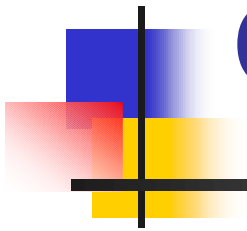


O que é o Middleware?

Prof. Michael Anthony Stanton

UFF

michael@ic.uff.br

Arquitetura de TI hoje

- A proliferação de aplicações configuráveis para o usuário requer centralizar a “configuração”
- O aumento em potência e complexidade da rede requer acesso ao perfil do usuário
- Serviços eletrônicos de segurança pessoal como impedimento à próxima geração de grades de computadores (*grids*)

O que é o Middleware?

- aplicações inter-institucionais requerem a implantação de diretórios e autenticação institucionais interoperáveis
- serviços de rede especializados que são compartilhados entre aplicações e usuários
- um conjunto de componentes críticos de software que permitem a escalabilidade de aplicações e redes

O que é o Middleware?

- ferramentas para domar a complexidade de integração das aplicações
- uma segunda camada da infra-estrutura de TI, localizada acima da rede
- o terreno onde a tecnologia se encontra com as políticas
- a interseção de que não querem fazer os projetistas das redes e os implementadores de aplicações

Exemplos ...

- Bibliotecas digitais precisam de autenticação e autorização escaláveis e interoperáveis
- A Grade (*Grid*): novo paradigma para recursos computacionais:
  - Globus provê *middleware*, incluindo segurança, localização e alocação de recursos, e escalonamento. Isto depende de serviços baseados nos *campi* e em padrões entre instituições

Exemplos ...

- Sistemas para Gestão de Instrução precisam de autenticação e diretórios.
- A próxima geração de portais precisam de autenticação e armazenamento comum.
- Colaboração acadêmica requer compartilhamento restrito de materiais entre instituições.
- Como fez a Internet1 para comunicação, a Internet2 pode fazer para colaboração.

A Terra do Middleware

Upperware p/ Comp. Acadêmica

Upperware para Pesquisa

Upperware para Negócios

Middleware essencial

Middleware da camada de rede

A grade (Grid)

- um modelo para um ambiente de computação distribuída, envolvendo diversos recursos computacionais, base de dados distribuídas, banda de rede, intermediação entre objetos (*brokering*), segurança, etc.
  - Globus (www.globus.org) é um software que implementa a maioria destes componentes; Legion é outro ambiente de software.

A grade (Grid)

- Precisa ser integrado com infra-estrutura do campus.
- Gridforum (www.gridforum.org) é atividade guarda-chuva de agências e acadêmicos.
- Deve-se esperar que grades sejam formadas local e nacionalmente, em física, geociências, biologia, etc.

Middleware essencial

- Identidade - marcadores únicos de quem é você (pessoa, máquina, serviço, grupo)
- Autenticação - como você demonstra que você corresponde a essa identidade
- Diretórios - onde são guardadas as características básicas da identidade
- Autorização - o que uma identidade é permitido fazer
- ICP - ferramentas p/ serviços de segurança

A natureza do trabalho

- Tecnologia
  - Estabelecer serviços extensíveis ao *campus* inteiro: espaço de nomes, autenticação
  - Construir um serviço de diretório corporativo
  - Popular o diretório a partir de sistemas nucleares existentes
  - Habilitar aplicações a usar o diretório

A natureza do trabalho

- Políticas e Política
  - Explicitar os relacionamentos entre indivíduos e a instituição
  - Determinar quem gerencia, que pode atualizar, e quem podem ler dados comuns
  - Estruturar regras de acesso e uso de informação entre departamentos e unidades da administração central
  - Reconciliação de regras e práticas

Quais são os benefícios?

- Economias para TI central - menos gestão de contas, melhores controles de acesso a sítios WWW, melhor segurança de rede, ...
- Economias para TI distribuída - menos administração, acesso a melhores fontes de informação, integração mais fácil de aplicações departamentais para uso no *campus* inteiro ...

Quais são os benefícios?

- Melhoria de serviço para estudantes e professores - acesso a informação escolar, controle de dados pessoais, redução de riscos legais ...
- Participação em novos ambientes para pesquisa - Grades, videoconferências, etc.
- Participação em novas iniciativas colaborativas (do Internet2) - DoD, Shibboleth, etc.

Quais são os custos?

- Aumento modesto em equipamentos e pessoal para TI central
- Muito tempo e esforço para realizar processos de planejamento e verificação para todo o *campus*
- Custos de adaptação de algumas aplicações para usar a nova infra-estrutura central

Quais são os custos?

- Custos para montar a alimentação de informação dos novos serviços centrais de diretório pelos sistemas de aplicação existentes
- Custos políticos de redefinição de feudos em dados e políticas

Usa-se OIDs p/ referenciar identificadores

- codificação numérica para definir unicamente elementos de middleware , tais como atributos de diretório e políticas de certificados
- numeração é apenas para identificação - sem ordenação, hierarquia, etc.

Usa-se OIDs p/ referenciar identificadores

- gerência distribuída; cada campus obtém uma “aresta”, p.ex. 1.3.4.1.16.602.1, e depois cria oids por extensão da aresta, p.ex. 1.3.4.1.16.602.1.0, 1.3.4.1.16.602.1.1, 1.3.4.1.16.602.1.1.1

Obtenção de uma OID

- solicitar à IANA em http://www.iana.org/cgi-bin/enterprise.pl (9.587 OIDs até 16/5/2001)
- mais info em http://middleware.internet2.edu/a-brief-guide-to-OIDs.doc

Principais identificadores do campus

- carteira de identidade
- no. de matrícula
- ID de login
- ID de rede local
- carteira de estudante
- ID de rede
- endereço de correio
- ID de biblioteca/ departamento
- CPF

Características Gerais de Identificador

- Unicidade (dentro de dado contexto)
- Burra X inteligente (depende se subcampos têm significado)
- Legibilidade (máquina X pessoa)
- Abrangência (emissão central X local)
- Resolução (como mapear identificador ao objeto associado)
- Metadados (associados à alocação e resolução de um identificador)

Características Gerais de Identificador

- Persistência (permanência da relação)
- Granularidade (agregado ou componente)
- Formato (dígitos de verificação)
- Versões (mudança das características)
- Capacidade (limitações impostos no número de domínios ou objetos)
- Extensibilidade (capacidade de estender um ID para servir de base de outro ID).

