2005
iSSE
INFORMATION SECURITY SOLUTIONS EUROPE

Pseudonymous Authentication and Authorization enhancing ubiquitous Identity Management

Thomas Hildmann
hildmann@prz.tu-berlin.de
Berlin University of Technology (TUB)

Content

- Motivation
  - Advantages of pseudonymous A+A
- Pseudonymous Authentication
- Pseudonymous Authorization
  - ADFBlinder
  - Hiding of Structure-Application Mapping
  - Isolated ADF-Components
- Summary

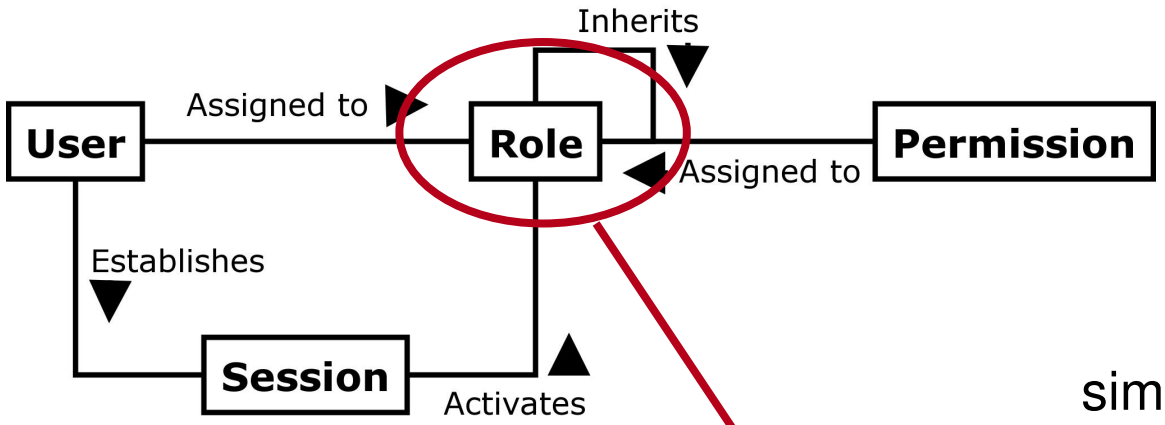
Motivation

- Ubiquitous A+A
  - Just one (meta-) database
  - Effective, consistent
- Pseudonymity
  - Privacy Law
  - Unions
  - Employees
  - Insider attacks
  - Works in B2B-Environments (multi-party A+A)
  - Good for outsourcing
  - In case of an incident
- Multilateral Security
  - Principles and Methods are well-investigated

