TECHNISCHE UNIVERSITÄT MÜNCHEN

Enhancing Trust in SOA Based Collaborative Environments

Latifa Boursas

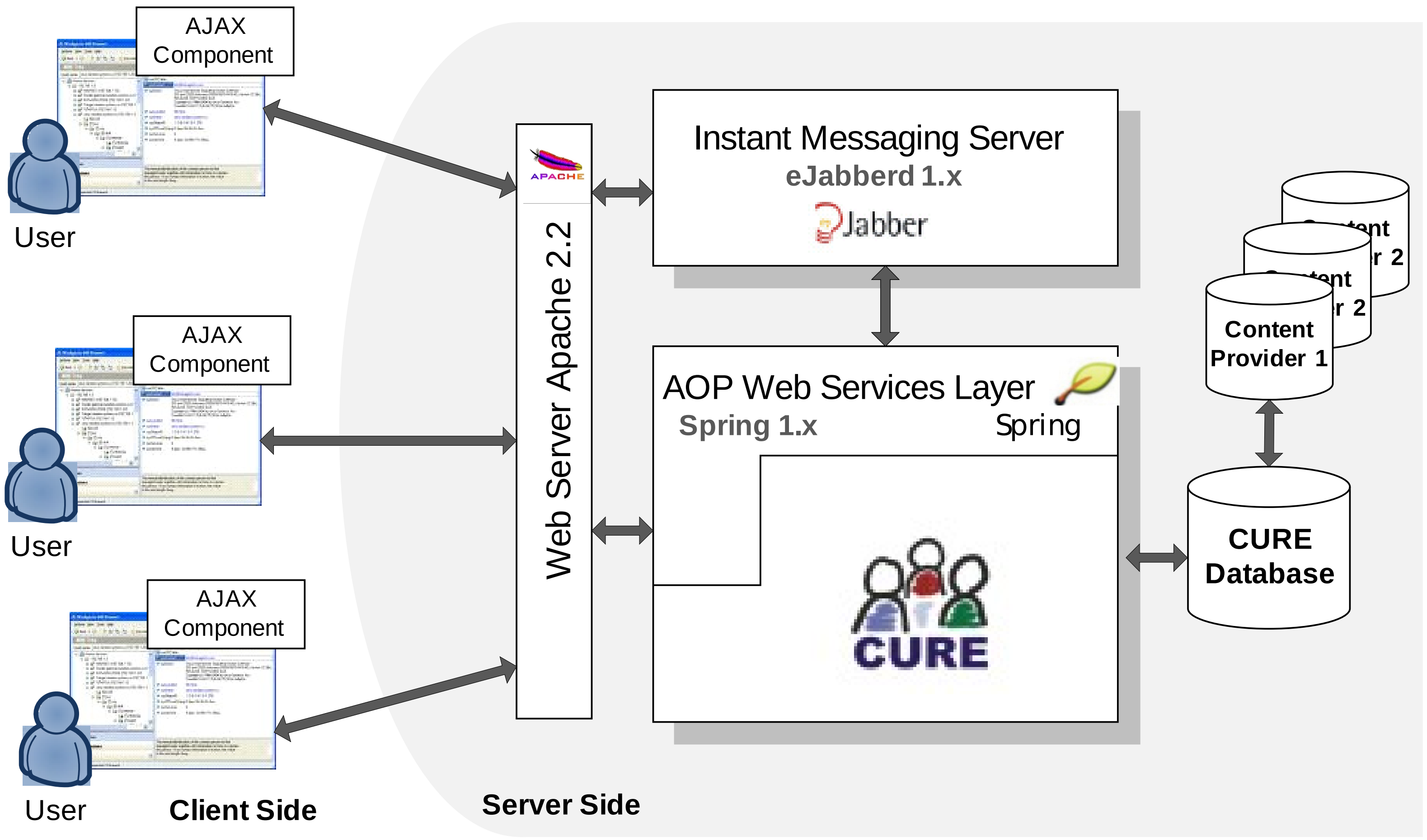
SVM’09 - Wuhan, China

MNM TEAM
MUNICH NETWORK MANAGEMENT TEAM

Agenda

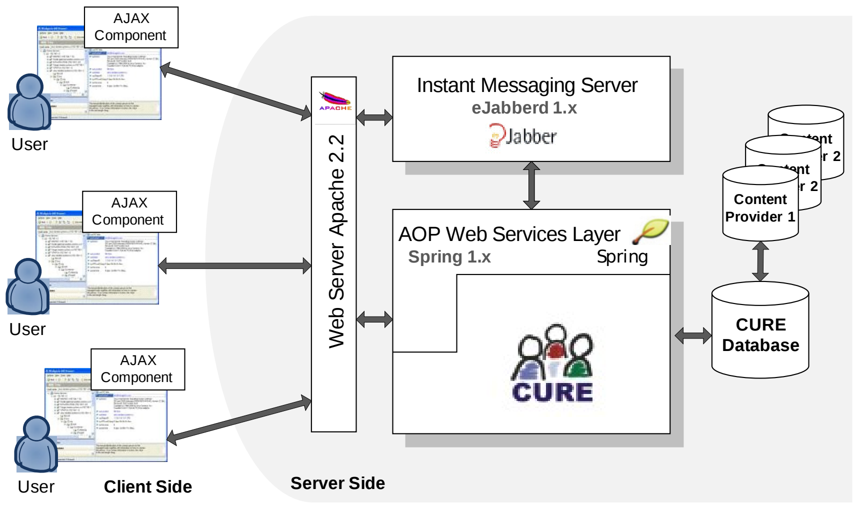
- Scenario in collaborative distance learning environments
- Problem statement
- Actual solutions and need of extensions with a Trust Management System
- Contribution of this study
- Implementation details
- Conclusion and future work

Scenario & Motivation (I)



Scenario & Motivation (II)

- The CURE System acts as a broker
