

# Controle de acesso e *privacy*

Antonio Carlos Salzvedel Furtado Junior, Roger Roberto Rocha  
Duarte, Tiago Rodrigo Kepe

Universidade Federal do Paraná - UFPR

5 de junho de 2011

# Sumário I

- 1 Introdução
- 2 Trabalhos relacionados
- 3 Propostas
  - Controle de acesso local dos participantes
    - Política de mapeamento
    - Diretório distribuído
  - P-Hera
- 4 Conclusão
- 5 Perguntas

# Motivação

- Aplicações colaborativas
- Grids Computacionais
- Redes de Distribuição de conteúdo (CDNs)

# Problemas

- Peers são igualmente confiáveis
- Quem é dono dos dados?

- Uso de supernodos apra guardar restrições
- Criptografia e distribuição de chaves

Limitação

Escalabilidade

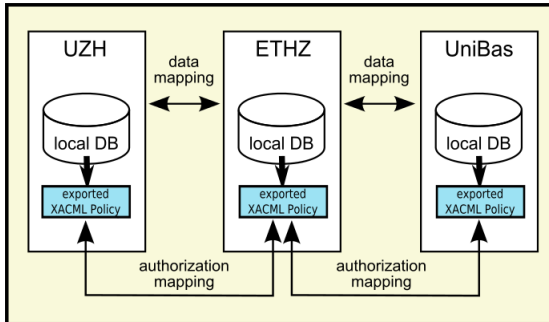
# Contexto

- Peers são estáveis
- Replicação não é considerada
- Controle de acesso local dos dados e estruturação
- Autoridade de certificação centralizada

# Componentes

## Níveis de funcionamento

- Nível de peer
- Baseado no usuário



```

<Rule RuleId="export:ethz" Effect="Permit">
  <!--
  <Grantor>
    <Subject>
      <SubjectMatch MatchId="&function;rfc822Name-equal">
        <AttributeValue
          DataType="&datatype;rfc822Name">admin@ethz
        </AttributeValue>
        <SubjectAttributeDesignator
          AttributeId="&subject;subject-id"
          DataType="&datatype;rfc822Name" />
        </SubjectMatch>
      </Subject>
    </Grantor>
    <RuleGrantOption DataType="&xml:string">yes</RuleGrantOption>
    <Timestamp></Timestamp>
  -->
  <Subject>
    <SubjectMatch MatchId="&function;rfc822Name-equal">
      <AttributeValue DataType="&datatype;rfc822Name">hans@ethz</AttributeValue>
      <!-- ... -->
    </SubjectMatch>
  </Subject>
  <Resource>
    <ResourceMatch MatchId="&function;anyURI-equal">
      <AttributeValue DataType="&xml:anyURI">ethz.object1</AttributeValue>
      <!-- ... -->
    </ResourceMatch>
  </Resource>
  <Action>
    <ActionMatch MatchId="&function;string-equal">
      <AttributeValue DataType="&xml:string">read</AttributeValue>
      <!-- ... -->
    </ActionMatch>
  </Action>
</Rule>