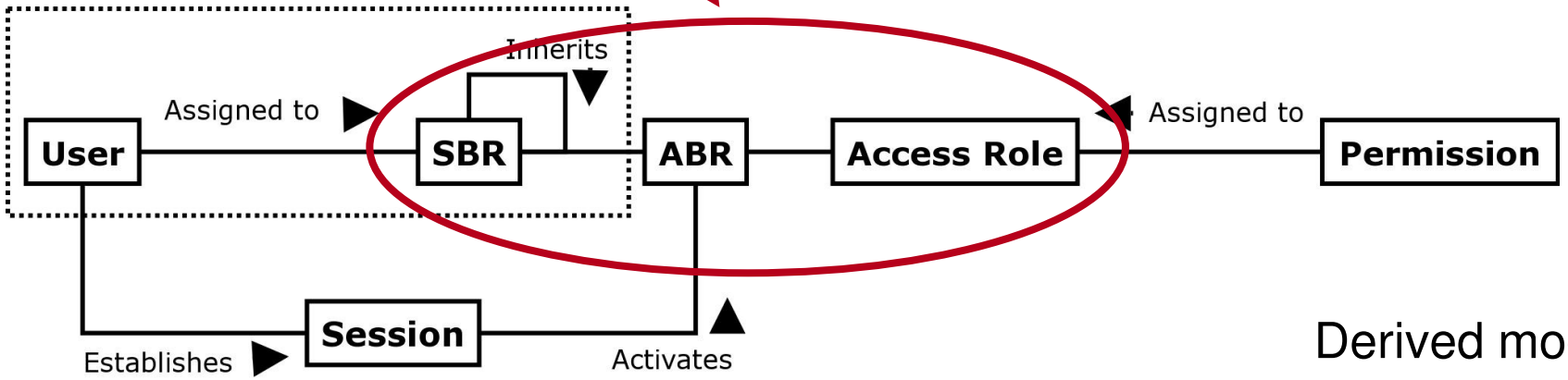
Pseudonymous Authentication

- Implemented in Project „Campuskarte“
- Basic idea
  - Separation of Card-ID and User-ID
  - Card-ID revocation-lists
  - Knowledge is distributed between Application, Authentication-Server, Card-Database and Client-Computer

Basic RBAC-Model



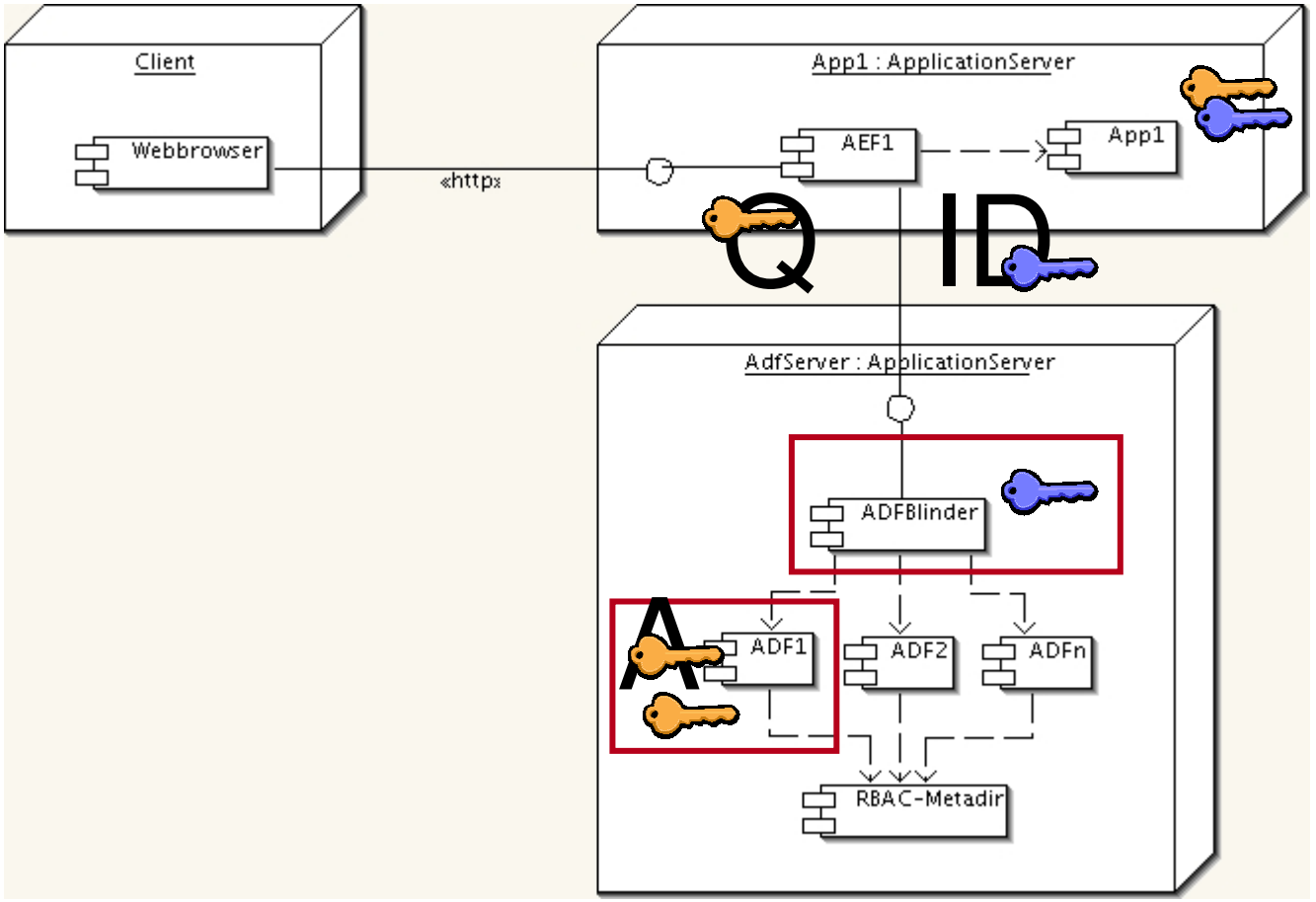
UML-representation of
simplified NIST RBAC model



