

## **Towards Privacy-Aware eLearning**

Katrin Borcea, Hilko Donker, Elke Franz,  
Andreas Pfitzmann, and Hagen Wahrig

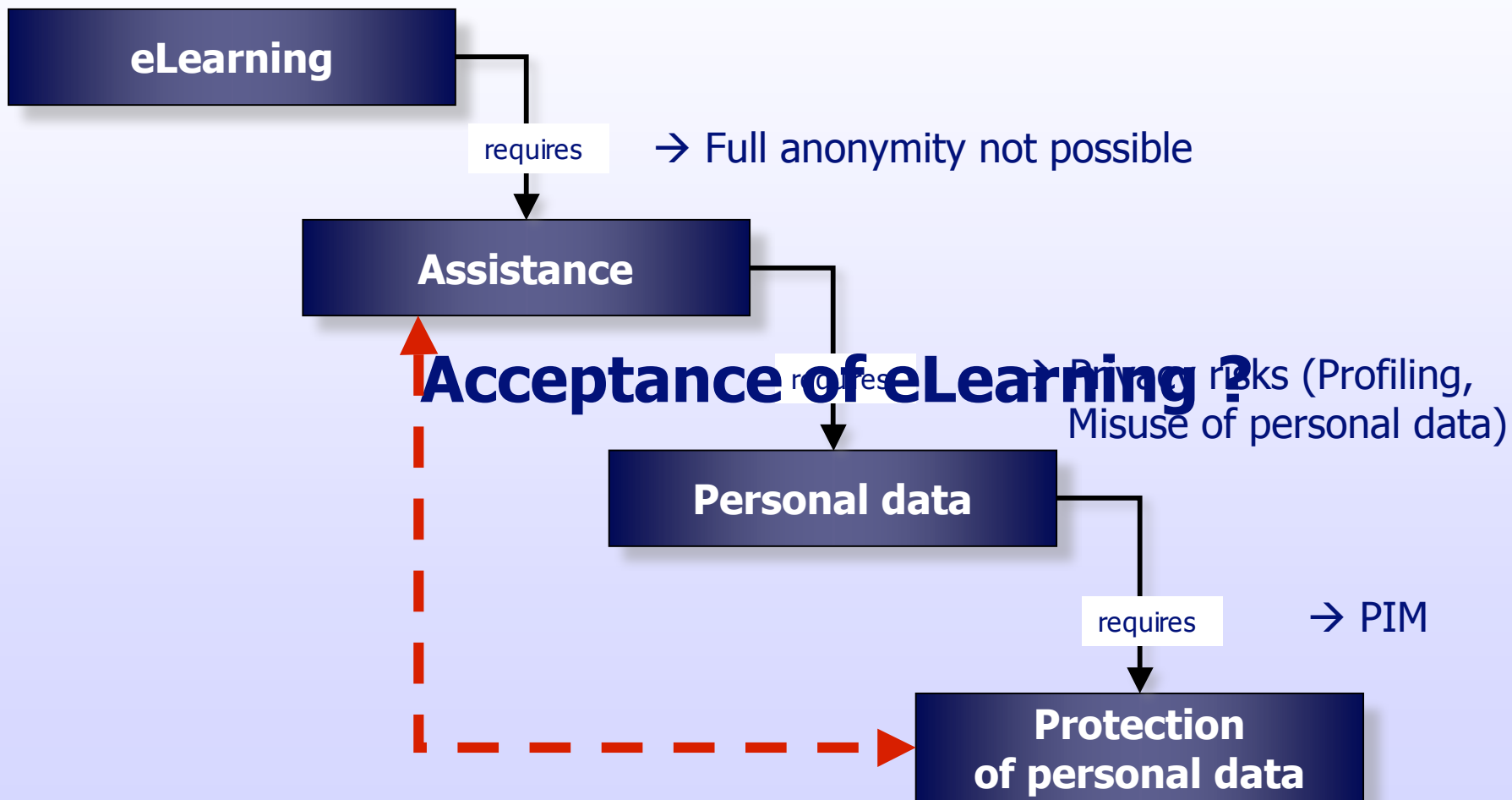
{borcea|donker|ef1|pfitza|wahrig}@inf.tu-dresden.de

