Controle de Acesso e Certificados de Atributo

Prezi

Controle de Acesso e Certificados de Atributo

Controle de Acesso

- Sistemas web necessitam de segurança.
- E para segurança, Controle de Acesso é imprescindível.
- Envolve determinar quais recursos estão disponíveis para que usuários, e em que circunstâncias.
- Para isso: Autenticação e Autorização.

Prezi

Autenticação

- Garantir a identidade do Agente.
- Ou seja, garantir que o Agente é quem ele diz ser.
- Para isso, há 3 Fatores:

Fatores de Autenticação

- O que o agente é:
  - Impressão Digital, Padrão Retinal, DNA etc.
- O que o agente possui:
  - CPF, RG, Username, Certificado Digital etc.
- O que o agente sabe:
  - Senha, PIN, Chave Privada
- Geralmente, utiliza-se uma combinação de 2 desses fatores.

Prezi

Fatores de Autenticação

- O que o agente é:
  - Impressão Digital, Padrão Retinal, DNA etc.
- O que o agente possui:
  - CPF, RG, Username, Certificado Digital etc.
- O que o agente sabe:
  - Senha, PIN, Chave Privada
- Geralmente, utiliza-se uma combinação de 2 desses fatores.

Prezi

Autorização

- Mas, saber quem o agente é não é suficiente para garantir a segurança dos recursos.
- Deve-se implementar a Autorização com uma Política de Acesso aos recursos.
- Certificados Digitais são excelentes para autenticação, mas péssimos para Autorização. Por quê?

Prezi

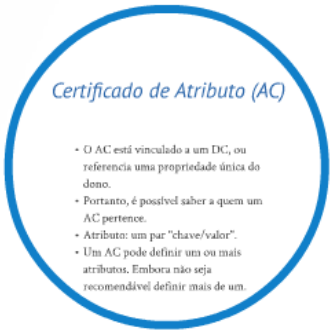
Interoperabilidade

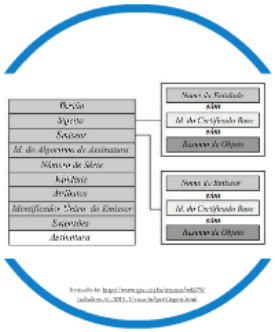
- A Autenticação possui soluções conhecidas e amplamente utilizadas que garantem interoperabilidade.
  - OAuth, OpenID, PKI (ICP).
- Para Autorização, até existem boas iniciativas, mas longe da maturidade.
- Um dos principais alicerces da Autorização com Interoperabilidade: o Certificado de Atributo.

Prezi

Certificado de Atributo (AC)

- É um certificado X.509, assim como o Certificado Digital de Chave Pública (DC)
- Ou seja, possui a mesma estrutura, mas com campos diferentes.
- Diferente do DC, é insuficiente para garantir a identidade, uma vez que não possui uma chave pública.
- Então, como saber o dono do certificado?





Prezi

Certificado de Atributo (AC)

