Segurança

Sistemas Distribuídos

2013

Segurança

- confidencialidade
- autenticidade
- integridade
- não repudiação

} comunicação

Ameaças

- interceptação
- interrupção
- modificação
- fabricação

ataques a canais de comunicação

- escuta
  - obtenção de informação na rede
    - senhas, etc
- masquerading
  - uso de identidades incorretas
- message tampering
  - alteração de mensagens trocadas
- replay
  - reenvio de mensagens obtidas por escuta
- negação de serviço
  - inundação de rede ou servidor

PUC RIO

garantias

- confidencialidade
- autenticação
- autorização
- auditoria

mecanismos

- protocolos
- criptografia

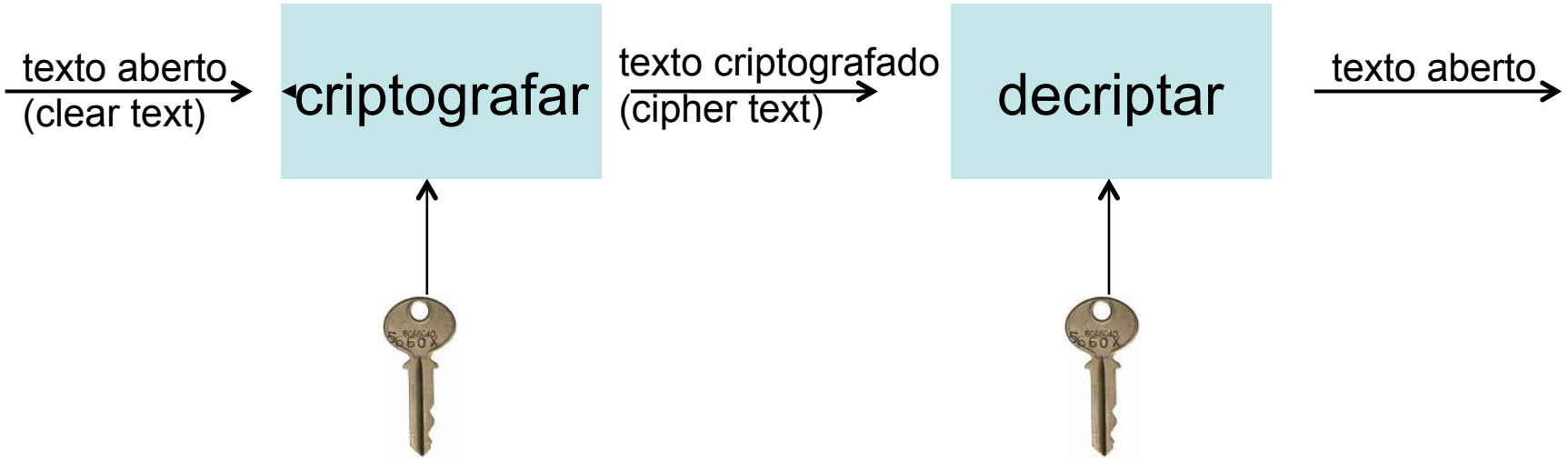
PUC
RIO

política de segurança

- equilíbrio entre custos
  - risco X sobrecarga

PUC RIO

Criptografia de chave secreta



- mesma chave nas duas direções
  - muitas vezes chamada de segredo compartilhado
- também chamada de criptografia simétrica

