Controle de acesso e *privacy*

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

Universidade Federal do Paraná - UFPR

6 de junho de 2011

Sumário I

1. Introdução
   - XACML
2. Propostas
   - Controle de acesso local dos participantes
     - Mapeamento
     - Diretório distribuído
   - P-Hera
3. Conclusão
4. Perguntas

Motivação

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

Problemas

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

- Padrão para controle de acesso
- Alvos e regras

Exemplo de alvo

```
<Policy PolicyId="SamplePolicy"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer</AttributeValue>
        <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                                     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" />
      </ResourceMatch>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>

    <!-- ... -->
</Policy>
```

Exemplo de regra

```
<Policy PolicyId="SamplePolicy"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">

    <!-- ... -->

  <Rule RuleId="LoginRule" Effect="Permit">
    <Target>
      <Subjects>
        <AnySubject/>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">login</AttributeValue>
          <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                                     AttributeId="ServerAction"/>
        </ActionMatch>
      </Actions>
    </Target>
    <Condition FunctionId="␣function#time-in-range">
        <Apply FunctionId="␣function:time-one-and-only">
          <EnvironmentAttributeDesignator AttributeId="current␣-time" DataType="#time" />
        </Apply>
        <AttributeValue DataType="␣#time">08:00:00</AttributeValue>
        <AttributeValue DataType="␣#time">20:00:00</AttributeValue>
    </Condition>
  </Rule>
  <Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```

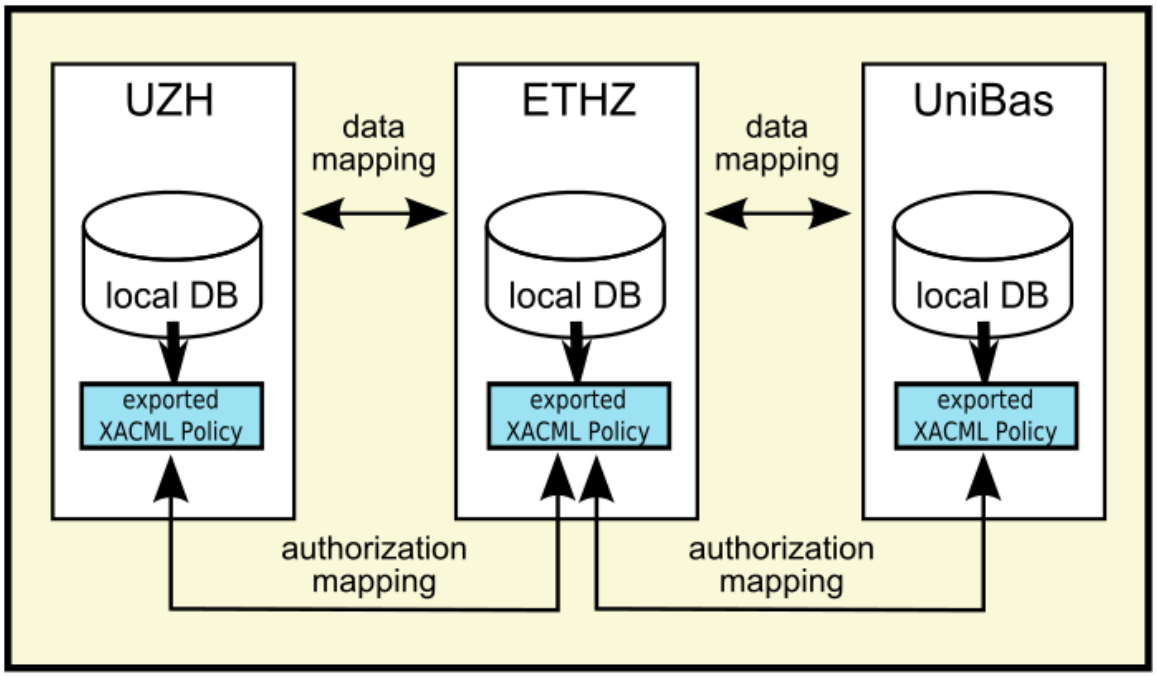
Contexto

- 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



Adaptação do XACML