**PET 2005**

**Workshop on Privacy Enhancing Technologies**

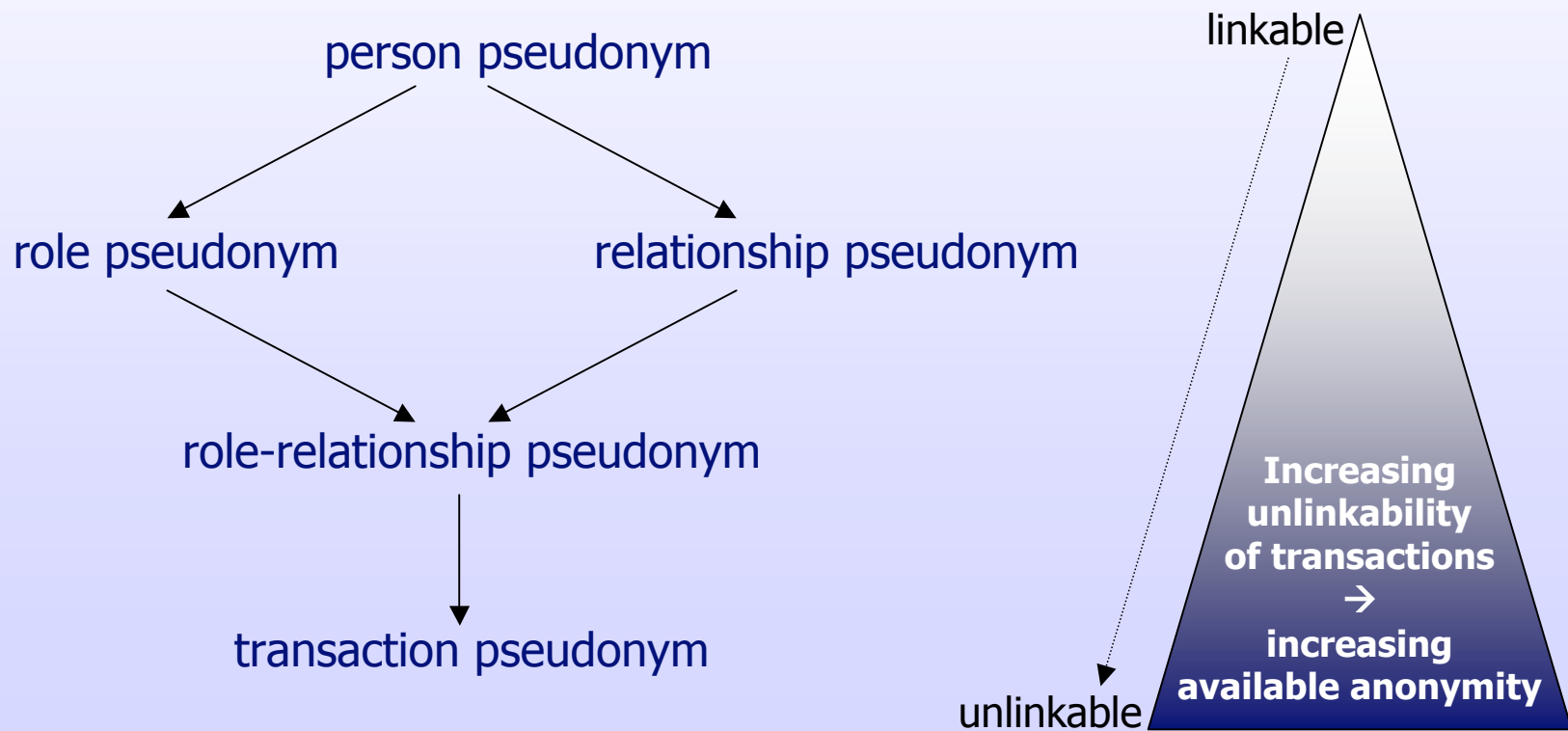
Dubrovnik (Cavtat), Croatia, May 30 - June 1, 2005

- **Motivation**
- **Principles of Privacy and Security**
- **Short Introduction to eLearning**
- **Privacy Issues within eLearning**
- **Sketch of a Privacy-Enhancing Architecture**
- **Example Scenario: Process Learning Modules**
- **Summary and Outlook**



- **Principles of privacy and security**
  - Data minimization and avoidance
  - Transparency and user control
  - Data partitioning
  - Unlinkability
- **PIM – Privacy-Enhancing Identity Management**
  - Enables users to control which personal information they disclose to whom in the digital world
  - Users can act as they are used to in everyday life
  - Subset of personal information: partial identity
  - Pseudonyms = identifiers for partial identities