algoritmos de chave secreta

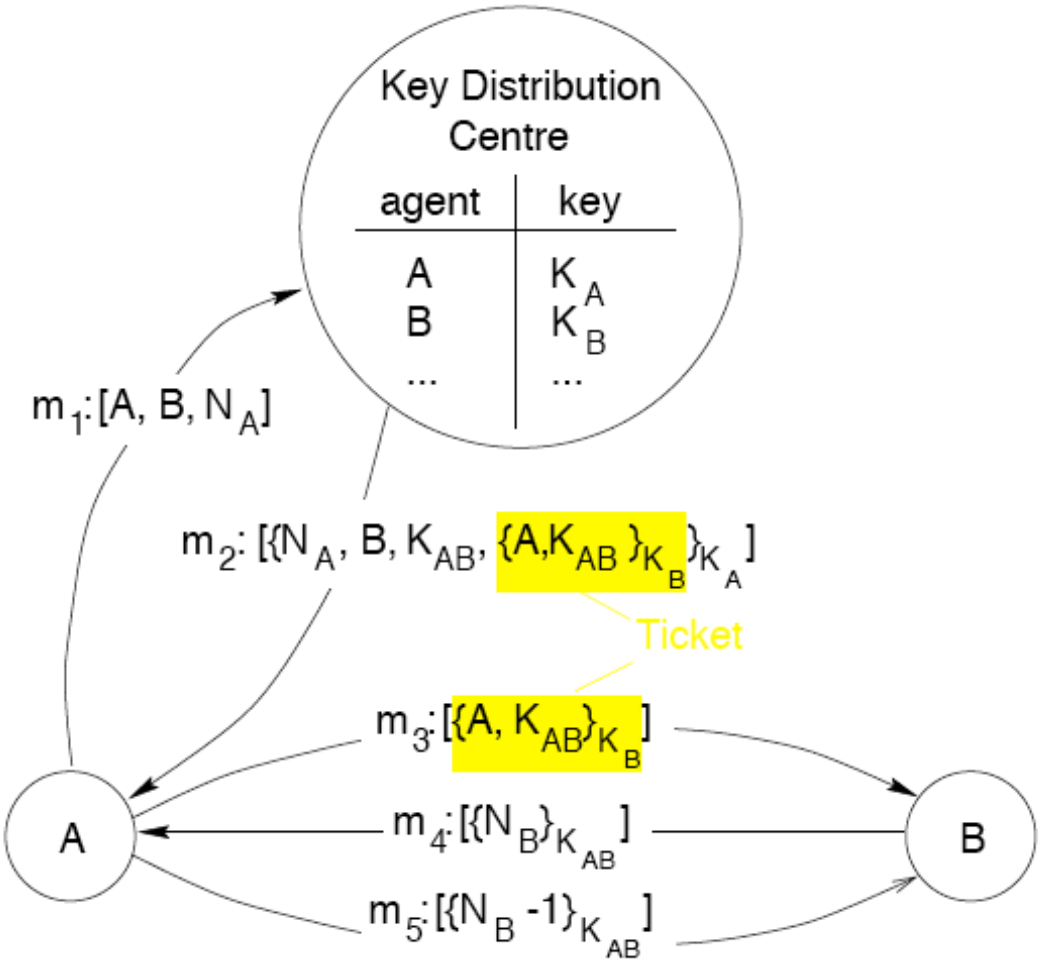
- técnicas de embaralhamento
- muitas vezes pensados para implementação em hardware

