Autorização após autenticação

Controle de acesso baseado em papéis e certificados de atributos X.509 para proteção de recursos

sneusatz@ime.usp.br

Objetivos

- Expor o modelo de controle de acesso baseado em papéis – RBAC
- Expor as infra-estruturas de chave pública (PKI) e de gerenciamento de privilégios (PMI)
- Mostrar dois projetos que fornecem arcabouços de segurança baseados em RBAC e na PMI

sneusatz@ime.usp.br

Requisitos para proteção de recursos

- Identificação – todo usuário deve ser mapeado para um identificador conhecido.
- Autenticação – o usuário deve fornecer credenciais para comprovar sua identidade.
- Autorização – o acesso aos recursos deve ser limitado aos usuários com privilégios para isso.
- Proteção dos dados – uso de criptografia para garantir a confidencialidade dos dados.

sneusatz@ime.usp.br

Role-Based Access Control

- Apareceu no inicio dos anos 90 como uma alternativa as listas de controle de acesso.
- Atribui as informações de autorização aos papéis que os usuários podem assumir.
- Reduz consideravelmente o trabalho de administração de privilégios.
- Especifica quatro modelos de controle de acesso.

sneusatz@ime.usp.br

$RBAC_0$ – O modelo simples

- Nesse modelo, o administrador define os papéis que os usuários podem desempenhar.
- A cada papel é atribuído um conjunto de privilégios que representam as ações que cada papel pode executar sobre os recursos.
- Ao acessar um recurso, os papéis do usuários são usados para decidir se o acesso deve ou não ser permitido.

sneusatz@ime.usp.br

$RBAC_1$ – modelo hierárquico.

- Extensão do modelo simples para facilitar ainda mais o gerenciamento de permissões.
- Permite que um papel estenda outros papéis herdando seu conjunto de permissões.
- Exemplo: programador ← gerente

  gerente define sua permissões próprias além de herdar todas as permissões de programador.

sneusatz@ime.usp.br

$RBAC_2$ – modelo restrito

- Outra extensão do modelo simples, mas não do modelo hierárquico.
- Nele pode-se definir restrições para os papéis e permissões alocadas.
- Exemplo: papéis A e B são mutuamente exclusivos, indicando que uma mesma pessoa não pode desempenhar os dois papéis ao mesmo tempo.

sneusatz@ime.usp.br

$RBAC_3$ – modelo consolidado

- Extensão que reúne as características dos modelos $RBAC_1$ e $RBAC_2$.
- Permite assim o uso de hierarquia de papéis conforme o $RBAC_1$ e também o uso de restrições conforme o $RBAC_2$.

sneusatz@ime.usp.br

A infra-estrutura de chave pública ou PKI

- O comitê X9 da ANSI definiu em um primeiro momento a infra-estrutura de chave pública ou PKI para prover um mecanismo forte de autenticação.
- A PKI tem como base os certificados de chave pública X.509 (PKCs), que associam a identidade de um usuário a uma chave pública e são digitalmente assinados por entidades conhecidas como Certification Authorities ou CAs.
- Os usuários podem comprovar a sua identidade apresentando seu PKC ao sistema de autenticação.

sneusatz@ime.usp.br

Surgimento da PMI

- Na prática o uso da PKI revelou a necessidade de armazenar outros dados além da chave pública em um PKC.
- Versões mais recentes do X.509 PKI definem uma série de campos - extensões - adicionais para armazenar essas informações.
- Pessoas começaram a usar esses campos para armazenar os privilégios dos usuários.

sneusatz@ime.usp.br

Surgimento da PMI

- Problemas com uso de extensões do PKC:
  - Informações de controle de acesso em geral tem tempo de vida mais curto que a chave pública.
  - Revogação de qualquer atributo contendo permissões implica na revogação do certificado inteiro.
  - Tipicamente a entidade que emite um certificado de chave pública não tem autoridade para estabelecer as permissões de um usuário.