- The results are accumulated from different Content Providers (CPs)
- The student may include Quality of Service (QoS) constraints on learning material



- The CURE System matches the QoS constraints with the available contents

Learning path between all intermediary providers

Problem statement

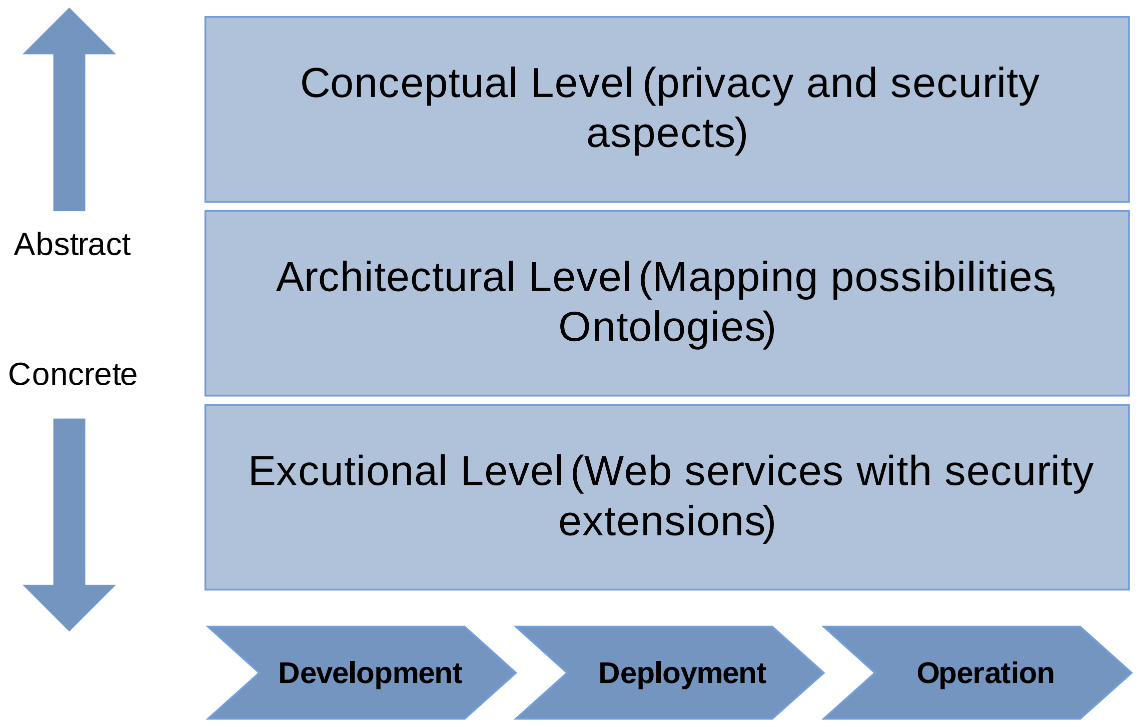
- Service-Oriented Architectures (SOA) and Web-Oriented Architectures (WOA)
- Collaboration rules within the Service Level Agreements
- The student's requirements have not been fulfilled as advertised
- Violation in the Content Provider's (CP) collaboration rules
- Involvement of third-parties