PUC
RIO

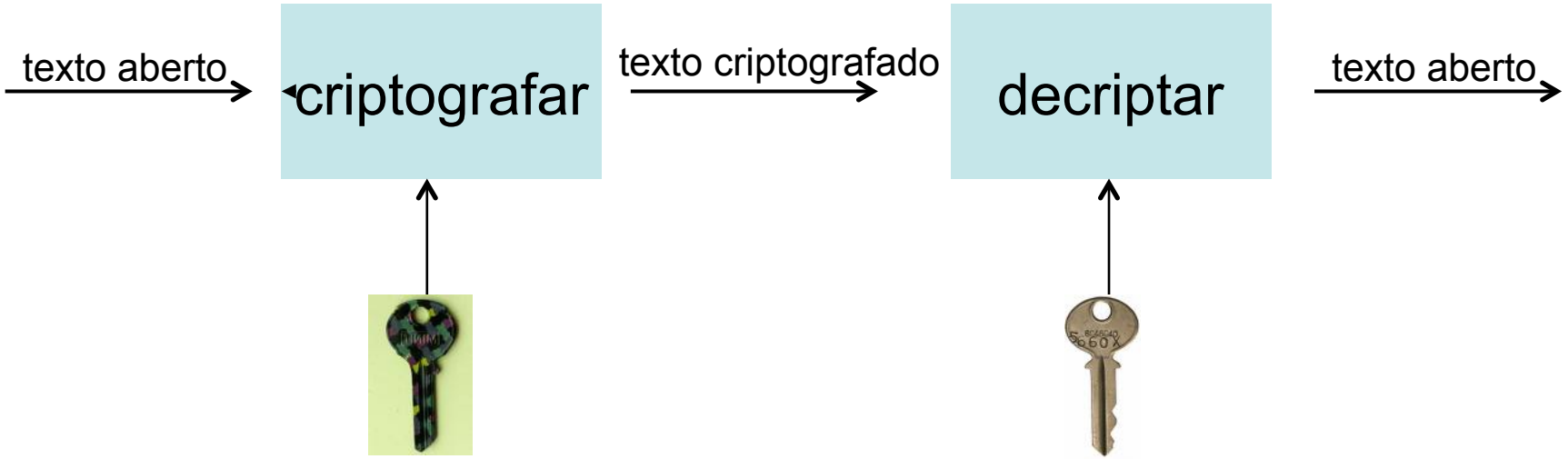
Distribuição de chaves secretas

- como fazer para as duas partes compartilharem um segredo?
- uso de *intermediários confiáveis* ou Key Distribution Centers
  - ex Kerberos

protocolos de acesso a KDCs

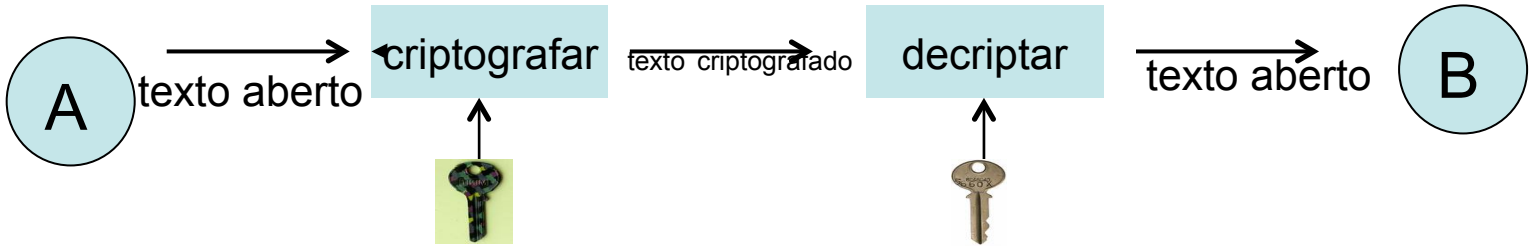


Criptografia de chave pública e privada



- chaves diferentes em cada direção
  - também chamada de criptografia assimétrica
- uma das chaves pode ser pública sem problemas

criptografia assimétrica



- confidencialidade:
  - A criptografa com chave pública de B
- autenticação e integridade:
  - A criptografa com chave privada de A
    - mas como B sabe que o que decriptou era de fato o que A queria enviar?
    - assinaturas digitais

PUC RIO

algoritmos de chave pública e privada

- técnicas aritméticas
  - manipulação de números primos muito grandes
- surgimento do conceito com Diffie-Hellman, em 1976
  - D-H apenas para estabelecimento de segredo compartilhado
- processamento mais custoso que o de algoritmos de chave secreta

Distribuição de chave pública

- intruso ainda pode fazer crer que sua chave pública é a de outra entidade
- infraestutrura de distribuição
  - certificados
  - autoridades de certificação
  - infraestruturas de chaves públicas
    - problemas de raizes de certificação
    - listas de confianca