sneusatz@ime.usp.br

Surgimento da PMI

- Para tratar esses problemas o comitê X9 definiu a infra-estrutura de gerenciamento de privilégios ou PMI, cujo elemento central é o certificado de atributos X.509.
- Esses certificados associam atributos ao seu portador, que tipicamente contém privilégios.
- São emitidos e assinados digitalmente por entidades chamadas Attribute Authorities ou AA.

sneusatz@ime.usp.br

PMI – Vantagens

- Vantagens do uso dos X.509 ACs:
  - Estabelecem uma separação clara entre os processos de autenticação e autorização.
  - Favorece o gerenciamento distribuído de privilégios.
  - Evita delegação de responsabilidades para as Certification Authorities.
  - Separa o tempo de vida dos atributos do tempo de vida da chave pública.

sneusatz@ime.usp.br

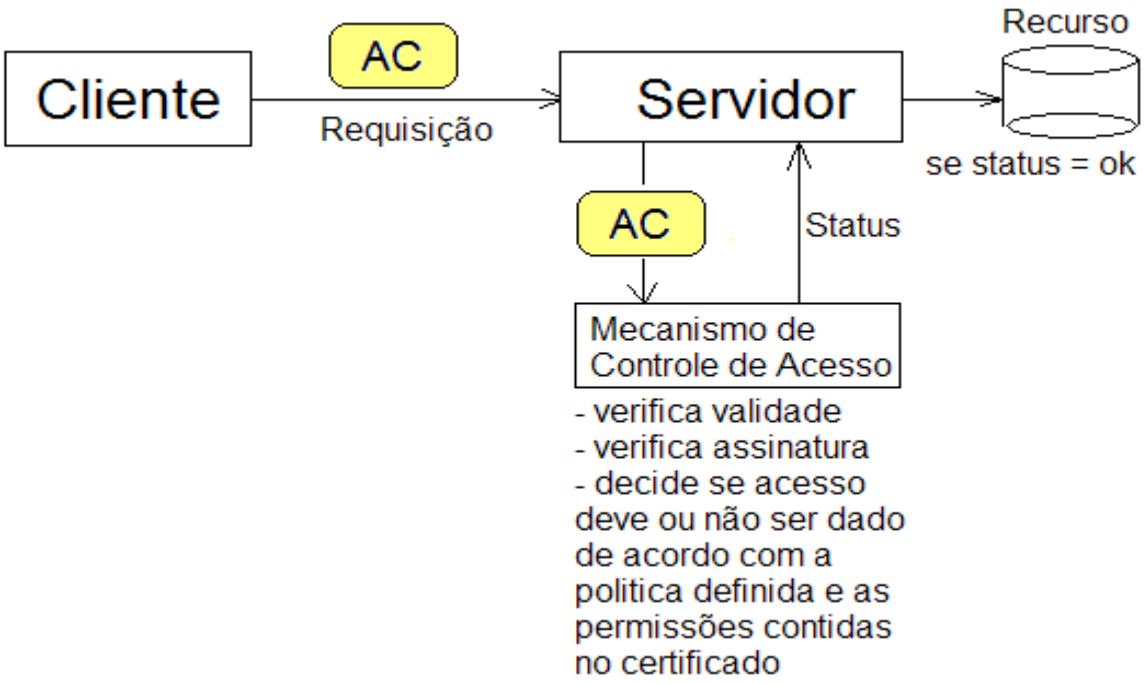
PMI e RBAC

- RBAC é suportado pela X.509 PMI através dos certificados de atributos.
- Para isso, define-se um ou mais ACs que contenham as permissões de cada papel como atributo (ex: gerente de RH pode alterar beneficios) e um outro conjunto de ACs associe os papéis ao seu portador (ex: João tem os papéis de Gerente e Diretor).