Características Importantes

- Semântica e sintaxe - o que é nomeado, e como
- Domínio - quem emite, qual o espaço de nomes
- Revogação - podemos mudar o ID do sujeito?
- Reutilização - o ID pode ser dado a outro?
- Opacidade - o que podemos deduzir do ID - questões de privacidade e uso

Processo de Mapeamento de IDs

- Mapear IDs do campus usando conjunto canônico de requisitos
- Para cada ID, estabelecer características chave (p.ex. revogação, reuso, privilégios, e opacidade)
- Ilumina os alicerces do middleware
- Primeiro passo essencial na direção das metas mais elevadas do middleware

Opções de Autenticação

- Baseada em senha
  - texto aberto
  - LDAP
  - Kerberos
- Baseada em certificado
- Outras - desafio-resposta, biométrica
- Problema interessante é entre domínios

Aspectos de Autenticação

- gerenciamento do lado do usuário - quebrar, mudar, revelar
- gerenciamento do lado do serviço - gerenciar mudanças, segurança do SO
- alocar primeira senha - entrega segura
- políticas - restrições ou requisitos de uso

Autenticação: boas práticas

- Pré-testar a qualidade das senhas novas
- Pré-testar usando dicionários de outras línguas, não apenas do português
- Verificar senhas novas diferentes das antigas
- Requer mudar senha se potencialmente comprometida
- Para mudar senhas esquecidas, exigir segredo compartilhado ou ID com foto

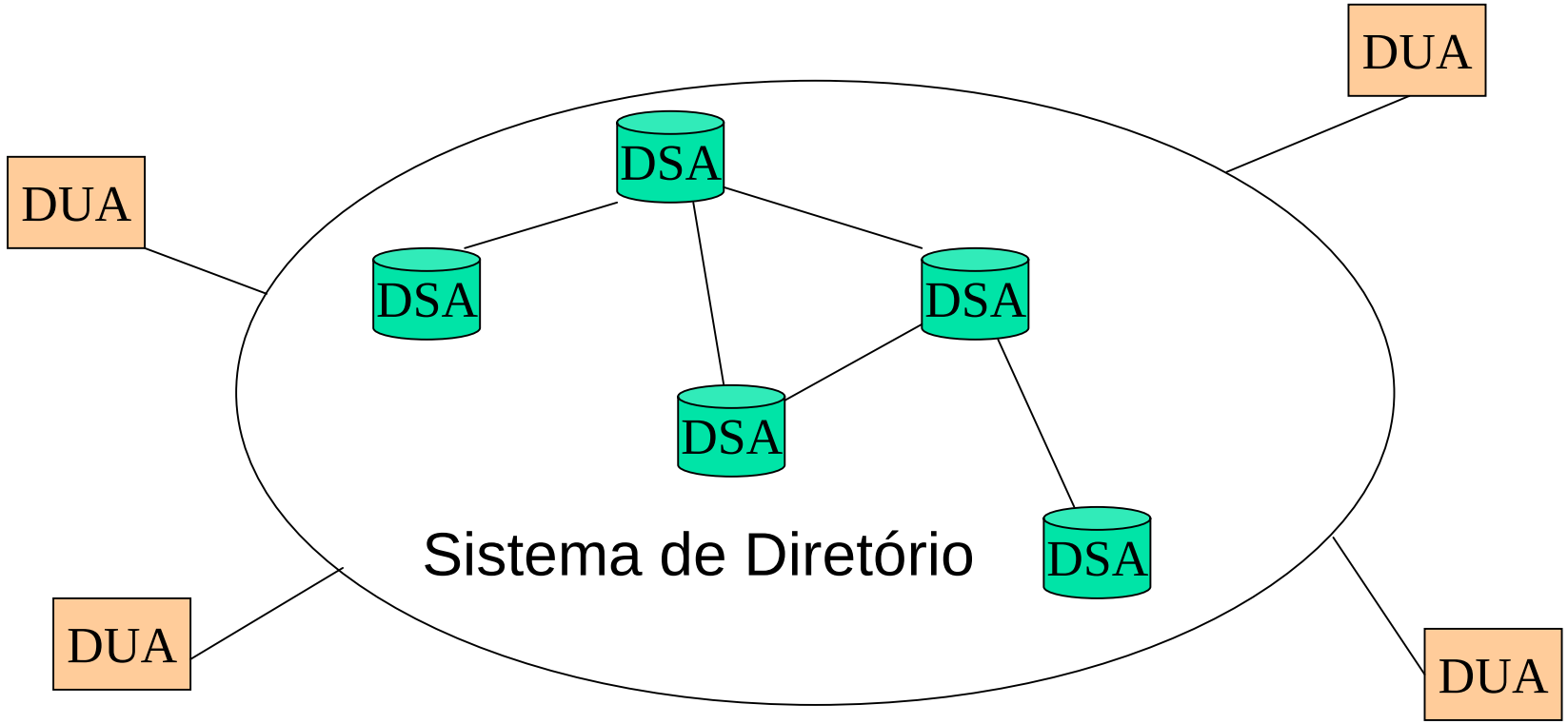
Autenticação: boas práticas

- Enviar pelo correio senha de 1 único uso
- Ao vivo, só com ID com foto
- Para usuário remoto, só ao vivo com representante departamental autorizado e com envio de ID com foto por fax
- Esta identificação/autenticação inicial se fará componente crítico de ICP

Diretório

- Base de dados *on-line* de informação arbitrário
- armazena objetos com atributos
- Implementações
  - X.500
  - LDAP v2, v3 (protocolos de acesso mais simples)