Extend centralized SOA-Based applications with a Trust Management (TM) approach:

3) Inspection of compliance with the QoS constraints

4) Manage trust among the involved parties in the learning path

Actual solutions


Conceptual Level (privacy and security aspects)
Architectural Level (Mapping possibilities, Ontologies)
Excutional Level (Web services with security extensions)
Abstract
Concrete
Development
Deployment
Operation

- Possible extension on the conceptual level of SOA applications
  - Evaluation mechanisms for the quality of the interactions
  - Reputation of the Content providers
  - Aggregation of the information

Contribution of this study

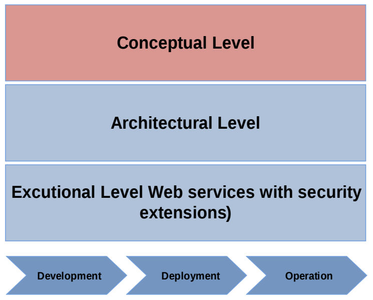
❶ Establishment of trust agreements

- Published, accessible
- Establishment according to a unified ontology

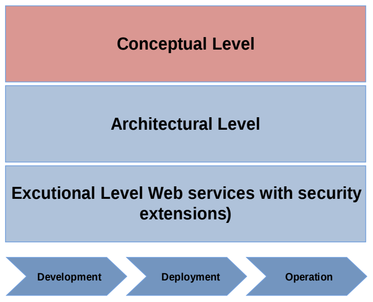
❷ Mechanisms for the assessment of trust

- Trust from past experiences
- Trust by reputation

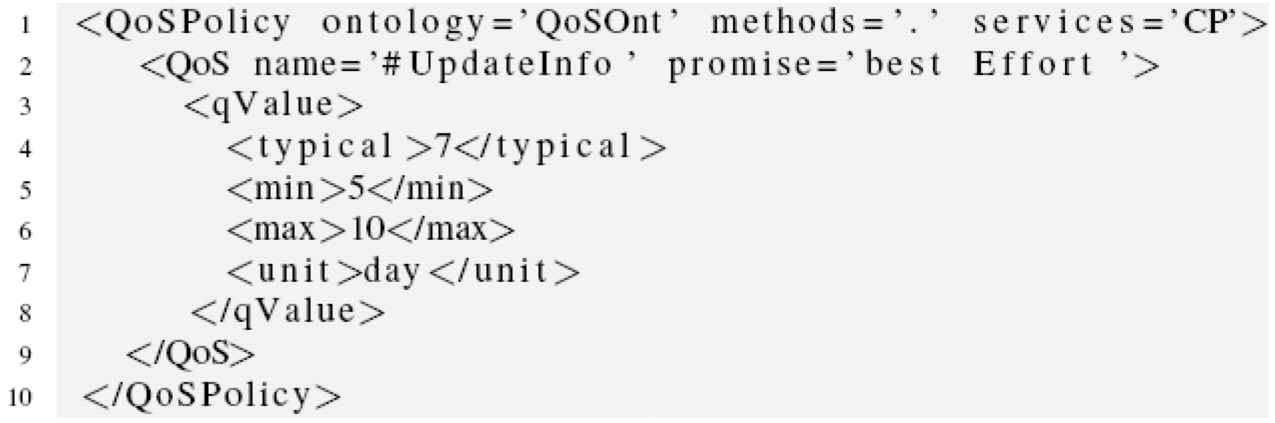
❸ Aggregating and updating the trust values