Derived model

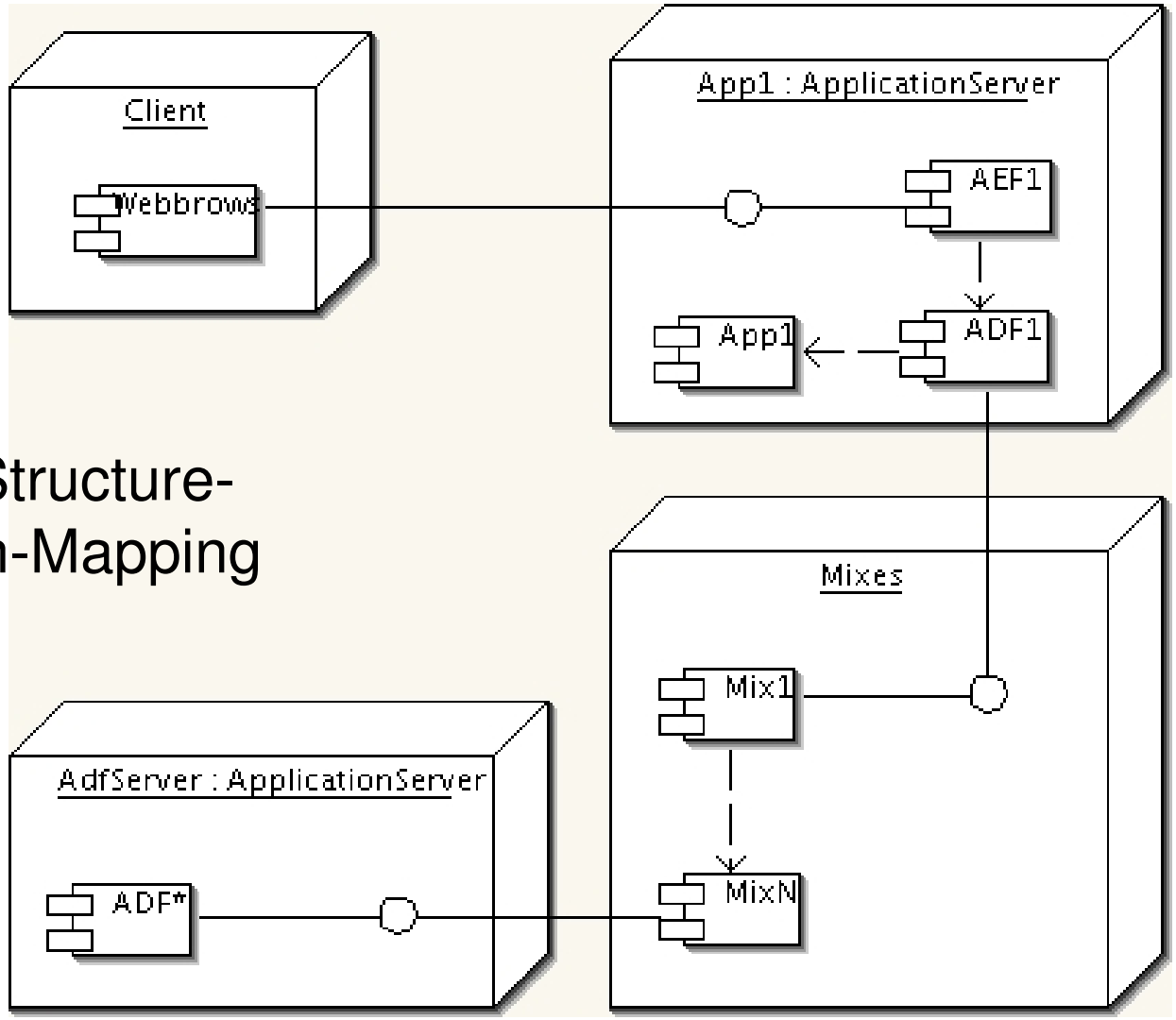
How to archive pseudonymity?