Diretório X.500



DUA - Directory User Agent
DAS - Directory Server Agent

Questões de Diretório

- Aplicações
- Arquitetura geral
  - *chainingl referrals*, redundância e balanceamento de carga, replicação, sincronização, descoberta de diretório
- Esquema e DIT (árvore de info.)
  - atributos, ou's, nomeação, classes de objetos, grupos

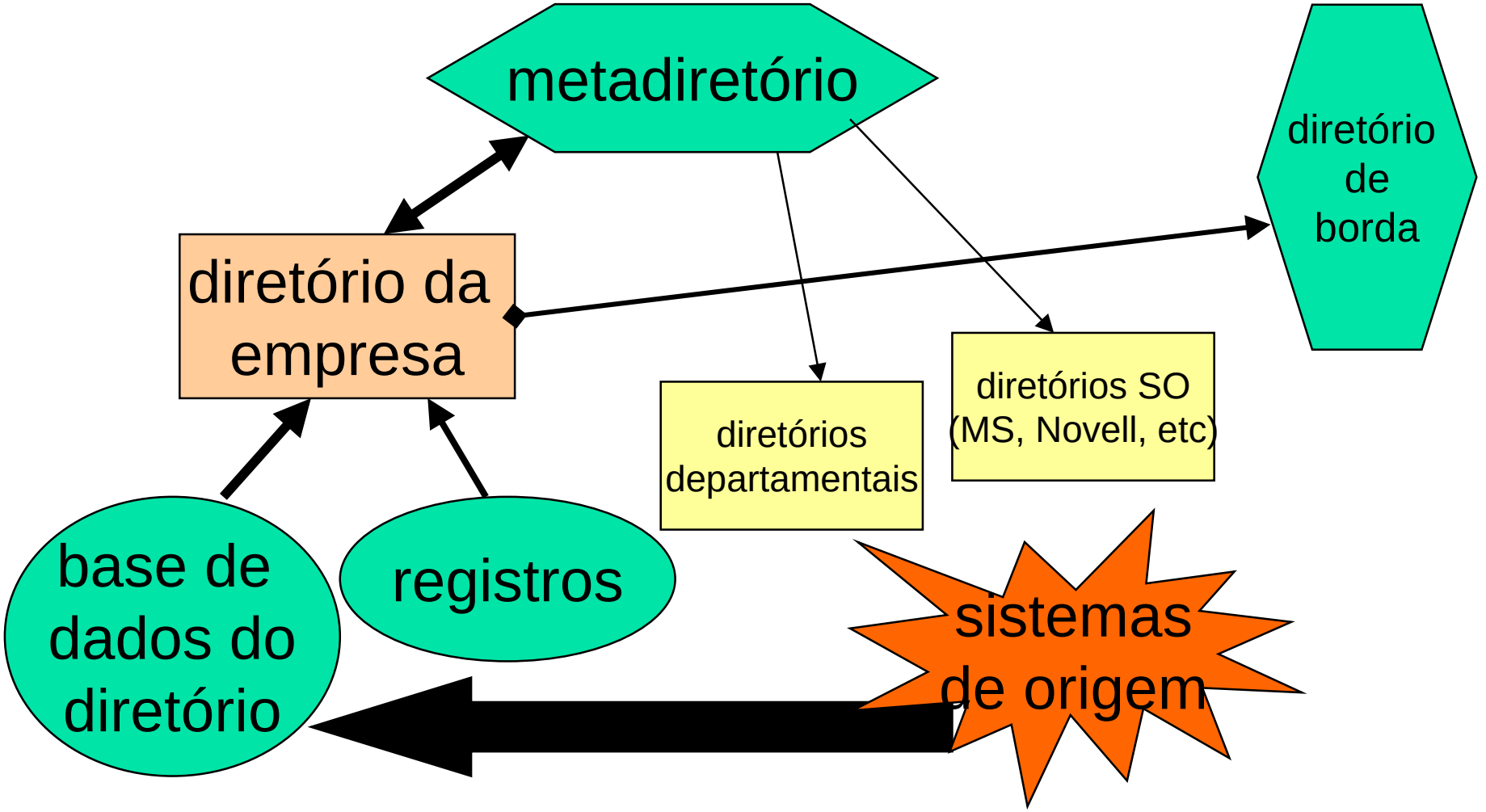
Questões de Diretório

- Atributos e indexação
- Gerenciamento
  - clientes, delegação de controle de acesso, alimentação

Aplicações viabilizadas pelo Diretório

- Correio eletrônico
- Gerenciamento de contas
- Controle de acesso WWW
- Suporte para portais
- Agendas
- Grades de computação (grids)

Arquitetura de Diretório de Campus



Questões chave da Arquitetura

- Interfaces e relacionamentos com sistemas legados
- Desempenho de pesquisa/busca
- Mapeamento ao diretório
- Balanceamento de carga e backups estão vindo, porém proprietários

Questões chave da Arquitetura

- Quem pode ler/atualizar que campos
- Acoplamento diretório da empresa com um SO específico
- http://www.georgetown.edu/giia/internet2/ldap-recipe/

Esquema e DIT: Boas Práticas

- Pessoas, máquinas, serviços
- O espaço de pessoas quase “plano”
- Manter contas como atributos, não “ou”
- Políticas de replicação e grupo não deve determinar esquema
- escolha de nomes RDN rica e crítica
- indexar usando outras chaves
- Criar e preservar espaços de nomes unificados

Atributos: Boas Práticas

- Use inetOrgPerson, eduPerson, localPerson
- Nunca reaproveite um campo já definido no RFC. Prefira incluir novos atributos
- Ligue verificação pelo esquema, se não for realizada pela BD de apoio; desempenho
- A maioria de clientes LDAP não lida bem com atributos com múltiplos valores, mas uso de múltiplos campos e dn's distintos não é melhor.