### Kinds of pseudonyms determine degree of anonymity



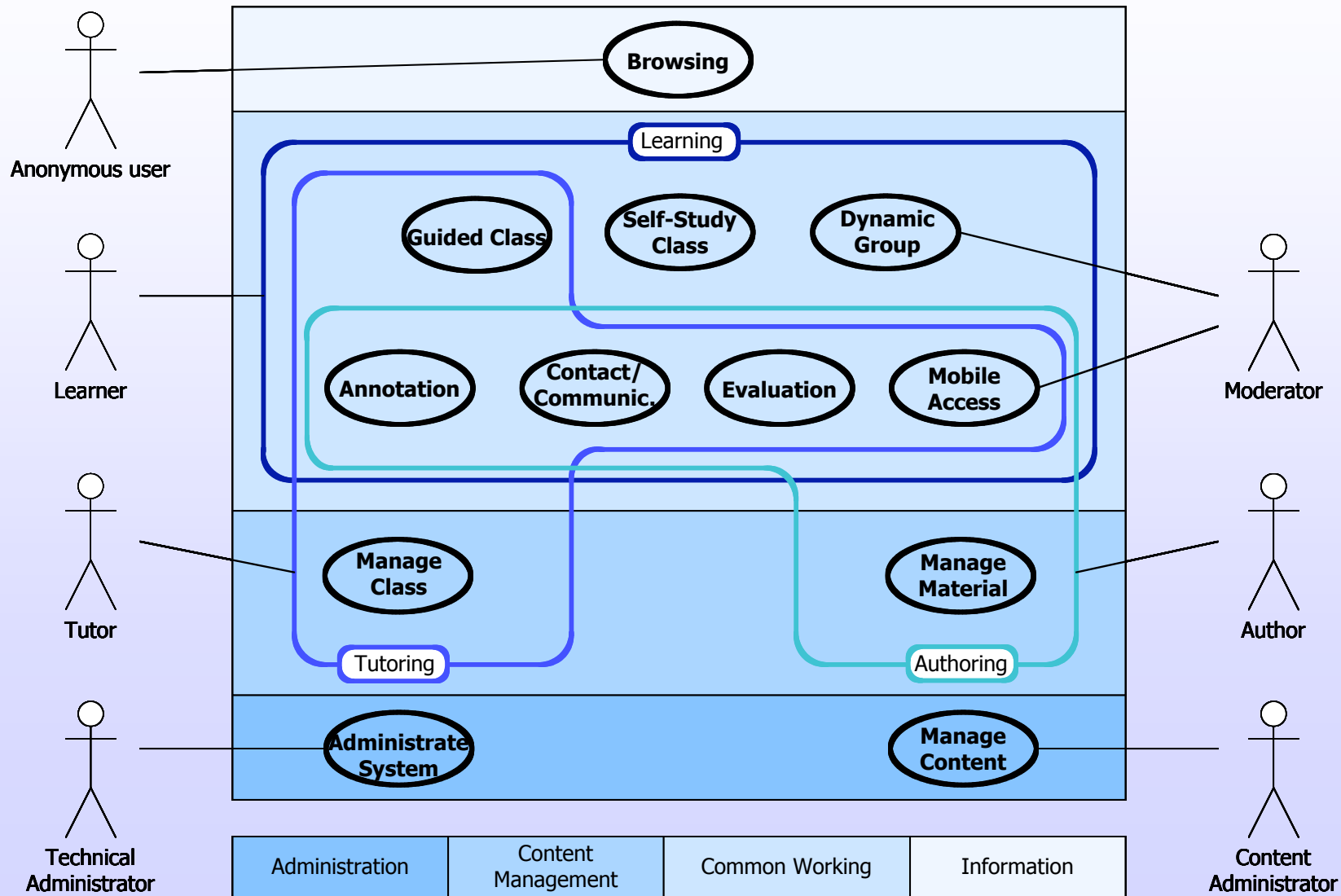
### **Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology**

[http://dud.inf.tu-dresden.de/Literatur\\_V1.shtml](http://dud.inf.tu-dresden.de/Literatur_V1.shtml)

Draft v0.21 Sep. 03, 2004

### **Privacy enhancing identity management enabling application design:**

An application is designed in a privacy enhancing identity management enabling way if neither the pattern of sending/receiving messages nor the attributes given to entities (i.e., humans, organizations, computers) imply more linkability than is strictly necessary to achieve the purposes of the application.