```



# Política de mapeamento

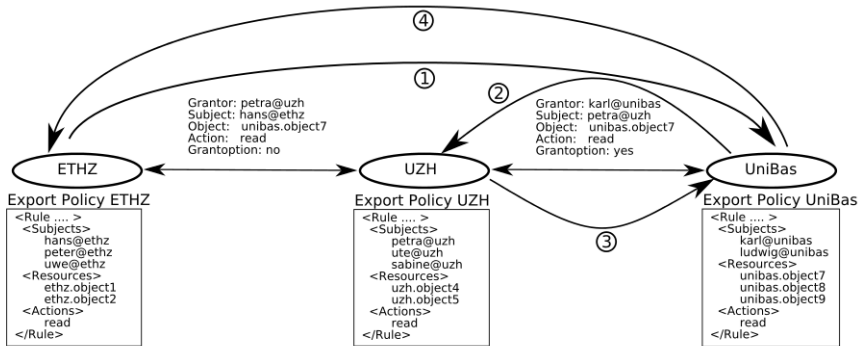
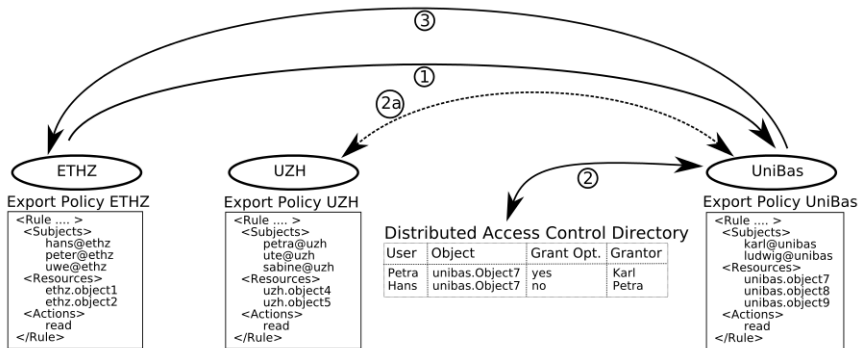


Figura: hanz@ethz requisita unibas.object7

# Diretório distribuído



# Diretório distribuído - Implementação

- Usa-se a DHT
- Chord
  - *Overhead* para manutenção do diretório

# Proteção do diretório e conteúdo distribuído

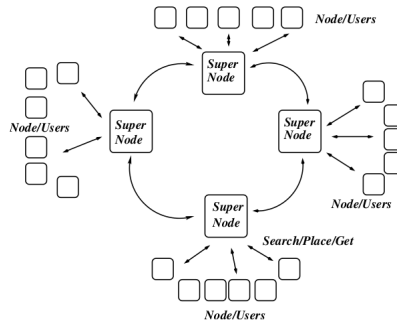
- Cada entrada possui uma assinatura
- Criptografia das entradas do diretório
  - Cada objeto corresponde a uma chave pública
  - Chaves privadas são distribuídas
- Somente o concessor pode alterar suas entradas
- Detecção de peers maliciosos

# Considerações

- Mapeamento
  - Tende a criar muitas regras
  - Mais controle
- Diretório distribuído
  - Política de remoção de entradas do diretório

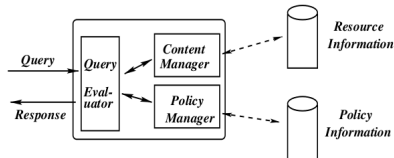
# Contexto

- Rede não-estruturada hierárquica
- Primitivas: *search*, *get* e *place*.



# Políticas

- Em XACML
- Tipos:
  - Política de replicação
  - Política de armazenamento
  - Controle de acesso

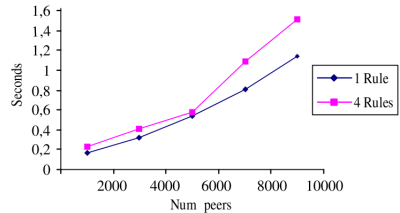
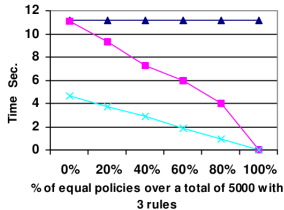


# Gerenciamento de políticas

- Armazenamento no supernodo
- Organização
  - Sem grupamento
  - Agrupados por políticas
  - Agrupados por expressões em políticas:  $\langle attr_i, expr_i \rangle$



# Testes



# Considerações

- Preza escalabilidade
- Confiança em supernodos

# Conclusão

- Propostas para contextos específicos
- Tráfego extra para estabelecimento de regras
- Estabelecimento de confiança entre peers

## Perguntas

# PERGUNTAS?