sneusatz@ime.usp.br

Propagação de credenciais

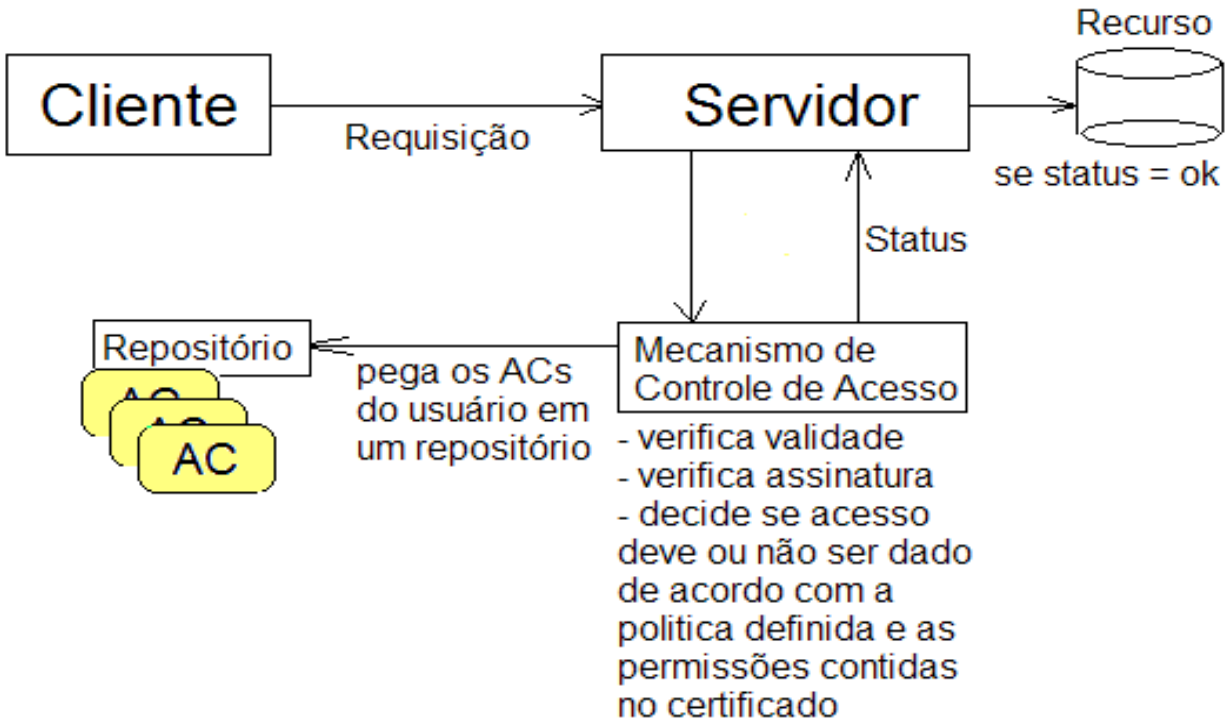
- Modelo Push



sneusatz@ime.usp.br

Propagação de credenciais

- Modelo Pull



sneusatz@ime.usp.br

Pull x Push

- O fator que mais pesa contra o modelo push são as listas de revogação. Para verificar se o certificado foi ou não revogado o serviço de autorização deve consultar a entidade emissora.
- O modelo pull não precisa se preocupar com revogação já que os certificados são gerenciados no próprio ambiente do servidor.
- Modelo pull pode apresentar pior desempenho no caso de repositórios distribuídos.

sneusatz@ime.usp.br

Akenti

- Motivação: permitir o gerenciamento distribuído de políticas de acesso a recursos.
- Cada participante deve poder definir as condições de acesso a um recurso de forma independente.
- O mecanismo de controle de acesso usa apenas o mínimo necessário de informações centralizadas.