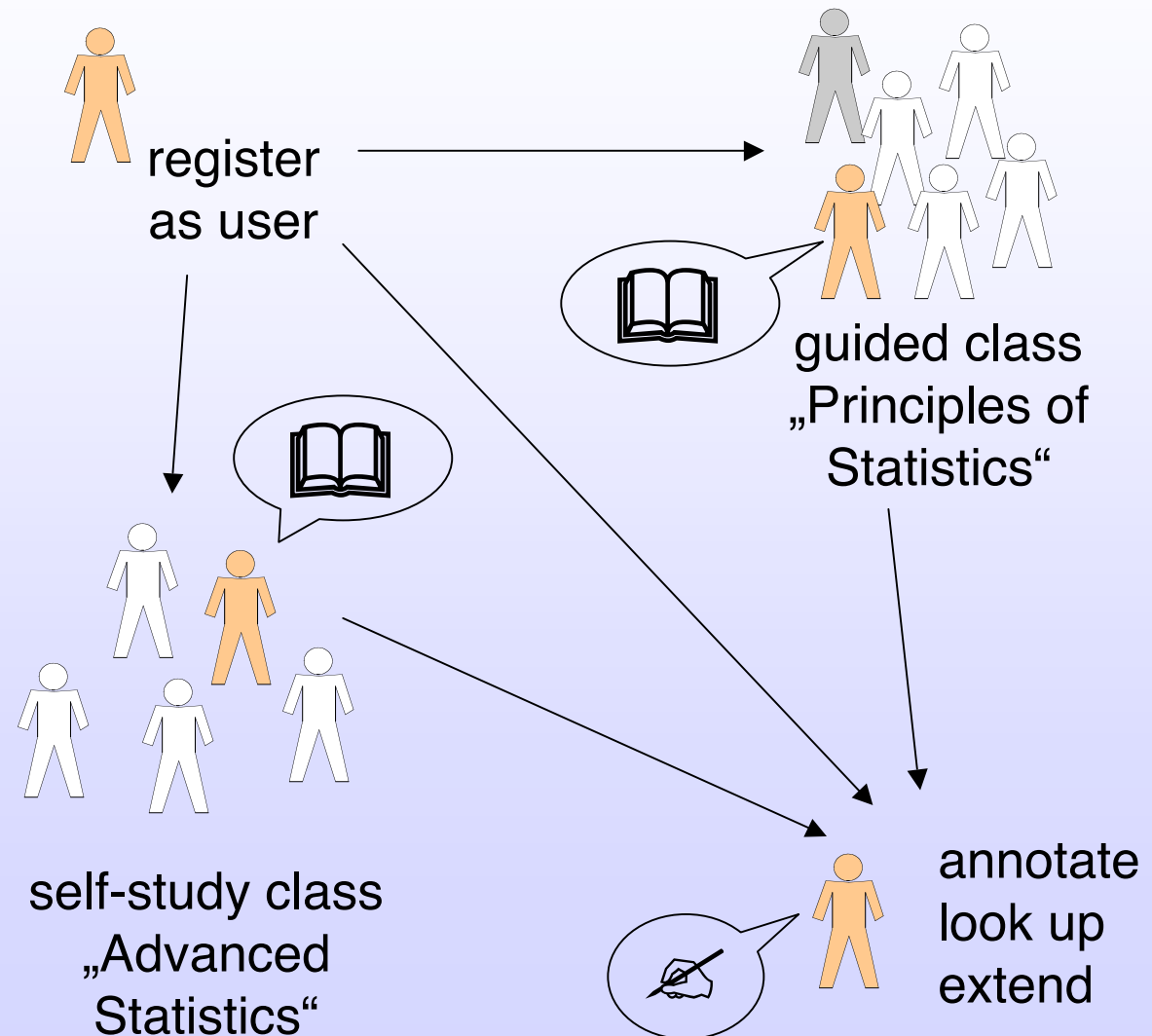
# Privacy Issues within eLearning (1)

John Primeur  
John.Primeur@aol.com  
Germany

attended class 1  
Principles of Statistics  
tutor: Mr Smith  
date: Jan. 9-27, 2004  
points: 79