PUC RIO

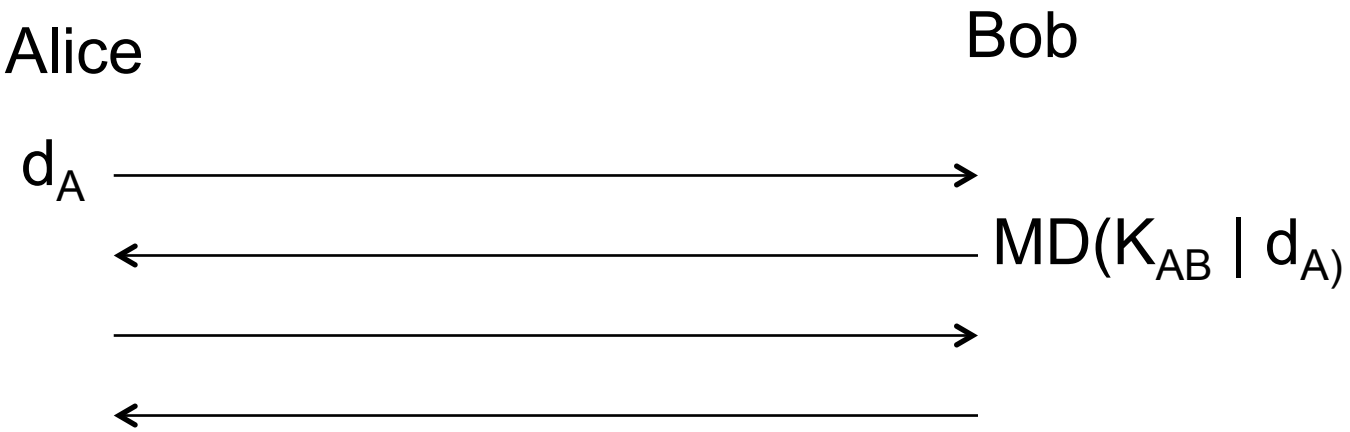
algoritmos de hash

- funções de hash:
  - dado um blobo de dados de tamanho arbitrário, retornam um string de bytes de tamanho fixo
    - entrada: mensagem
    - saída: hash ou digest
  - pequenas alterações nos dados de entrada devem alterar o valor do hash
  - não é possível descobrir a mensagem a partir do hash
  - duas mensagens diferentes dificilmente levam ao mesmo hash

PUC RIO

hash como técnica criptográfica

– em conjunto com segredo compartilhado K_{AB}



ataques para descoberta de chaves

- Diferentes níveis de dificuldade se atacante dispõe de:
  - apenas texto criptografado
  - pares (texto aberto, texto criptografado)
  - pares escolhidos
- ataques de “força bruta”
  - tentativa de quebra com cada chave possível
  - tamanho de chaves e o “computacionalmente difícil”

usos em comunicação

- confidencialidade
- autenticidade
- não repudiação
- integridade
  - aplicação de criptografia sobre *digest* da msg
  - uso combinado de criptografia simétrica e assimétrica