Gerenciamento: Boas Práticas

- Não permita “arrastão”; mais pesquisa que leitura
- Acesso: cliente LDAP X WWW
- Pense muito sobre quem pode atualizar
- Pense muito sobre quando atualizar
- LDIF deve ser substituído por XML com formato de intercâmbio

Gerenciamento: Boas Práticas

- Delegação de controle - escalabilidade
- “Vide tb”, encaminhamento, replicação, sincronização na prática
- Replicação não deve ser feita baseada em árvores, mas usando regras e atributos

ICP - Infra-estrutura de Chave Pública

ICP - Infra-estrutura de chave pública

- Primeiras idéias
- Fundamentos - Componentes e Contextos
- As peças que faltam - na tecnologia e na comunidade

ICP: Algumas observações

- Pense nela como conectividade para indivíduos, não para máquinas...é tão ubíqua e importante
- É necessário ter uma única infra-estrutura? Quais são os custos de múltiplas soluções? Subredes e ITPs...
- Opções trazem complexidade; gerir complexidade é essencial
- ICP pode fazer tanta coisa, que hoje faz muito pouco

Algumas a mais...

- Conectividade IP foi um negócio dos sonhos. Foi construída, e depois chegaram as aplicações. Infelizmente, com ICP as aplicações chegaram primeiro, antes da infra-estrutura,o que torna mais difícil o desenvolvimento.
- Ninguém parece estar desenvolvendo soluções para a ágora.

Aplicações de ICP e Certificados

- autenticação e pseudo-autenticação
- assinatura de docs
- criptografia de docs e correio
- não repudiação
- canais seguras numa rede
- autorização e atributos
- multicast seguro, e mais...

Componentes ICP

- Certs. X.509 v3 - perfis e usos
- Validação - Listas de Revogação de Certs (CRLs), construção de caminhos
- Gerência de certs. - gerar certs, usando chaves, arquivamento e depósito (“escrow”), mobilidade, etc.

Componentes ICP

- Diretórios - para guardar certs, e chaves públicas, e talvez chaves privadas
- Modelos de confiança e I/A
- Aplicações habilitadas por certs

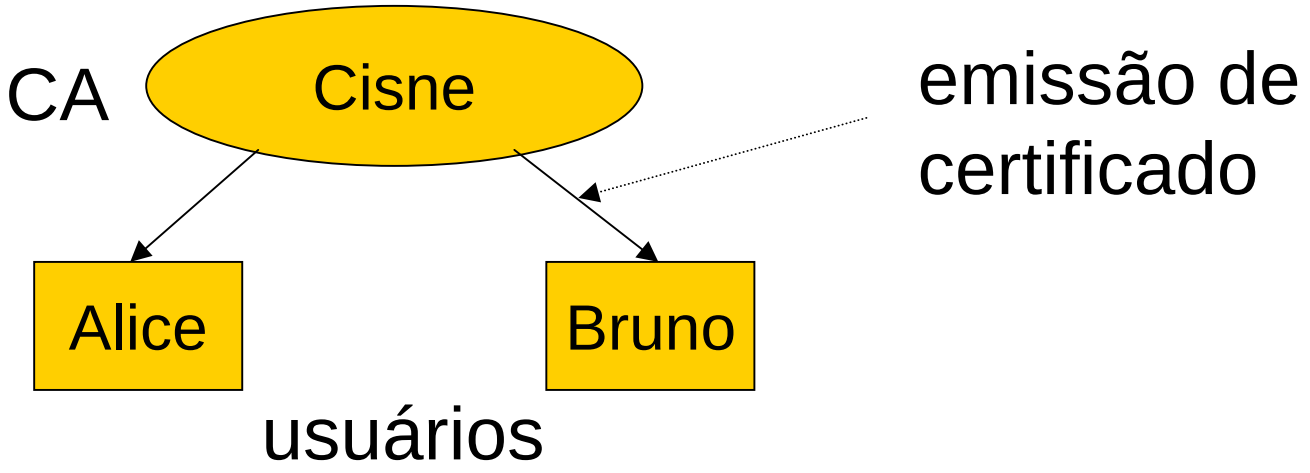
Arquiteturas de ICP

- Autoridade certificadora (CA) - entidade confiável para aceitar/validar certificado
- Fácil quando o certificado emitido pela CA “local” ... e, se não for?
- Precisamos discutir múltiplas CAs

Arquiteturas simples

CA única

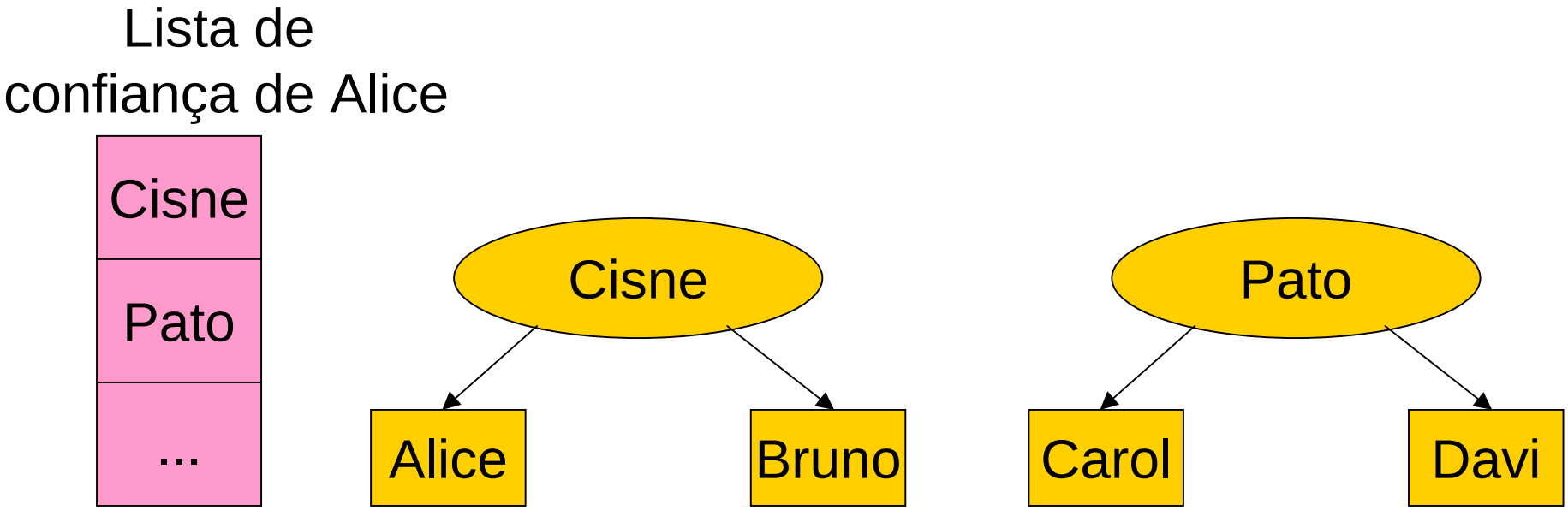
- CA não precisa confiar em outra
- Caminho de certificação de 1 cert