personal workspace

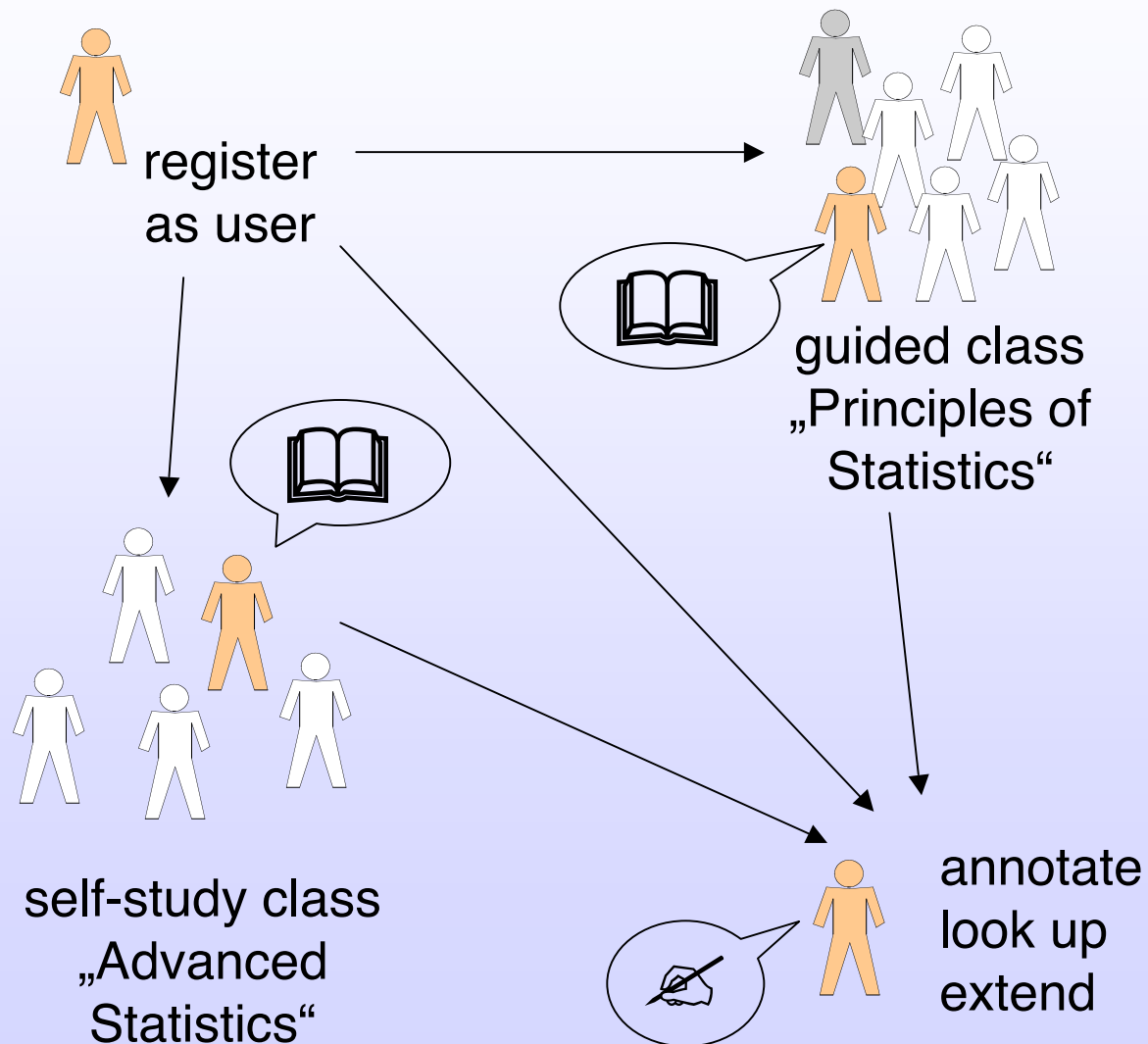
attended class 2  
Advanced Statistics  
date: June 23, 2004  
points: 50



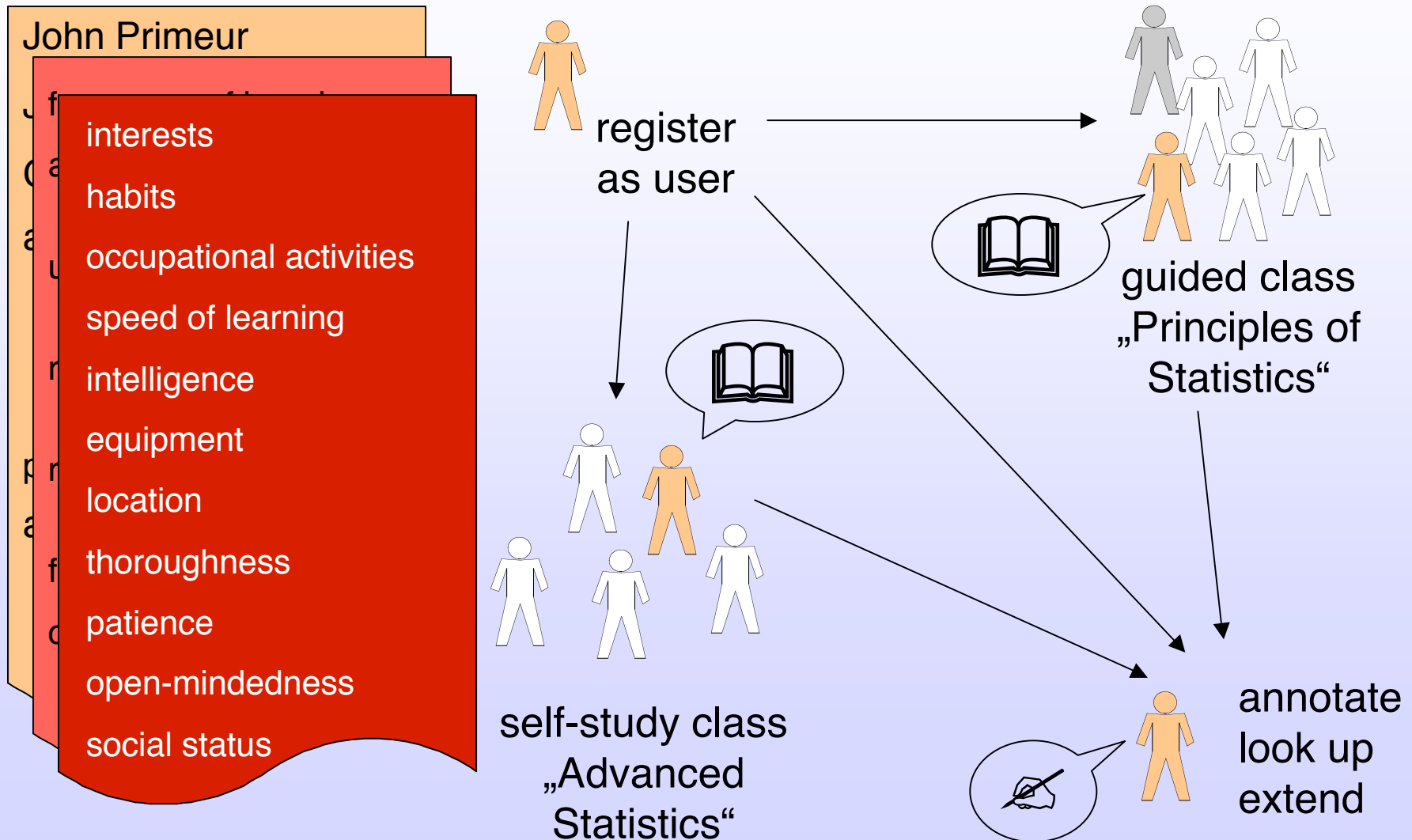
## Privacy Issues within eLearning (2)