❶ Establishment of trust agreements



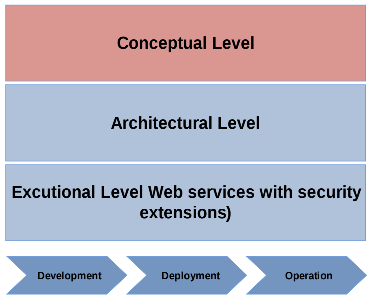
- The providers express their policies and advertised QoS parameters using a unified ontology (e.g. performance, cost of transaction, etc)
- Example about the quality parameter UpdateInfo



```
<QoSPolicy  ontology='QoSOnt'  methods='.'  services='CP'>
   <QoS  name='#UpdateInfo'  promise='best  Effort'>
      <qValue>
         <typical>7</typical>
         <min>5</min>
         <max>10</max>
         <unit>day</unit>
      </qValue>
   </QoS>
</QoSPolicy>
```

- The promised values on the element <qValue> are: min, max, and unit

❷ Assessment of trust (I)



- Reasoning about trust from past experiences requires:
  - Fine-grained and unified description of the shared resources with quality parameters
  - Unified specifications for describing the commitments with regard to the offered services and resources
- Monitoring tools to compare the log files of interactions with the agreements
- The trust level for a given quality parameter as a percentage in a point of time t_0 as follows:

$$T_\phi(t_0) = 100\% - \frac{\sum failedInteraction_\phi(t_0)}{\sum interaction_\phi(t_0)}$$

$T_\Phi \in [0,1]$ (trust scale)

Φ = (Resource, Param) refers to a distinct scenario (trust context)

❷ Assessment of trust (II)

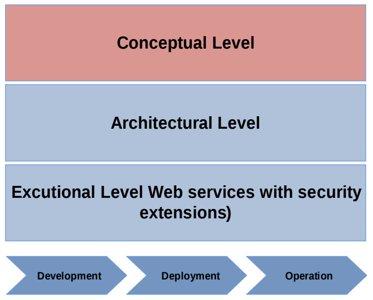
- Example: Φ = (multimediaFile, visualizationPerformance)

```
<QoSPolicy ontology='QoSOnt' methods='.' services='CP'>
   <QoS name='#visualizationPerformance' promise='best Effort'>
     <qValue>
       <typical>250</typical>
       <min>200</min>
       <max>300</max>
       <unit>dpi</unit>
     </qValue>
  </QoS>
</QoSPolicy>
```

Φ = (multimediaFile, VisualizationPerformance)

- Reasoning about trust by reputation requires:
  - Collection of recommendations from the end users
  - Reputation values according to the same trust scale $T_{\Phi} \in [0,1]$ as for trust from past experiences

❸ Aggregation of trust



- The different trust levels might be unequal
- Aggregation rules:

```
if ((∃$T_\phi^{past}$) and (∄$T_\phi^{reputation}$)) then
    $T_\phi^{final} = T_\phi^{past}$
end if
if ((∄$T_\phi^{past}$) and (∃$T_\phi^{reputation}$)) then
    $T_\phi^{final} = T_\phi^{reputation}$
end if
if ((∃$T_\phi^{past}$) and (∃$T_\phi^{reputation}$)) then
    $T_\phi^{final} = \text{aggregate}(T_\phi^{past}, T_\phi^{reputation})$
end if
```