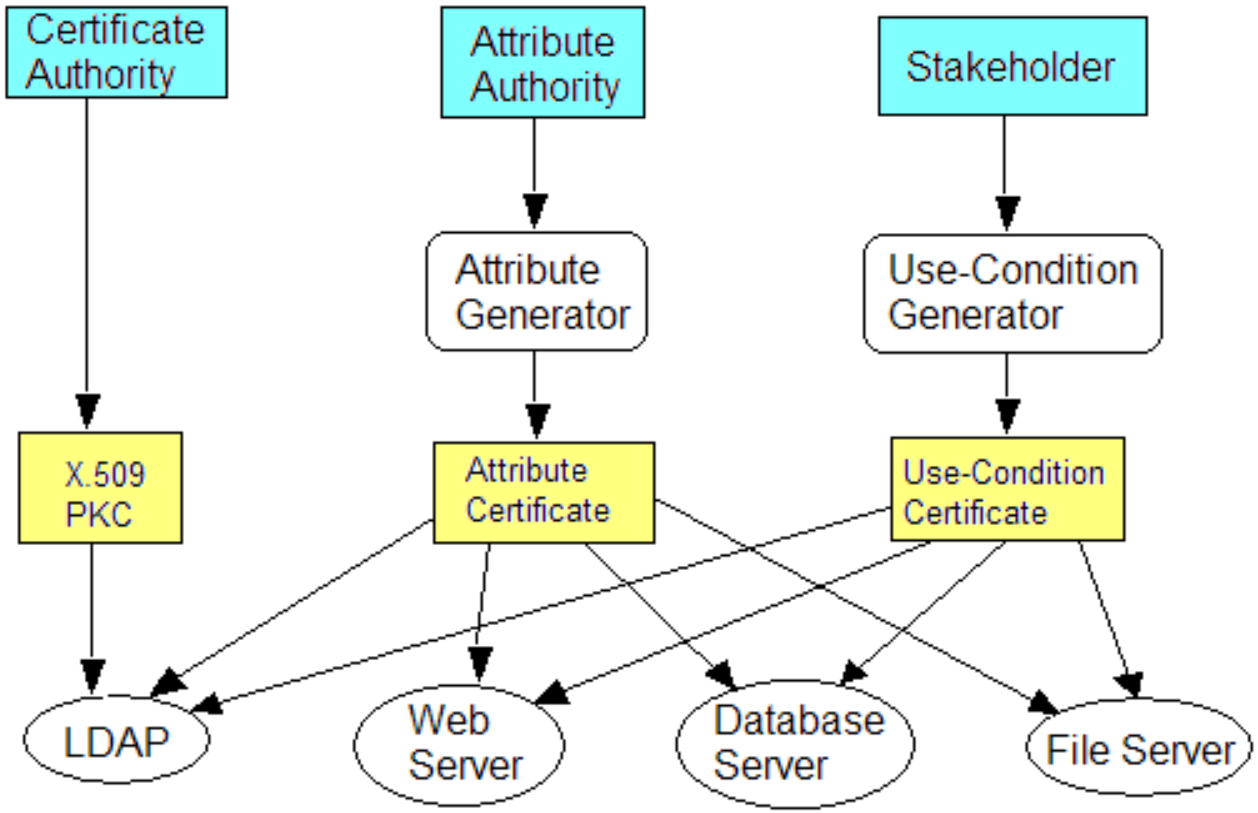
sneusatz@ime.usp.br

Akenti - Abordagem

- A abordagem baseada em certificados digitais para promover identificação e autorização.
- Usuários são autenticados usando o certificado de chave pública X.509.
- Participantes criam e assim certificados de condição de uso contendo a política de acesso ao recurso.
- Atributos como papéis dos usuários são assinados por autoridades através de certificados de atributos.