Autenticação

- login e senha
- biometria
- algoritmos de autenticação

algoritmos de autenticação

- uso de desafios e criptografia
  - simétrica e assimétrica

PUC RIO

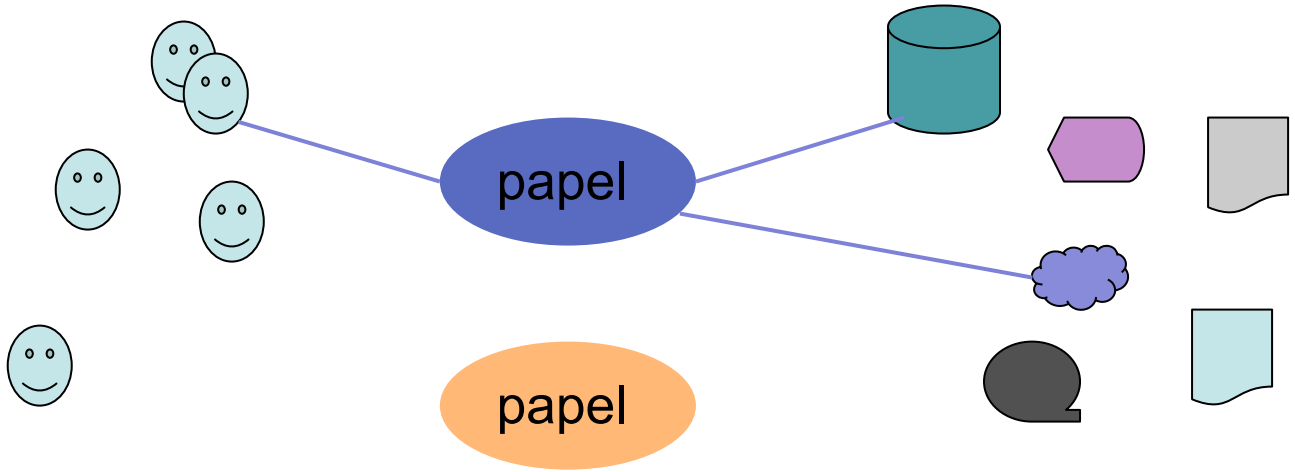
Controle de acesso

- matrizes de acesso
  - usuários X recursos
- normalmente esparsas
- opções:
  - lista de recursos para cada usuário/grupo
  - lista de usuários/grupos para cada recurso

PUC RIO

RBAC

- direitos nem sempre associados a usuários individuais
  - papel do usuário na organização
  - um mesmo usuário pode desempenhar diferentes papéis
    - dinamismo



ABAC

- simplificação de RBAC
  - atributos de usuário utilizados para definir autorizações

PUC
RIO

Autenticação em sistemas distribuídos

- acesso a serviços em diferentes pontos
  - (administrativos e geográficos)
  - escalabilidade
- cada um deles deve identificar o usuário individualmente?
  - cenários como grades, bibliotecas digitais, etc
  - autenticação e controle de acesso

soluções clássicas

- cadastro individual de cada usuário em cada serviço
  - ônus para administrador de serviço
    - cadastro de cada usuário e de seus direitos
  - ônus para usuário:
    - senha (ou outra coisa) para cada serviço?
- conta única para todos os usuários de certa instituição
  - ônus para administrador de serviço:
    - não há como fazer auditoria
  - ônus para usuário
    - não há como diferenciar direitos

PUC RIO

sistemas de identidade web

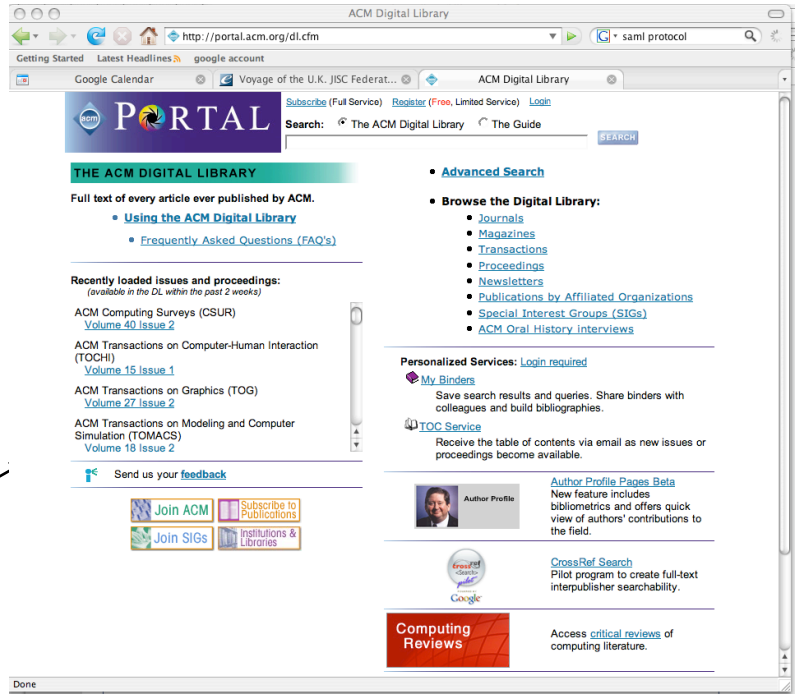
- institucionais
- centrados em usuários