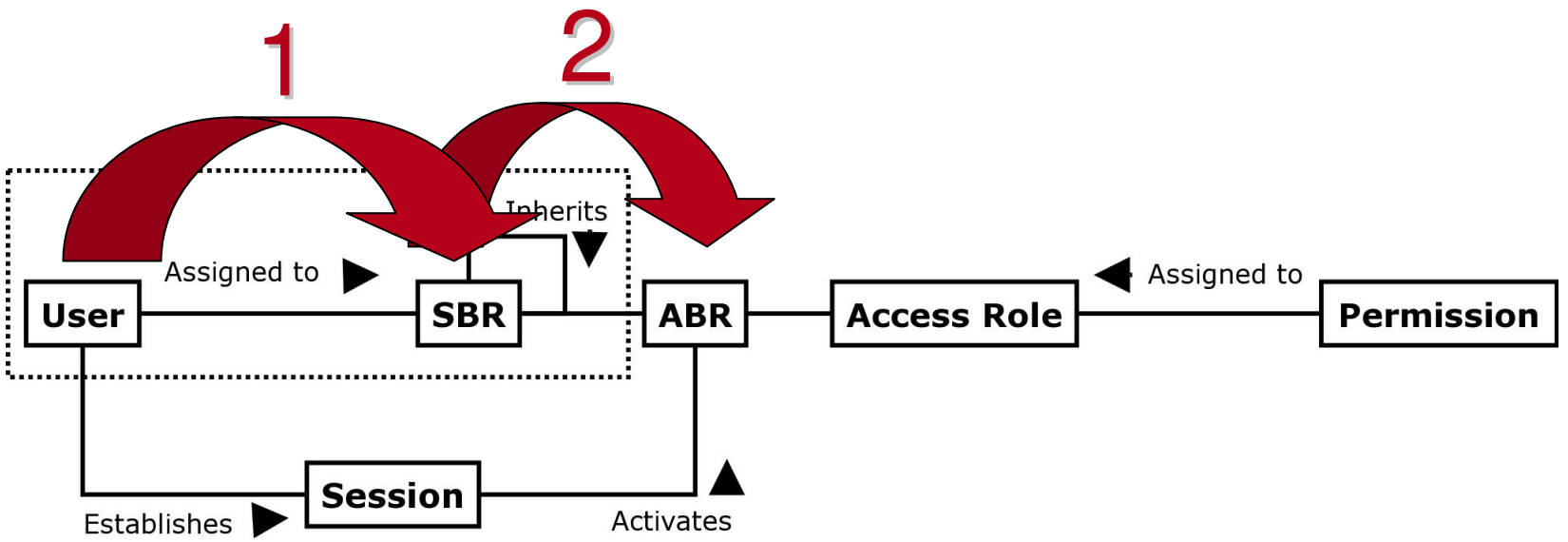
- To authorize a person (s)he must be identified (may be pseudonymously).
- Maintaining pseudonymity during the authorization-process.
- This is possible by deploying necessary information: Initiator (subject), application/data (object), function (operation)