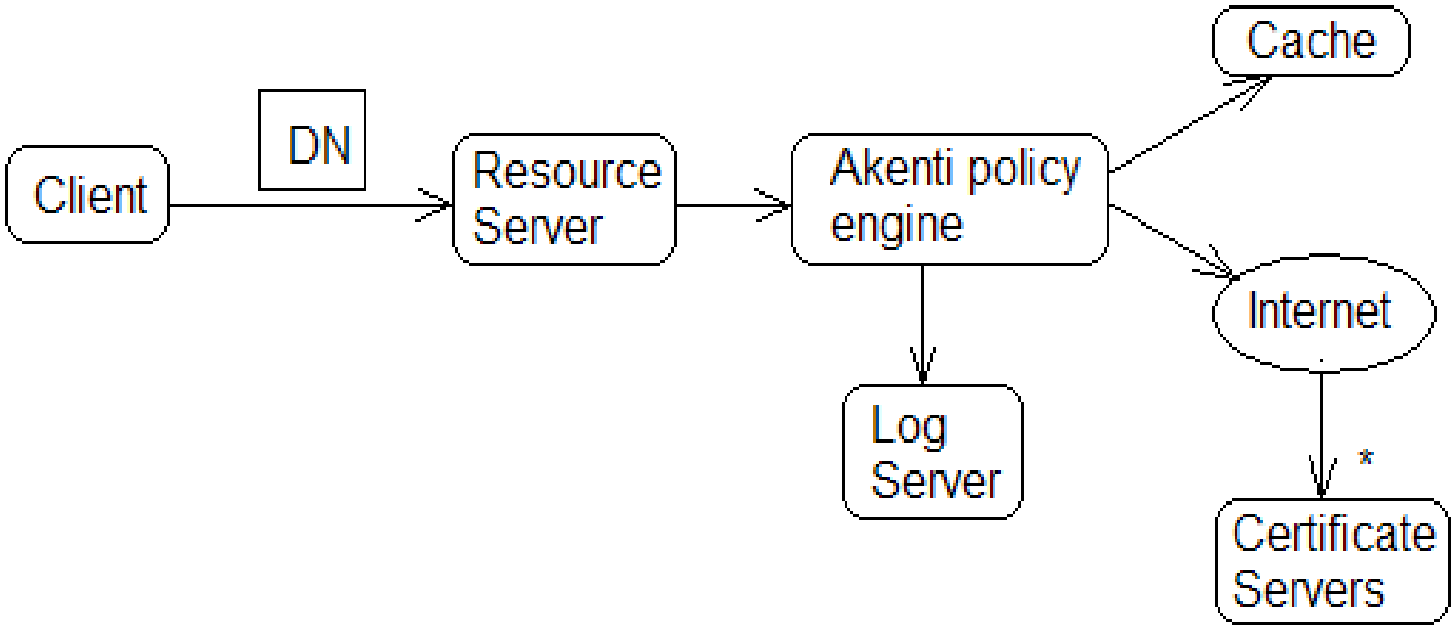
sneusatz@ime.usp.br

Akenti – Geração dos certificados



sneusatz@ime.usp.br

Akenti – Arquitetura



sneusatz@ime.usp.br

Akenti Policy Certificate

```
<AkentiCertificate>
  <SignablePart>
     <Header type="Policy" SignatureDigestAlg="RSA-MD5" CanonAlg="AkentiV1">
     (...)
     </Header>
   <PolicyCert>
    <ResourceName>ResName</ResourceName>
    <CAInfo>
        <CADN>/C=US/O=Lawrence Berkeley National Laboratory/OU==ICSD/CN=IDCG-C</CADN>
        <X509Certificate>
           -----BEGIN CERTIFICATE-----
                 pem encoded X509 certificate of CA
           -----END CERTIFICATE-----
       </X509Certificate>
      <IdDirs>
       <URL> ldap://idcg-ca.lbl.gov/</URL>
      </IdDirs>
      <CRLDirs>
       <URL> ldap://idcg-ca.lbl.gov/</URL>
      </CRLDirs>
    </CAInfo>
    <UseCondIssuerGroup>
       <Principal>
          <UserDN>/C=US/O=LBNL/OU=ICSD/CN=Mary R. Thompson</UserDN>
          <CADN> /C=US/O=LBNL/OU=ICSD/CN=IDCG-CA</CADN>
       </Principal>
       <URL> http://www-itg.lbl.gov/~mrt/Certificates/</URL>
    <UseCondIssuerGroup>
    <AttrDirs>
        <URL>file:/usr/mrt/Attributes</URL>
        <URL> http://idcg-ds.lbl.gov/~kjackson/Certificates/</URL>
    </AttrDirs>
    <CacheTime>1800</CacheTime>
  </PolicyCert>
  </SignablePart>
</AkentiCertificate>
```