**John Primeur**

- frequency of learning sessions
- average duration of learning
- usual points in time for learning
- ratio points/average points of other learners
- ratio points/necessary points
- frequency of questions
- content of questions



# Privacy Issues within eLearning (3)



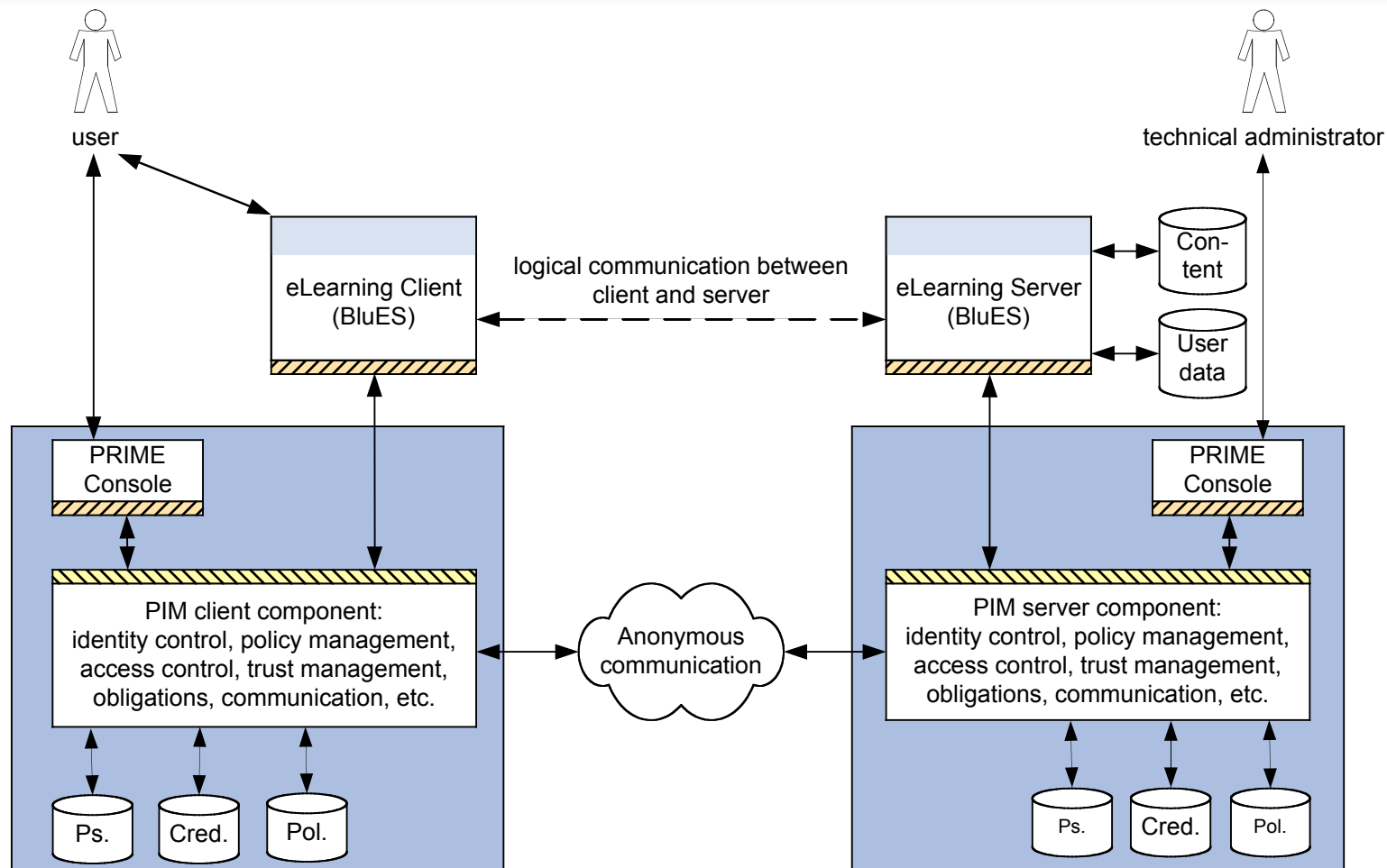
### Conclusion

- Users must be able to **control what others know** about them
- Necessary: **fine-grained partitioning of personal data** within application, even within single application scenarios
- Use of **pseudonyms**, since users cannot act completely anonymously
- **Partial identities** must be established depending on the working context of the users
- **Transaction pseudonyms**: maximum anonymity, used only once
- **Role-relationship pseudonyms, relationship-pseudonyms**: support recognition, e.g., enable reasonable discussions in dynamic groups