Arquiteturas simples

Lista de confiança

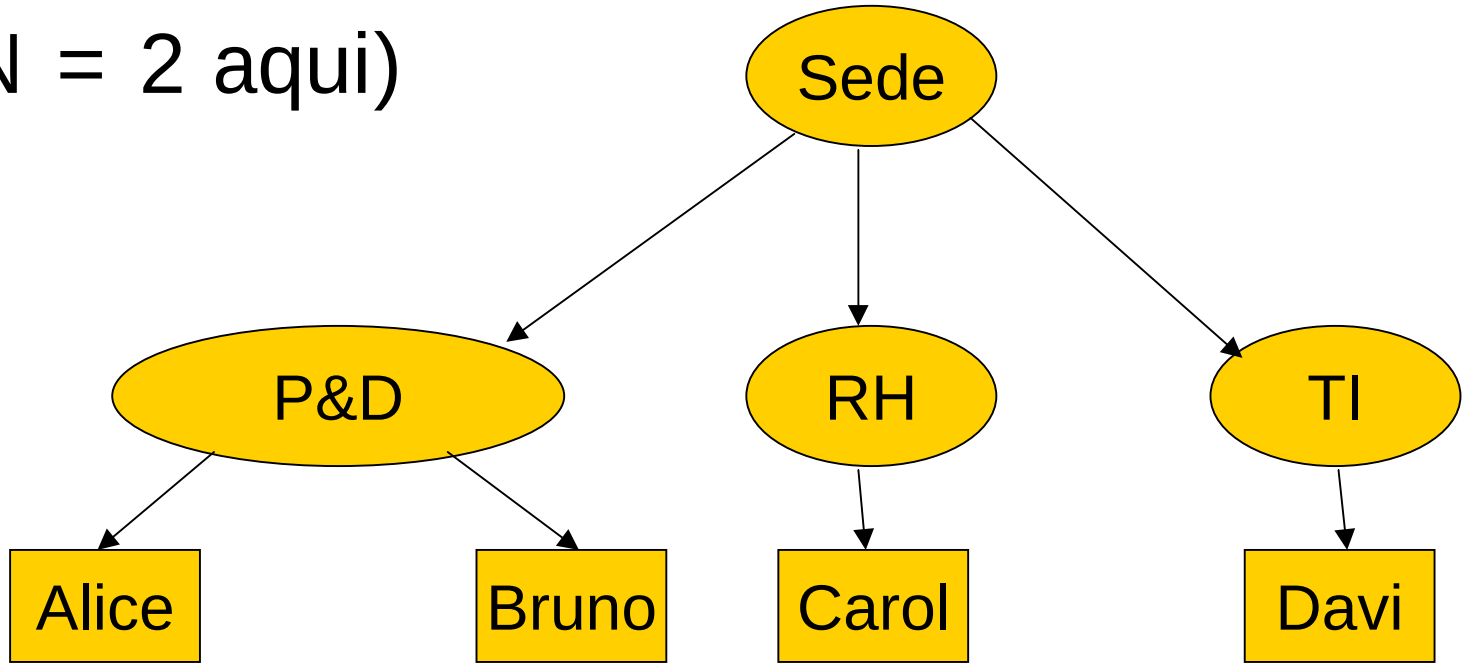
- Usuário mantém lista própria de CAs confiáveis
- Caminho de confiança de 1 cert



Arquiteturas de empresa

ICP hierárquica

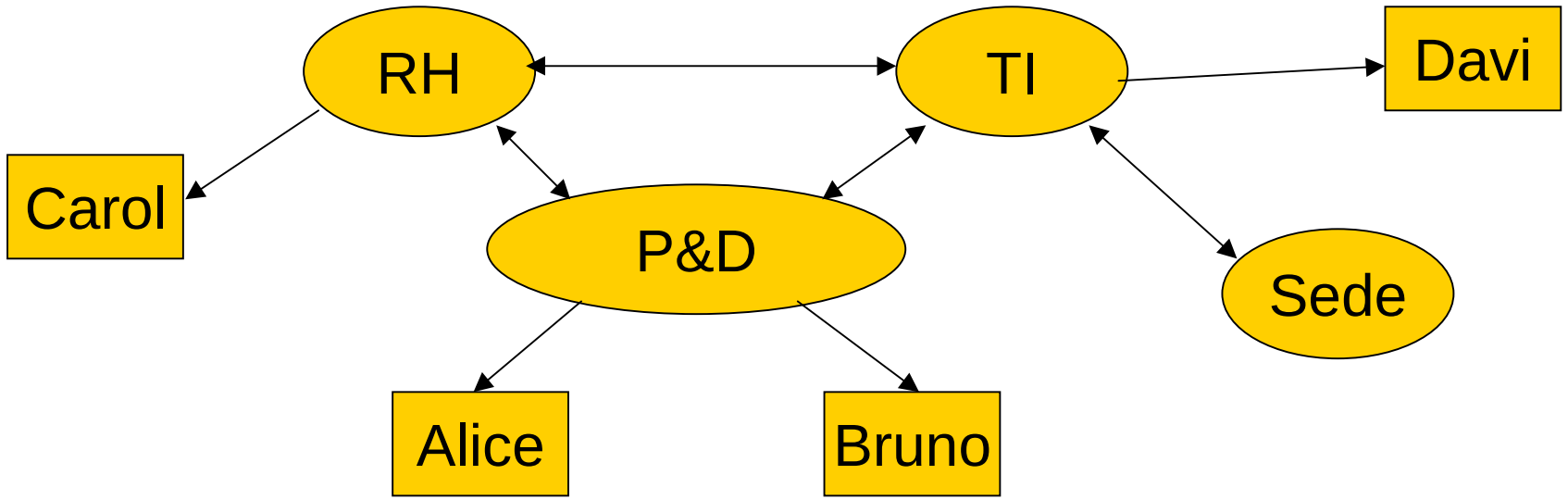
- Ponto de confiança = raíz
- caminho = N certs
  (N = 2 aqui)