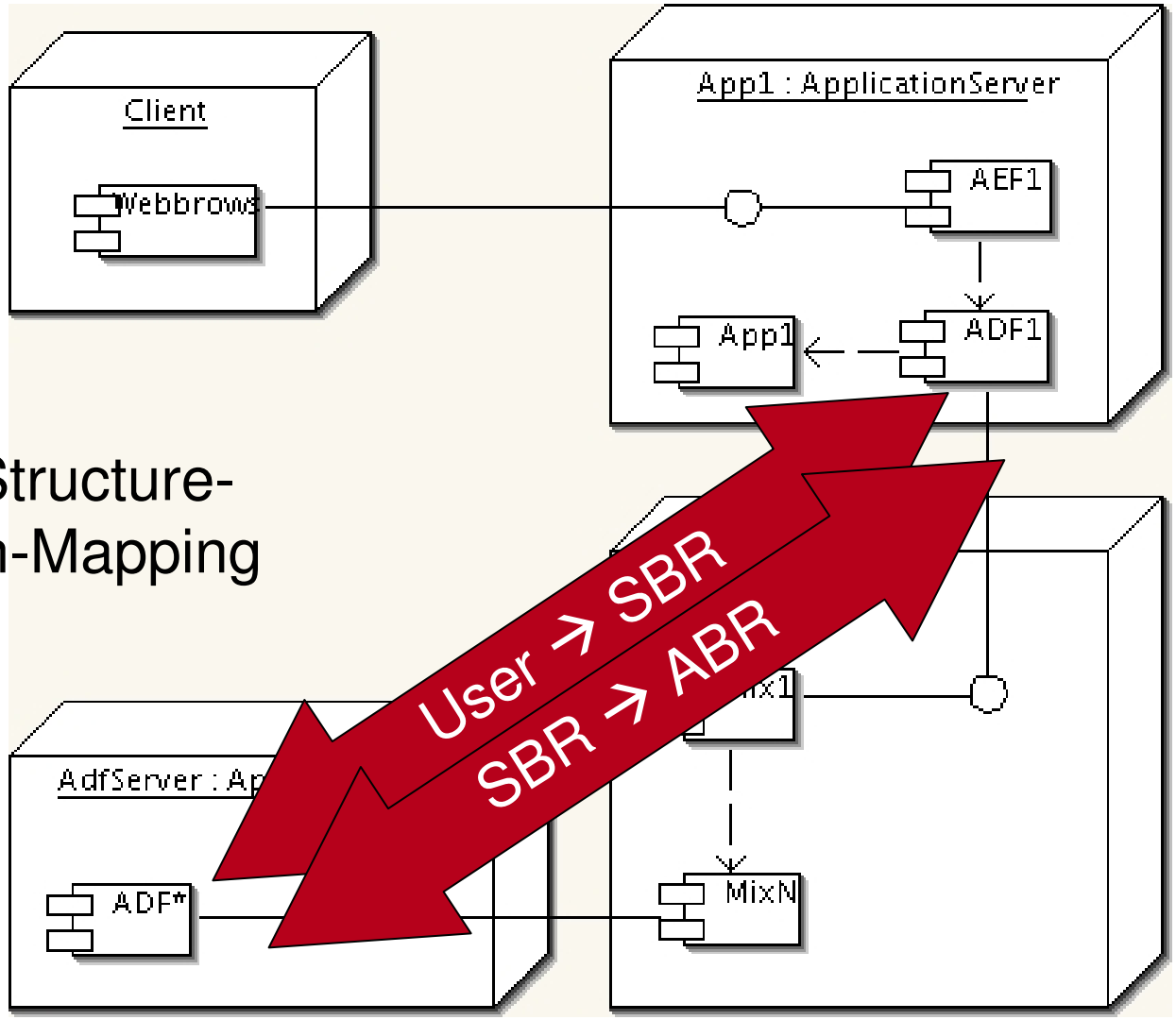
ADFBlinder-Architecture

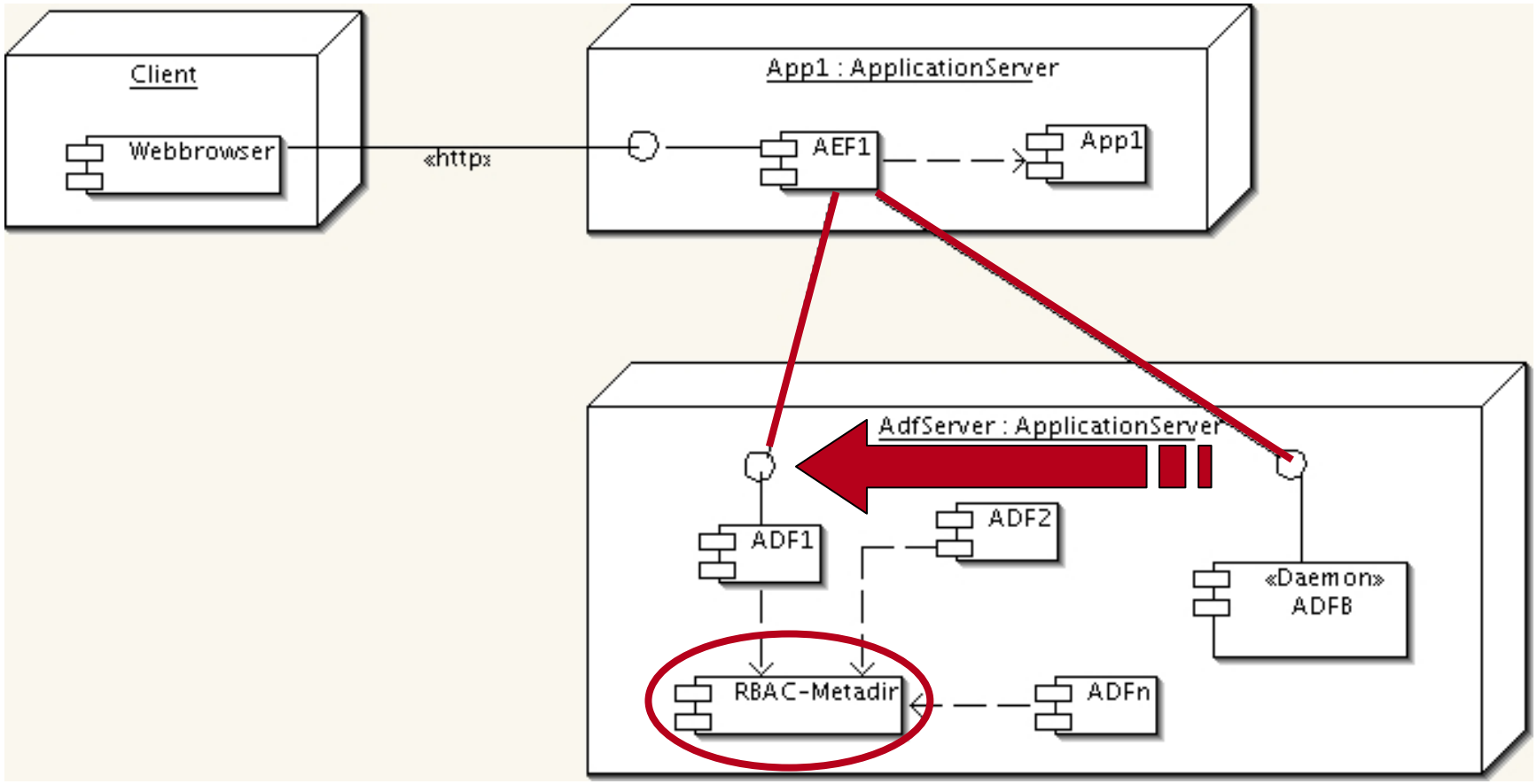
Hiding of Structure-Application-Mapping




1
2
Inherits
Assigned to
Assigned to
User
SBR
ABR
Access Role
Permission
Session
Establishes
Activates

