
- **connecting other control systems**
- **try to establish community software development for DESY Registry application**
  - **PKI infrastructure**
  - **support for EPICS-records as individual resources**