Arquiteturas de empresa

ICP em malha

- “teia de confiança”
- certificação cruzada entre CAs
- caminhos mais difíceis de achar



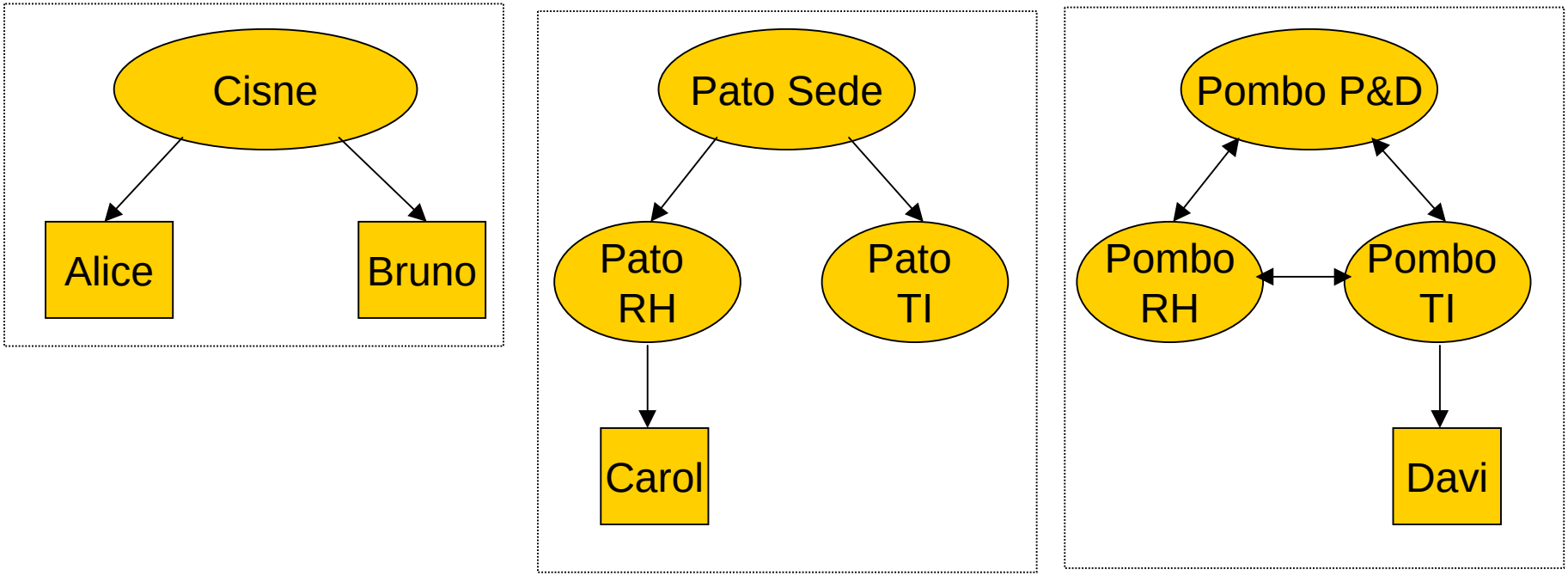
Arquiteturas de empresa

Hierarquia X Malha

- Hierarquia:
  - solução elegante, apropriada para empresa de estrutura hierárquica
  - CA raíz é ponto crítico de compromisso
- Malha:
  - solução pragmática
  - Robusto
  - Encontrar caminho (bem) mais complexo