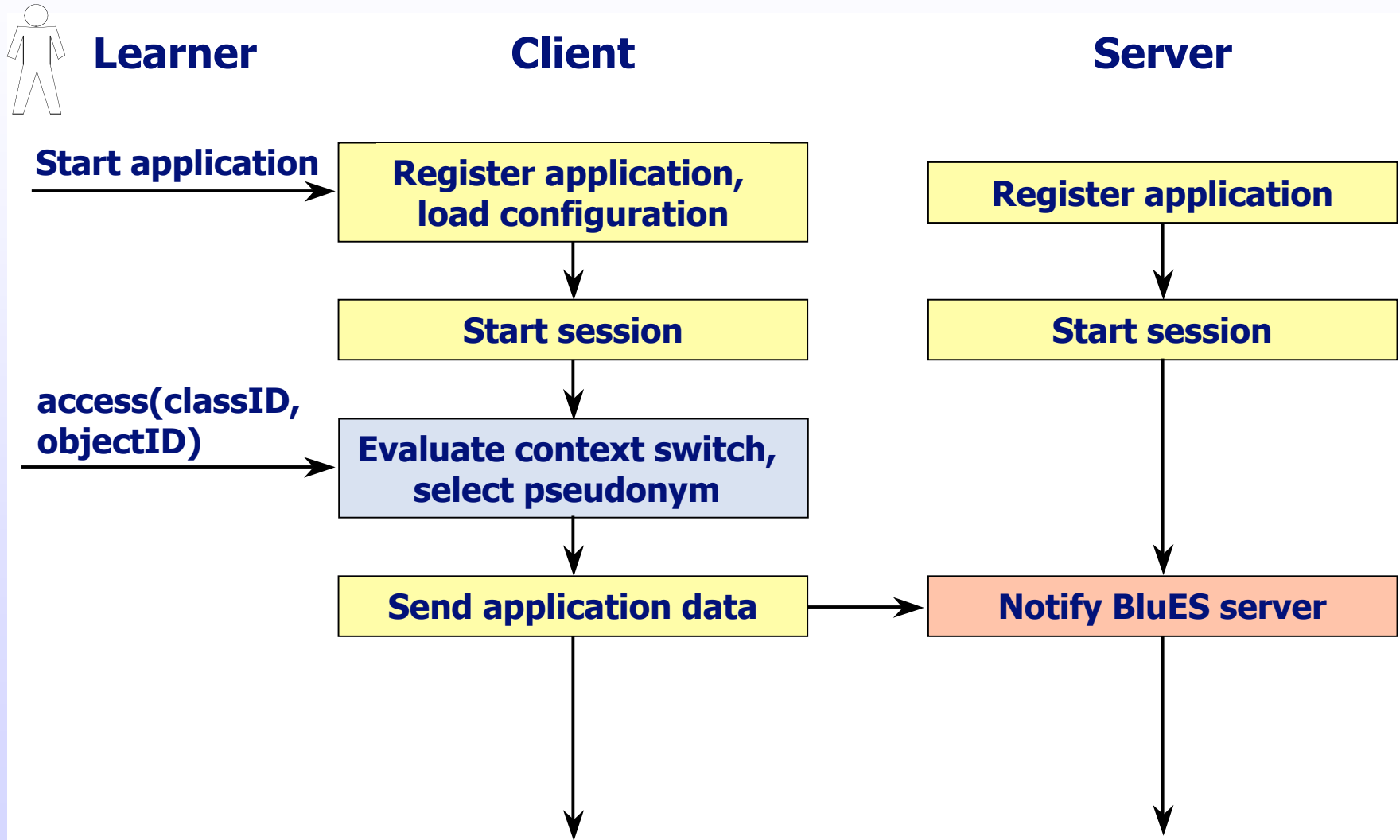
### Use of PIM

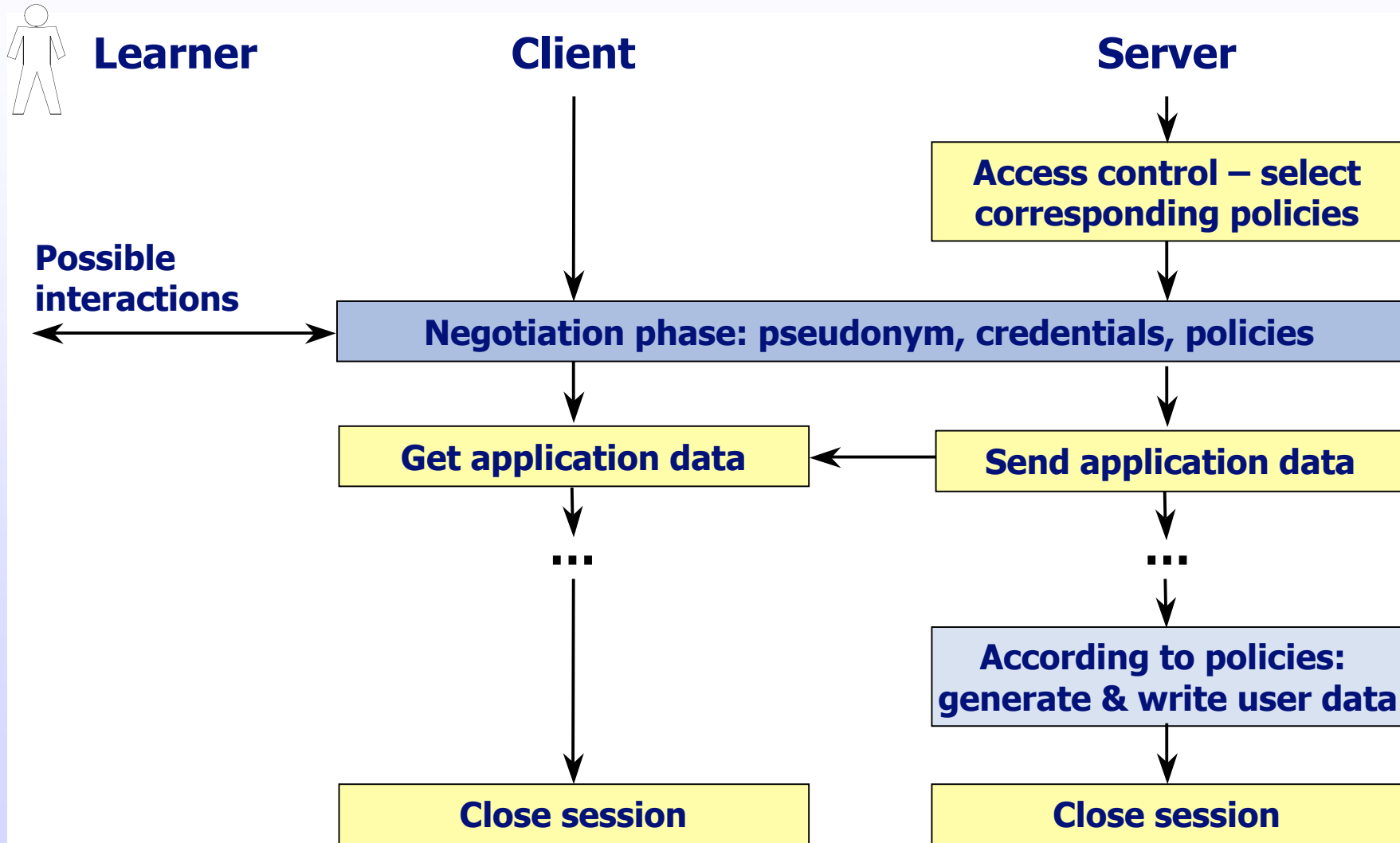
- Information about users can be assigned to their different partial identities only
- Assistance is possible – tutor can monitor learning progress w.r.t. partial identities
- Only holder of pseudonyms can link different partial identities (e.g., in order to build up one's own reputation)

# Sketch of a Privacy-Enhancing Architecture



- PIM-aware platform
- eLearning specific extension w.r.t. PIM
- Interface provided by application
- Interface provided by PIM
- Ps. Pseudonyms
- Cred. Credentials
- Pol. Policies





- **Discussion about privacy issues within eLearning**
- **Conflicting requirements: Anonymity vs. assistance**
- **Approach: using a platform that provides PIM**
- **Expected advantages of a privacy-aware eLearning environment:**
  - **Opportunity to increase awareness of privacy threats**
  - **Increases understanding of privacy-enhancing mechanisms**
- **Currently: realization of the approach**
- **Future work: investigate practical issues (performance, usability, user acceptance)**
- **Self-reflexive learning**