```
<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>
                  <!-- ... -->
    </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>
```

Mapeamento

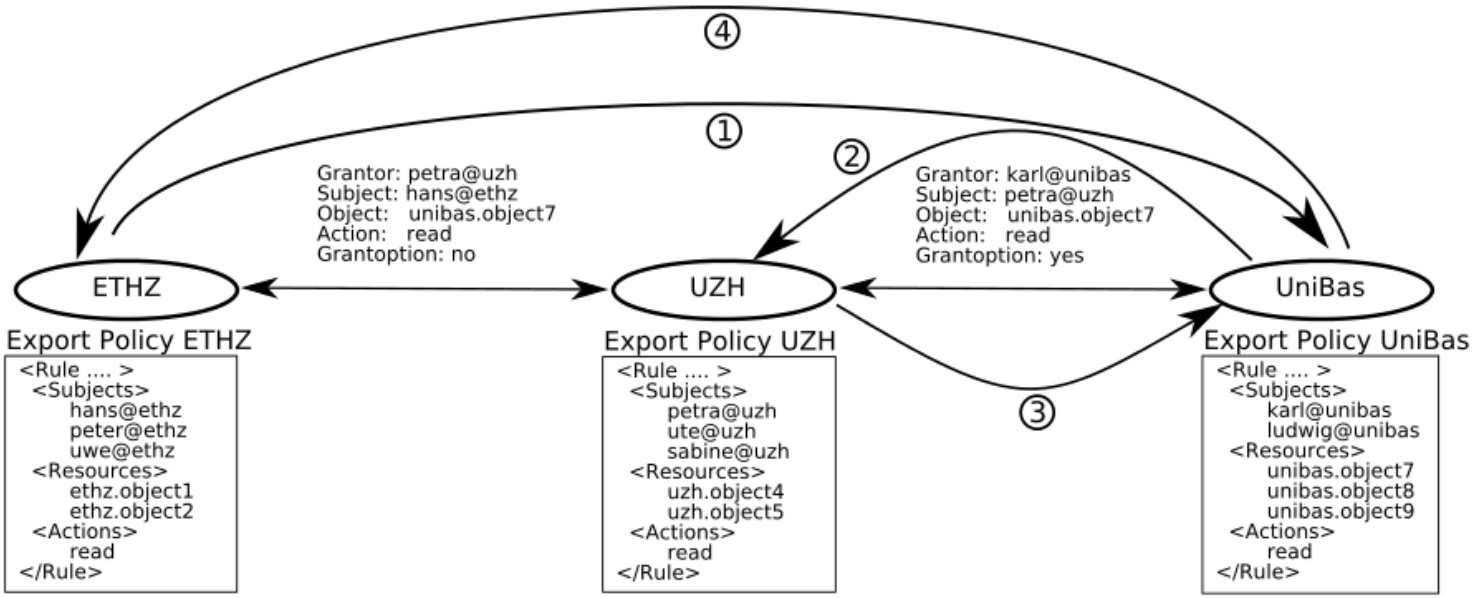
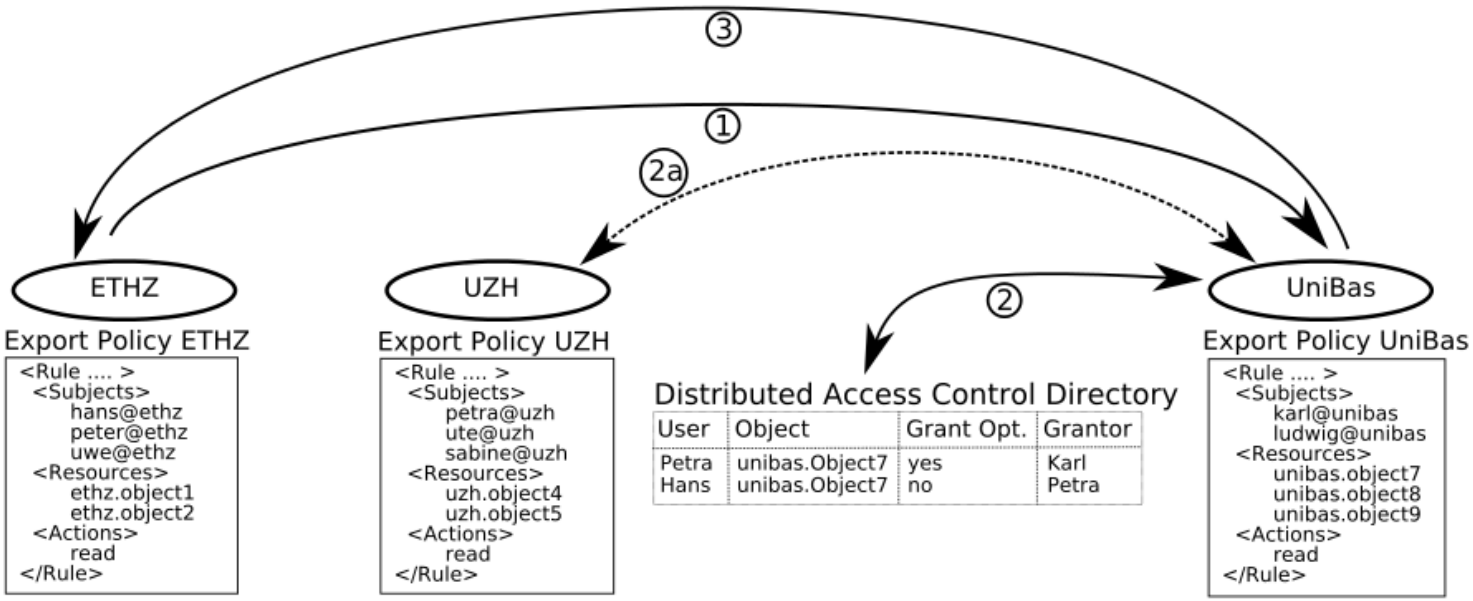


Figura: hanz@ethz requisita unibas.object7

Diretório distribuído



Diretório distribuído - Implementação

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

Proteção do diretório e conteúdo distribuído

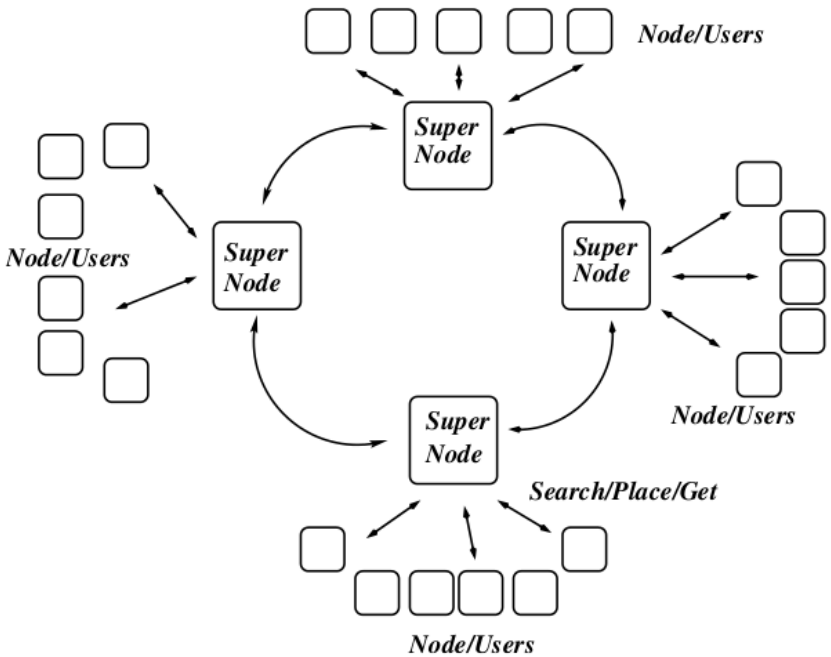
- Cada entrada possui uma assinatura