Akenti Use-Condition Certificate

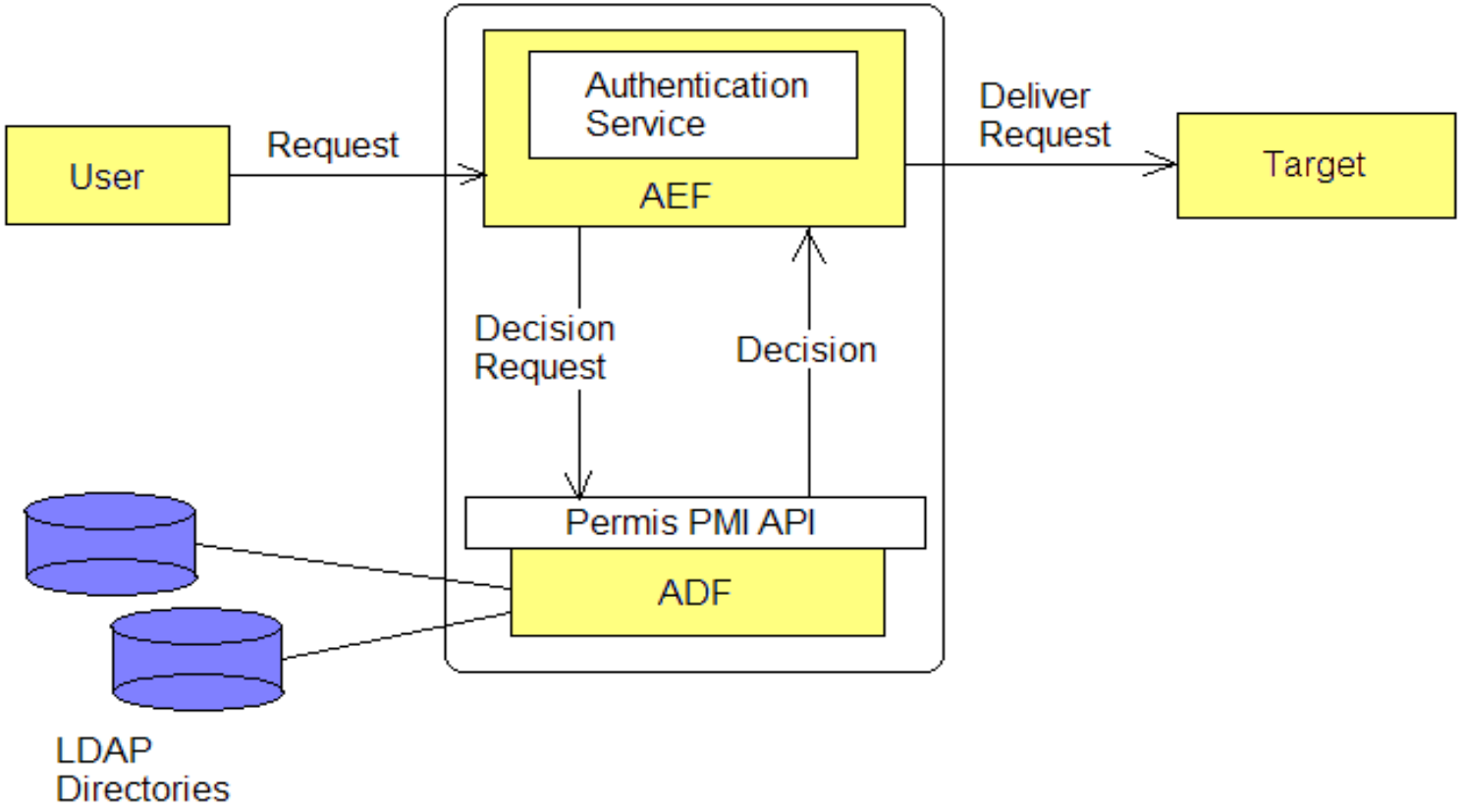
```
<AkentiCertificate>
  <SignablePart>
    <Header type="UseCondition" SignatureDigestAlg="RSA-MD5" CanonAlg="AkentiV1">
        (...)
   </Header>
   < UseConditionCert scope="sub-tree" enable="false">
     <ResourceName>DieselCollab/PREServer/chad </ResourceName>
     <Condition>
       <Constraint>(( cn = Diane Gomes ) | ( cn = Mary R. Thompson ))</Constraint>
       <AttributeInfo type="X509">
          <AttrName>cn</AttrName>
          <AttrValue>Diane Gomes</AttrValue>
          <CADN>/C=US/O=Diesel Combustion Collaboratory/OU=SNL/CN=DieselCert.ca.sandia.gov </CADN>
       </AttributeInfo>
       <AttributeInfo type="X509">
          <AttrName>cn</AttrName>
          <AttrValue>Mary R. Thompson</AttrValue>
          <CADN>/C=US/O=LBNL/OU=ICSD/CN=IDCG-CA</CADN>
       </AttributeInfo>
    </Condition>
    <Rights>read,execute </Rights>
  </UseConditionCert>
  </SignablePart>
</AkentiCertificate>
```