PUC RIO

arquiteturas distribuídas

- provedor de serviço:
  - responsável por serviço controlado
- provedor de identidade
  - responsável por autenticação de usuários
- provedor de atributos
  - fornece informações que podem ser usadas pelo controle de acesso
  - rede de confiança entre provedores
  - propostas específicas para aplicações web

exemplos



acesso a editoras online

- reconhecimento de usuários de instituições cadastradas

PUC RIO

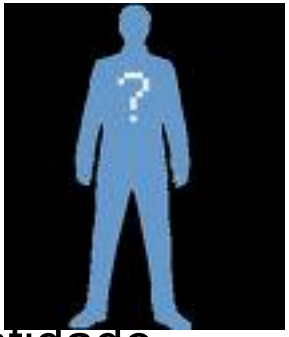
exemplos

vendas com descontos p/ estudantes

- como saber que usuário é estudante?
- certificado? mas serviço tem que conhecer cada usuário?

uso de provedores de identidade

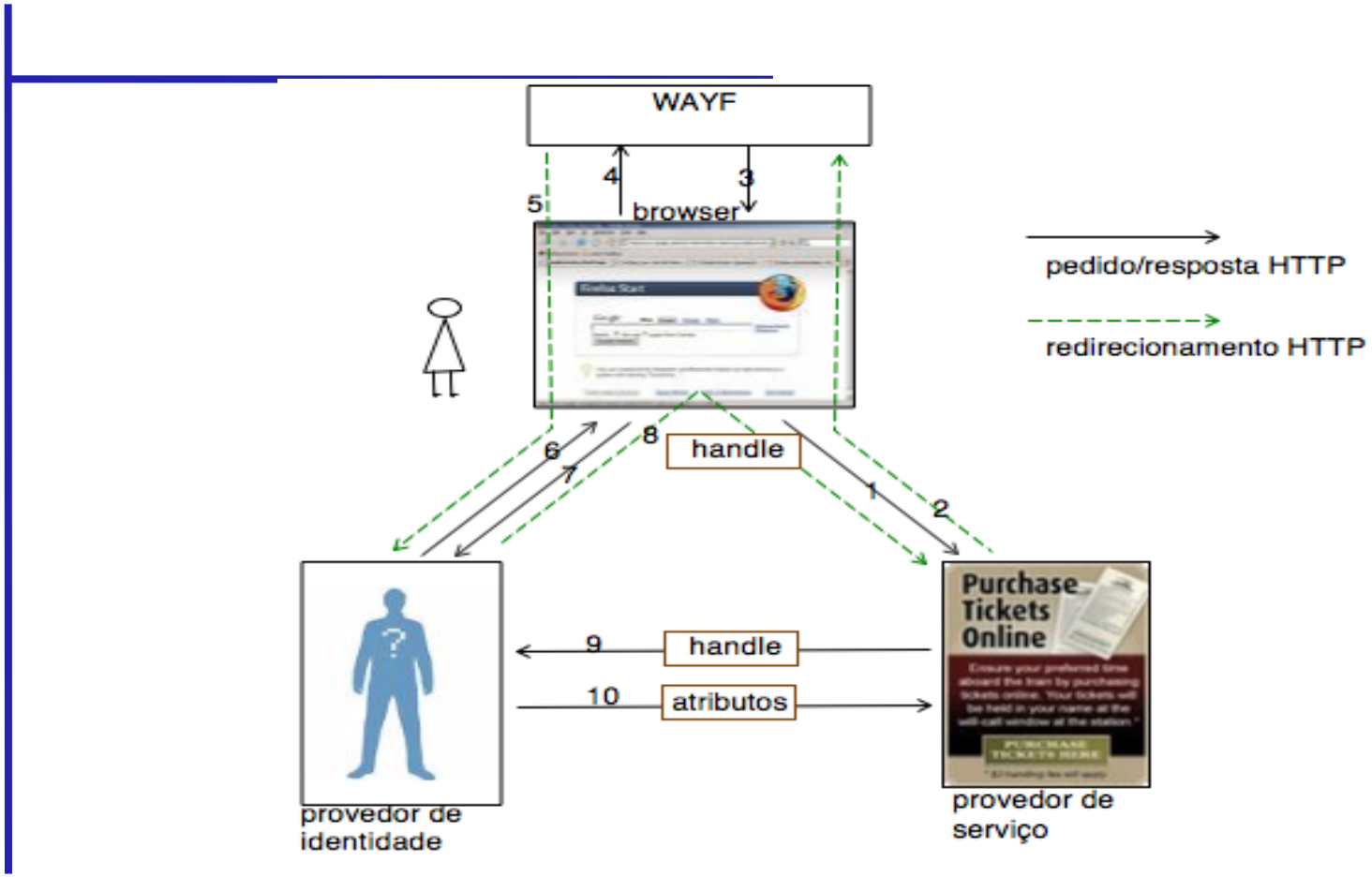
- provedores de serviços confiam em algumas fontes de indentidade