- Criptografia das entradas do diretório
  - Cada objeto corresponde a uma chave pública
  - Chaves privadas são distribuídas
  - Usa unidade certificadora centralizada
- Somente o concessor pode alterar suas entradas
- Detecção de peers maliciosos

Considerações

- Na Alteração de algum previlégio, pode ocorrer o efeito de cascata
- Não tem replicação
- Mapeamento
  - Tende a criar muitas regras
  - Mais controle
- Diretório distribuído
  - Política de remoção de entradas do diretório
  - Sobrecarga da unidade certificadora

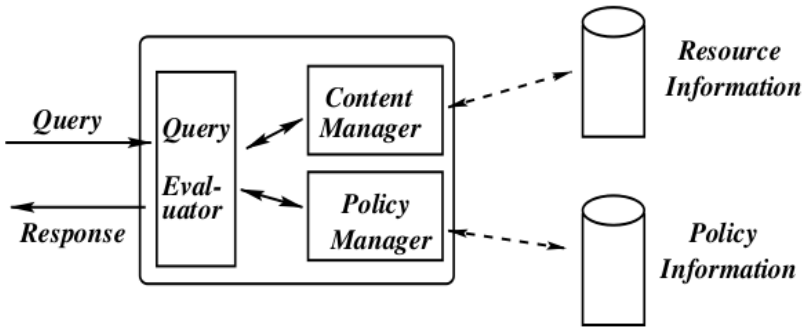