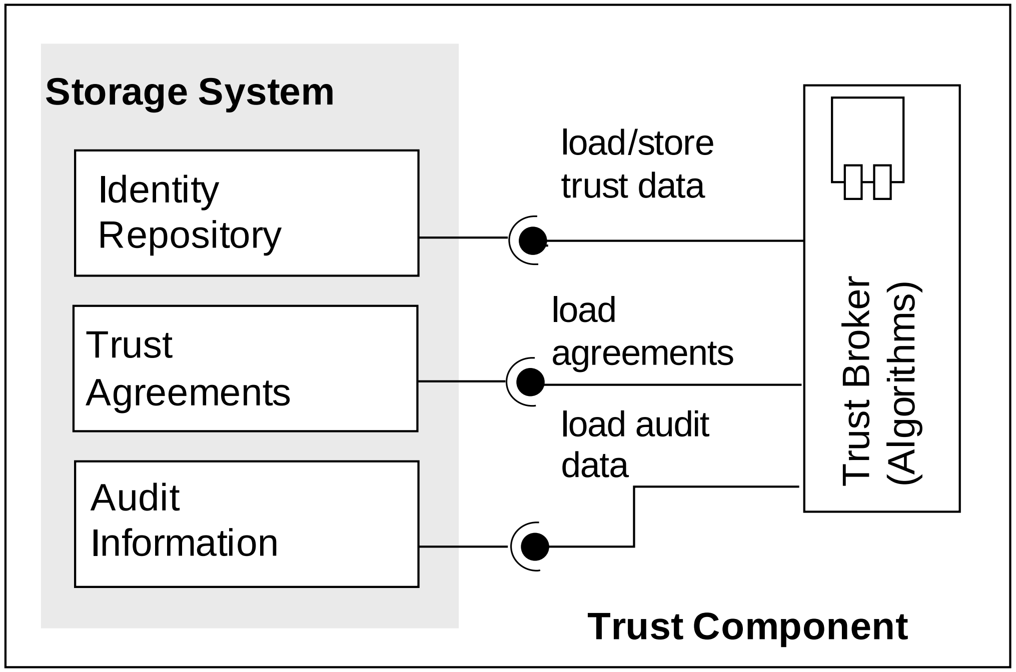
- The function *aggregate()* is based on an update function ($T_\Phi(t) = T_\Phi(t-1) \pm \Delta T_\Phi$)
- For incrementing T, ΔT_Φ is computed as $\left(1 - \frac{1}{2} e^{-\alpha(\sum interaction(\chi))}\right)$