PERMIS – PrivilEdge Role Management Infraestructure Standards

- Infra-estrutura de autorização desenvolvida na universidade de Salford, UK.
- Implementa uma PMI usando RBAC e certificados de atributos X.509.
- Utiliza XML como linguagem de definição da política de controle de acesso.
- Implementa $RBAC_1$ e parcialmente $RBAC_2$.

sneusatz@ime.usp.br

PERMIS - Arquitetura



sneusatz@ime.usp.br

PERMIS – Componentes Principais

- PA – Privilege Allocator: gera e assina os certificados contendo os papéis de cada usuário além de gerar e assinar o certificado contendo a política de controle de acesso.
- AEF – Access-Control Enforcement Function: Fornece a autenticação de forma dependente de aplicação e invoca a ADF para decisão quanto ao acesso ao recurso.
- ADF – Access-Control Decision Function: Decide se o acesso ao recurso deve ou não ser permitido baseado na política definida e nos papéis do usuário.
- Permis PMI API: Fornece a API pela qual a AEF invoca a ADF.

sneusatz@ime.usp.br

PERMIS – Políticas de Autorização

- Especificada em XML segundo um DTD publicado em www.xml.org. Dividida em:
- SubjectPolicy – especifica os domínios cobertos pela política.
- RoleHierarchyPolicy – especifica os papéis e seus relacionamentos.
- SOAPolicy – especifica quais AA's são confiáveis como emissoras de certificados.

sneusatz@ime.usp.br

Políticas - continuação

- RoleAssignmentPolicy – especifica quais AAs podem alocar papéis para quais usuários.
- TargetPolicy – especifica os recursos (alvos) cobertos por esta política.
- ActionPolicy – especifica as ações suportadas pelos recursos.
- TargetAccessPolicy – especifica quais papéis podem executar quais ações no alvo.

sneusatz@ime.usp.br

XACML

- eXtensible Access Control Markup Language, criada a mantida pelo consórcio OASIS.
- Define uma série de perfis para o uso da XACML como forma de definição de políticas de controle de acesso.
- Um dos perfis, o *Core and Hierarchical Role Based Access Control (RBAC) profile* fornece uma especificação para utilizar a XACML juntamente com RBAC básico e hierárquico.
- Surgiu depois do DTD definido pelo PERMIS, mas ambos contém muitas semelhanças.

sneusatz@ime.usp.br

Conclusão

- Uma grande parte dos sistemas que foram desenvolvidos nos últimos anos utiliza algum modelo de RBAC para suportar controle de acesso. Esse mecanismo está presente desde frameworks específicas de segurança até servidores de aplicação, o que comprova o seu fortalecimento e amadurecimento como meio de fornecer controle de acesso a recursos computacionais.

sneusatz@ime.usp.br

Referências

- RBAC:
  - R. S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, “Role-Based Access Control Models”, *IEEE Computer* 29(2): 38-47, IEEE Press, 1996 – disponível em http://csrc.nist.gov/rbac/
- Akenti:
  - Documentação disponível em http://dsd.lbl.gov/Akenti/
- PERMIS:
  - D.W. Chadwick, A. Otenko, “Implementing Role Based Access Controls Using X.509 Attribute Certificates – the PERMIS Privilege Management Infrastructure”.
  - D.W. Chadwick, A. Otenko, “RBAC POLICIES IN XML FOR X.509 BASED PRIVILEGE MANAGEMENT”
  - Documentação disponível em http://sec.isi.salford.ac.uk/permis/private/wip.html
- XACML:
  - Documentação disponível em http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

sneusatz@ime.usp.br