Contexto

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



Políticas

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



Gerenciamento de políticas

- Armazenamento no supernodo
- Organização
  - Sem agrupamento
  - Agrupados por políticas
  - Agrupados por expressões em políticas: $< attr_i, expr_i >$

Testes

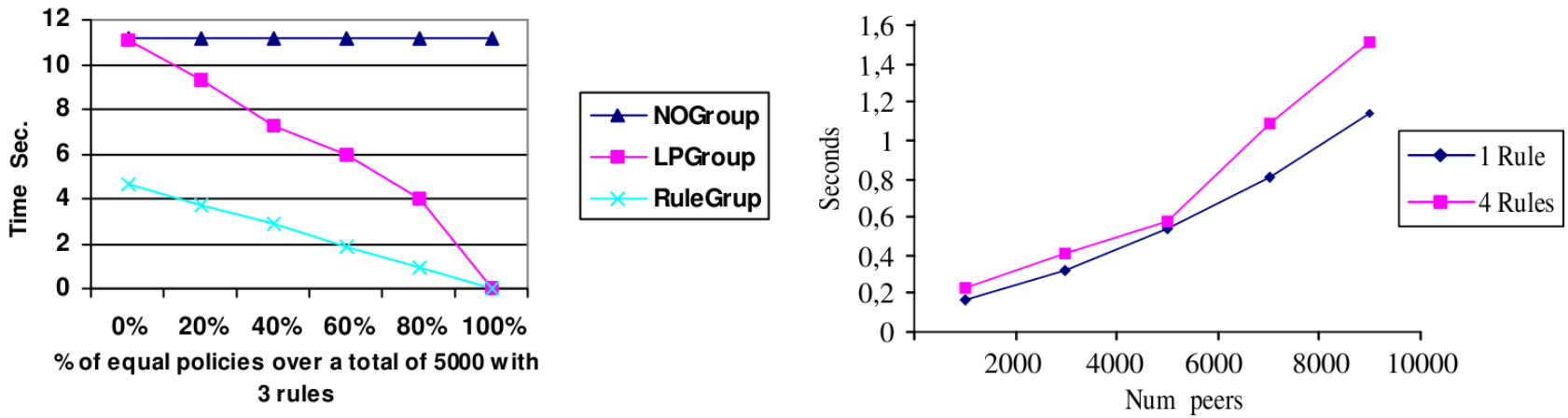


Figura: Avaliação de 5000 políticas

Considerações

- Preza escalabilidade
- Confiança em supernodos

Conclusão

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

Perguntas

PERGUNTAS?