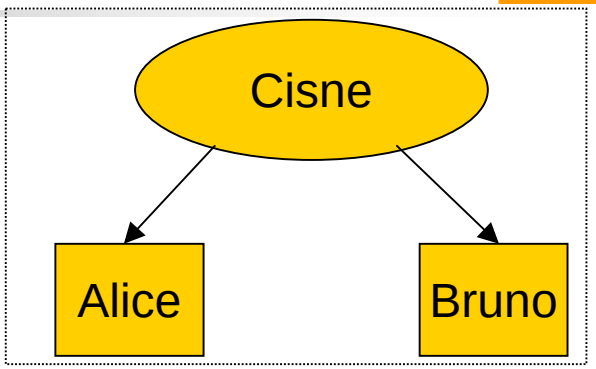
Arquiteturas hibridas

- Não se pode sempre montar uma única ICP
- Considere 3 ICPs diferentes



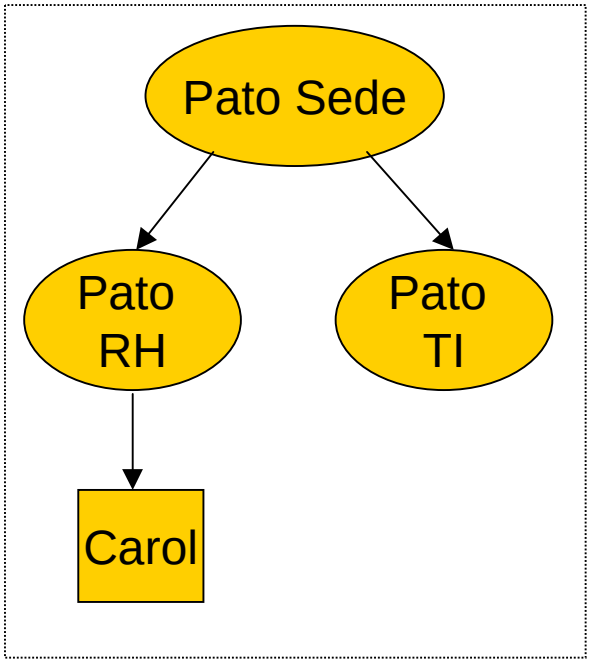
Lista de confiança estendida

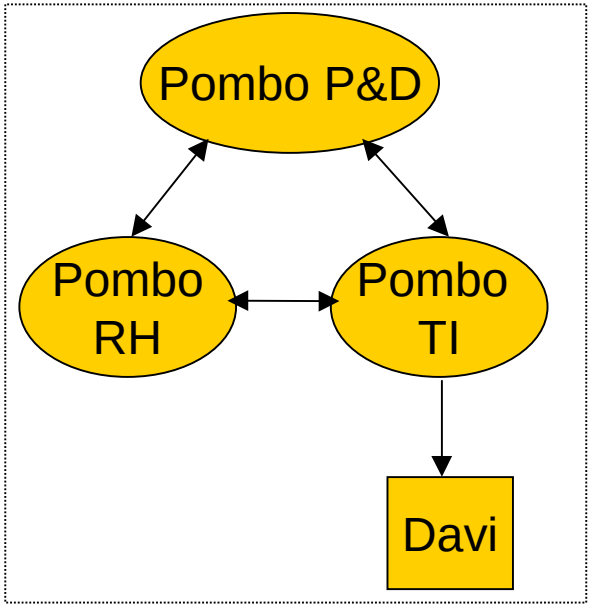
- solução “rápida”