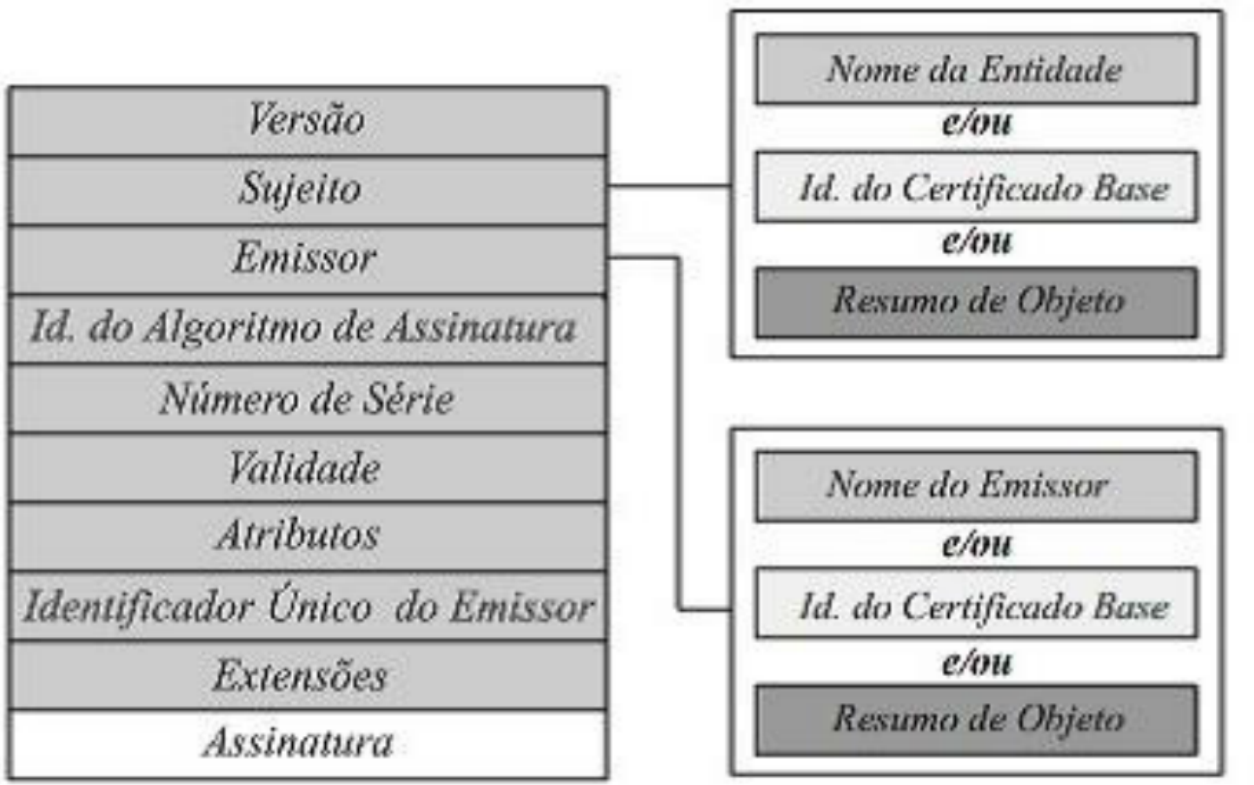
- O AC está vinculado a um DC, ou referencia uma propriedade única do dono.
- Portanto, é possível saber a quem um AC pertence.
- Atributo: um par "chave/valor".
- Um AC pode definir um ou mais atributos. Embora não seja recomendável definir mais de um.

Prezi

Certificado de Atributo (AC)

- O atributo pode ser um requisito para acesso a recursos dentro de um determinado contexto.
- Ou o AC pode armazenar um papel (Role) do usuário, para ser distribuído entre vários sistemas.
- Para a emissão, revogação e distribuição de ACs, foi pensada a Infraestrutura de Gerenciamento de Privilégios (PMI).

Prezi



Retirado de: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/ricardo/privilegios.html

Prezi

Por exemplo

Em um sistema de prontuários médicos eletrônicos exigência de AC com o atributo "CRM" do usuário.
Quem se responsabiliza pela emissão e revogação desses atributos, é o Conselho Regional de Medicina (ou o Federal, possivelmente).
Aos sistemas cabe consultar os certificados de atributo do usuário e determinar se ele possui permissões para realizar determinadas operações com base na existência de um AC, emitido pelo CRM/CFM, com o atributo CRM definido - desde que o certificado esteja dentro da validade e não esteja revogado.

Prezi

Infraestrutura de Gerenciamento de Privilégios (PMI)

- Análoga à Infraestrutura de Chave Pública.
- Ou seja, também utiliza o conceito de Cadeia de Confiança (Chain of Trust).
- É uma infraestrutura cujo objetivo final é a verificação dos privilégios de um agente frente a um sistema, ou conjunto de sistemas.
- Ela estende a Infraestrutura de Chave Pública, uma vez que existem elementos comuns a ambas.

Prezi

Infraestrutura de Gerenciamento de Privilégios

- Elementos já conhecidos: Autoridade Certificadora, Autoridade Certificadora Raiz, DC.
- Novos elementos:
  - Verificador de Atributo.
  - Autoridade de Atributo (AA).
  - Certificado de Atributo (AC).

Prezi

Autoridade de Atributo (AA)

- Encarrega-se de emitir os ACs para usuários finais.
- Esses ACs são assinados com o certificado de chave pública da AA.
- Portanto, qualquer possuidor de um DC, é elegível para ser uma AA. Mesmo uma pessoa física, desde que o verificador confie nessa AA.