provedor de identidade

serviço em qualquer lugar

exemplo: uso de shibboleth



- protocolo SAML usado na comunicação (shib 2.x)

federações

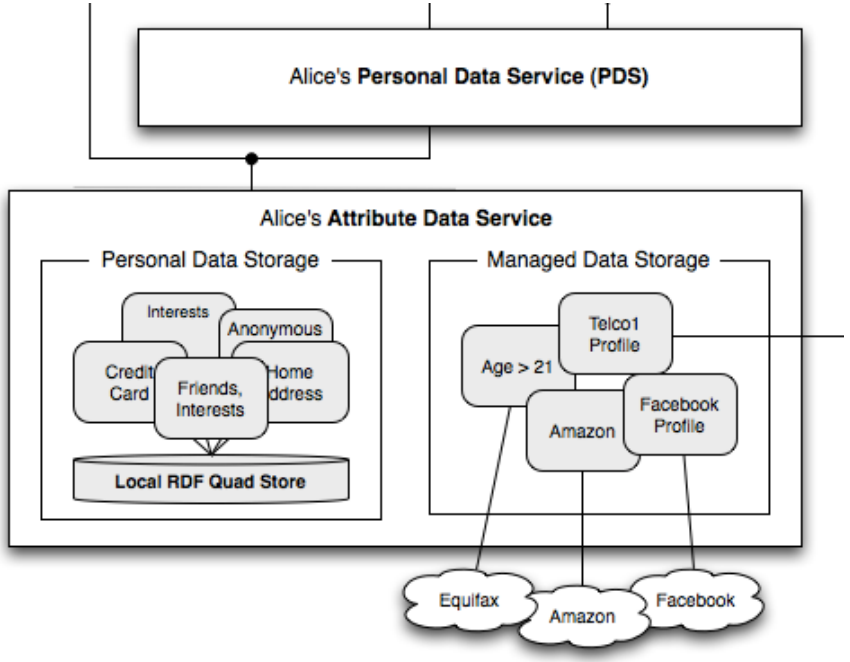
- em andamento em muitos países
- acoplamento com projetos de infraestruturas de chaves públicas
- privacidade: fornecimento do conjunto mínimo de atributos necessários
- foco atual em aplicações web

PUC RIO

identidades centradas em usuários

identidades centradas em usuários

- um conceito semelhante ao do intermediário confiável pode ser usado para armazenar dados do usuário



PUC RIO

Bibliografia

- Charlie Kaufman, Radia Perlman, Mike Speciner. Network Security: Private Communication in a Public World. Prentice-Hall, 1995.
- Ihor Kuz, Felix Rauch, Manuel M. T. Chakravarty, Gernot Heiser. Security in Distributed Systems. Notes for Lectures on COMP9243. University of New South Wales

  www.cse.unsw.edu.au/~cs9243/lectures/
- Dan Alistarh, Seth Gilbert, Rachid Guerraoui, Zarko Milosevic, and Calvin Newport. 2010. Securing every bit: authenticated broadcast in radio networks. In *Proc. of the 22nd ACM symposium on Parallelism in algorithms and architectures* (SPAA '10).