Architectural level – Implementation

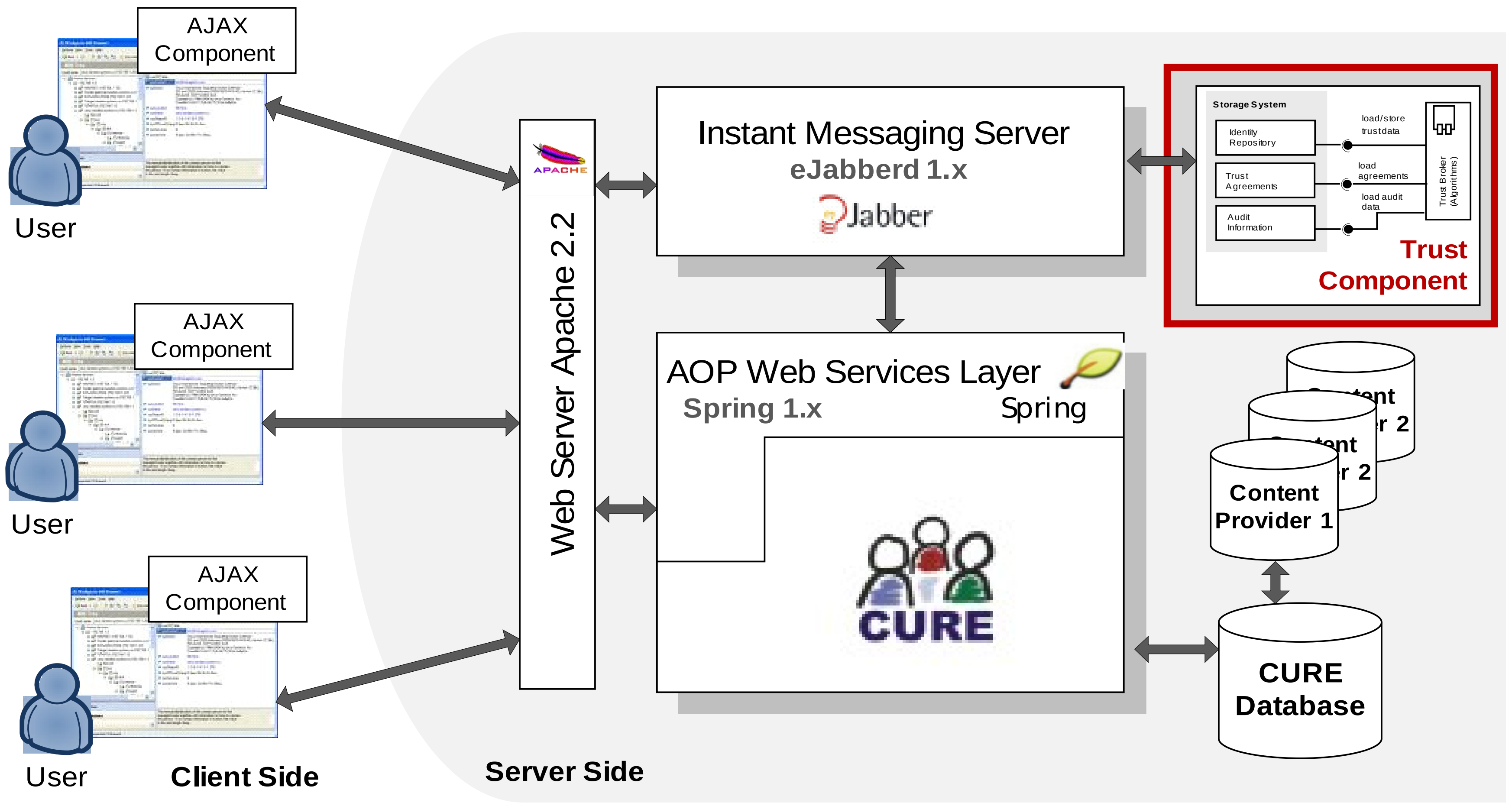
- Trust Component is composed of 4 sub-components:

  (1) Trust Broker (2) Storage System

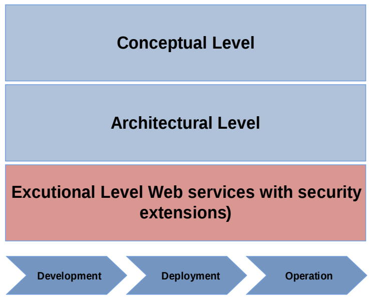
  (3) Identity Repository (4) Auditing Engine



Integration of the trust component



Policy and access control on the executional level



- Extending the existing authorization policies and access control decisions with the trust level
- Realization within an Access Decision Engine (ADE)
- Attribution of trust levels to the content provider's advertised quality parameters
- Use of the trust levels as conditions thresholds

Conclusion and future work

- Summary
  - Complement the static aspects of SOA-Based applications
  - Establishment of trust agreements with unified ontologies
  - Dynamic trust assessment from past experiences and by reputation
  - Aggregation of trust from more than on dimension
- Open issues and future work
  - Investigation of more generic QoS and trust agreements ontologies
  - Identification and the aggregation of further trust information dimensions
  - Risks involved: Evaluation of the Quality of Trust (QoT) and reputation feedbacks
- Areas of application: Virtual Universities (Virtual University of Bavaria) for web-based learning systems – Fern-Universität Hagen

Thank you for your attention !

Latifa Boursas

MNM TEAM

Munich Network Management Team

Requirements

- Trust information; reporting on other participants' experiences requires archiving of information on previous interactions
- Trust Level; it needs to be quantified and must reflect various degrees of trust
- Trust scale; a definition of an expressive scale for encoding the derived trust information into distinct values is required
- Trust context; the trust level according to the given trust scale may indicate the trustworthiness of the CP for a given context
- Trust agreements; the appraisal of the trust information needs to be based on collaboration agreements among the partners