Verificador de Atributo

Realiza a checagem de validade e estado de revogação sempre que um AC é recebido.

Prezi

Verificador de Atributo

Realiza a checagem de validade e estado de revogação sempre que um AC é recebido.

Prezi

Infraestrutura de Gerenciamento de Privilégios

Procedimento:

- Um agente autentica-se no sistema.
- O agente requisita acesso a um recurso.
- É necessário o atributo X para que o acesso a esse recurso seja concedido.
- O sistema executa uma chamada ao Verificador de Atributo, informando o agente e o atributo requisitado.
- O Verificador procura pelo certificado de atributo (com o atributo requisitado).
- O Verificador checa a validade do certificado.
- O Verificador informa se o agente possui o atributo ou não.
- O sistema autoriza/bloqueia o acesso de acordo com a resposta do Verificador.

Prezi

Retirado de: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/ricardo/privilegios.html

Prezi

Sistemas de Controle de Acesso

Alguns exemplos de Sistemas de Controle de Acesso baseado em PMI são:

- PERMIS
- Akenti
- SESAME
- CORBAsec

Prezi

Sistemas de Controle de Acesso

No entanto, todos os sistemas existentes de ampla difusão apresentam algum tipo de limitação crucial:

Prezi

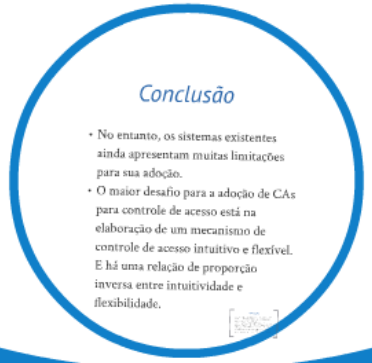
PERMIS

PERMIS utiliza um atributo proprietário (não há liberdade para a aplicação definir qual atributo), e permite armazenamento de CAs apenas em serviços de diretório LDAP.

Prezi

Conclusão

- Autorização é fundamental na implementação de mecanismos de Controle de Acesso.
- PMI permite um modelo descentralizado de autorização, favorecendo a Interoperabilidade de Sistemas.



Prezi

Conclusão

- No entanto, os sistemas existentes ainda apresentam muitas limitações para sua adoção.
- O maior desafio para a adoção de CAs para controle de acesso está na elaboração de um mecanismo de controle de acesso intuitivo e flexível. E há uma relação de proporção inversa entre intuitividade e flexibilidade.

Prezi

Referências

CUSTÓDIO, Igor Vitório. H-PMI: Uma Arquitetura de Gerenciamento de Privilégios para Sistemas de Informação da Área da Saúde. 2010. 139 f. Trabalho de Conclusão de Curso (Pós-graduação) - Universidade Federal de São Carlos, São Carlos, Sp, 2010. Disponivel em: <http://www.bdtd.ufscar.br/htdocs/tedeSimplificado//tde_busca/arquivo.php?codArquivo=3197>. Acesso em: 06 jun. 2013.

BEZERRA, Ernandes Lopes. Introdução a Certificado de Atributo. 2011. Disponivel em: <http://ernandeslb.files.wordpress.com/2011/07/certificado-de-atributo1.pdf>. Acessoem: 06 jun. 2013.

ARREBOLA, Fábio Villamarin. Um modelo de controle de acesso a recursos de rede baseado em Infra- estrutura de Chaves Públicas e Infra-estrutura de Gerenciamento de Privilégios. 2006. 123 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Universidade de São Paulo, São Paulo, 2006. Disponivel em: <http://www.lsi.usp.br/~volnys/academic/trabalhos-orientados/Controle-acesso-baseado-em-ICP-e-IGP.pdf>. Acesso em: 06 jun. 2013.

FARRELL, S.; HOUSLEY, R.; TURNER, S.. An Internet Attribute Certificate Profile for Authorization. RFC5755. IETF, 2010. Disponivel em: <http://datatracker.ietf.org/doc/rfc5755/>. Acesso em: 06 jun. 2013.

BURNETT, Steve; PAINE, Stephen. Criptografia e Segurança: O Guia Oficial RSA. 5. ed. Rio de Janeiro: Elsevier, 2002. 367 p.

Prezi

Controle de Acesso e Certificados de Atributo

Prezi