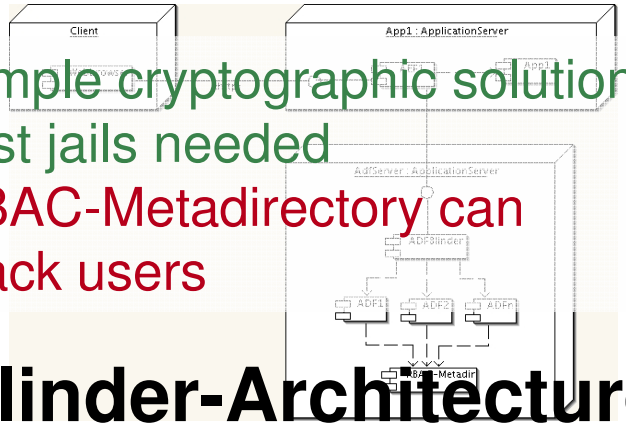
Hiding of Structure-Application-Mapping





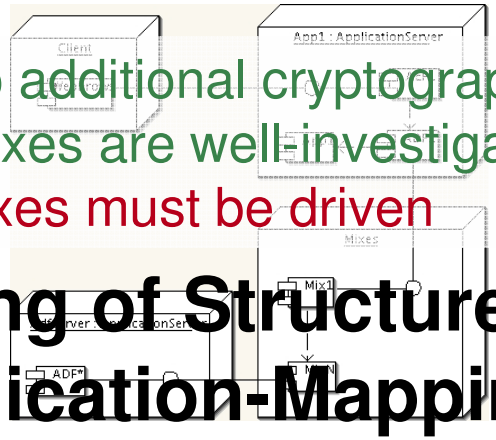
Isolated ADF-Components

Comparing



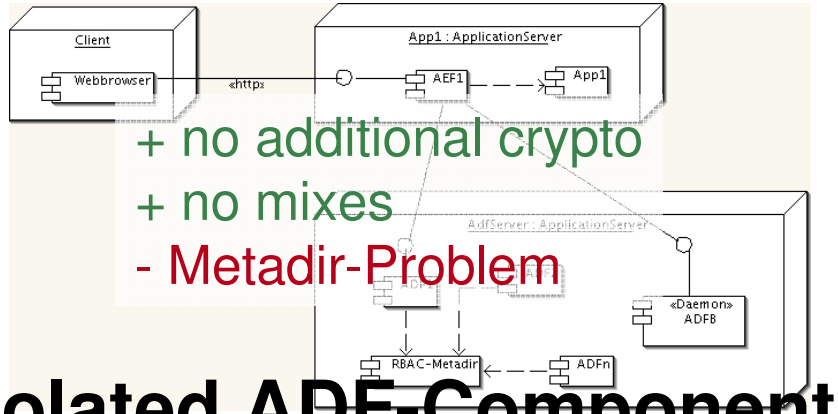
+ simple cryptographic solution
+ just jails needed
- RBAC-Metadirectory can track users

ADFBlinder-Architecture



+ no additional cryptography
+ mixes are well-investigated
- mixes must be driven

Hiding of Structure-Application-Mapping



+ no additional crypto
+ no mixes
- Metadir-Problem

Isolated ADF-Components

Summary

- Advantages of ubiquitous IDM
  - Centralized structure / decentralized management
  - Homogeneous policy / fine grained customization
  - Users controlling their own identity
- Disadvantages without pseudonymity
  - Traceability
- Pseudonymous Authorization
  - Different implementation possible
  - We are implementing one

Outlook

- Implementation of RBAC-IDM System at Berlin University of Technology (TUB)
  - Application comprehensive
  - Modeling of organization- and access-roles
  - Use of modeling patterns (like programming patterns)
  - Pseudonymous Authentication and Authorization
  - Self administration and delegation of rights
  - Privacy suitable IDM
  - Distributed cross-organizational RBAC

hildmann@prz.tu-berlin.de