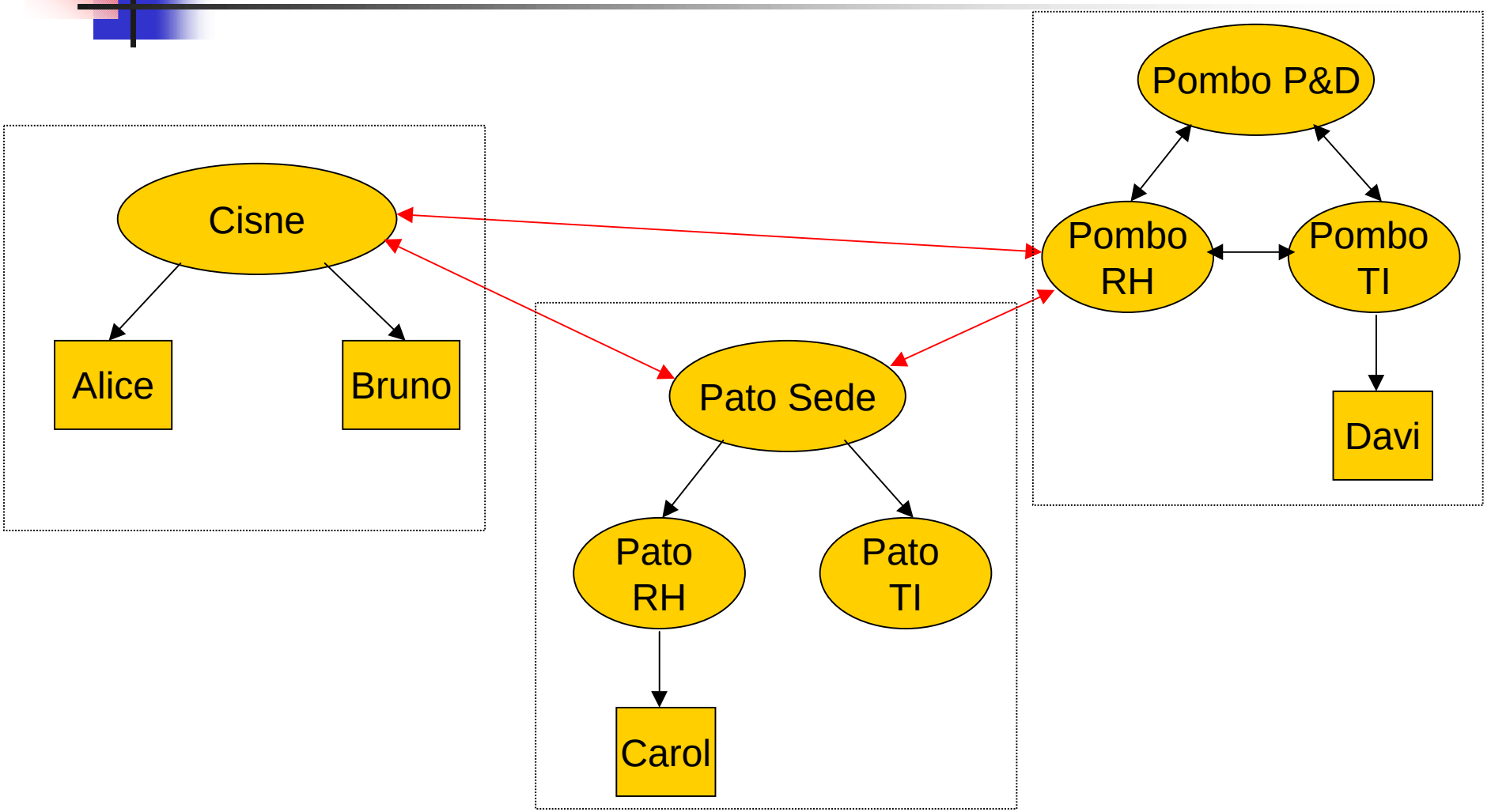
Lista de confiança de Alice

Cisne
Pato Sede
Pombo P&D

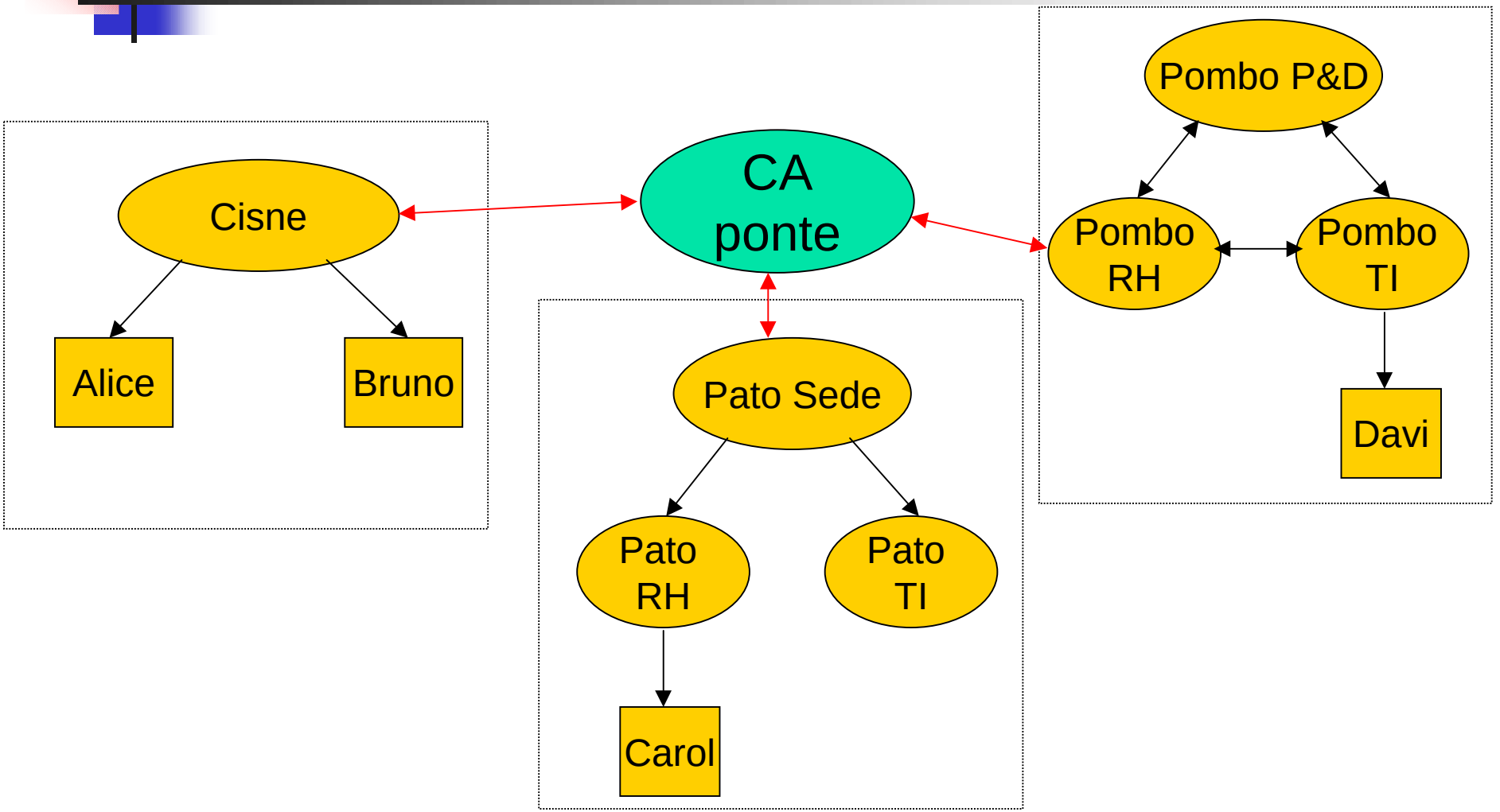




Certificação cruzada de ICPs de empresa



CA ponte


Cisne
Alice
Bruno
CA
ponte
Pombo P&D
Pombo
RH
Pombo
TI
Davi
Pato Sede
Pato
RH
Pato
TI
Carol

Avaliação comparativa

- Certificação cruzada de ICPs
  - funciona para no. pequeno de ICPs, ou com relações estáticas
- Ponte
  - solução eficiente para no. arbitrário de ICPs, ou com relações dinâmicas

ICP: Contextos para Uso

- Intra-campus
- Dentro da comunidade de Ensino Superior de interesse
- No mundo mais amplo

ICP: Opções de Implementação

- Própria - com s/w de domínio público ou próprio ao campus
- Própria - usando produto comercial
- Terceirizada - usando serviços comerciais
- Terceirizada - uma gama de serviços e questões
- o que fazer depende de quando o faz...

Certs X.509

- objetivo - associar uma chave pública a um sujeito
- campos padrão
- campos estendidos
- perfis para capturar protótipos
- questões de cliente e servidor
- v2 para quem começou cedo, v3 agora, v4 sendo finalizado para tratar formatos adicionais de certs (atributos, etc.)

Campos padrão em certs

- número de série do cert
- sujeito, como DN de x.500, ou ...
- chave pública do sujeito
- validade
- emitente, com ID e nome comum
- algoritmo de assinatura
- info da assinatura do cert, usando a chave privada do emitente

Campos de extensão

- Exemplos - sob-códigos de autorização/ sujeito, uso da chave, URL LDAP, pontos de distribuição de CRL, etc.
- Uso da chave é muito importante - para assinaturas digitais, não repudiação, criptografia de chave ou dados, etc.

Campos de extensão

- Certas extensões podem ser marcadas “críticas” - se uma apl não entende da extensão, então ela não usa o cert
- Requer perfis para documentar, e muito cuidado...

Gerência de Certs

- Protocolo de Gerência de Certificados - p/ a criação, revogação e gestão de certs
- Opções de Revogação - CRL, OCSP
- Armazenamento - onde (dispositivo, diretório, cache privada, etc.)
  e como - formato (DER, BER, etc.)
- Escrow e arquivamento de chaves - quando, como, e o que mais precisa ser guardado?

Gerência de Certs

- Software de Autoridade Certificadora (CA), ou opção terceirizada
  - feito em casa
  - fonte aberto - OpenSSL, OpenCA, Oscar
  - comercial - Baltimore, Entrust, etc.
  - integrado no SO - W2K, Sun/Netscape, etc.

Diretórios

- para guardar certs
- para guardar CRL
- para guardar chaves privadas, por enquanto
- para guardar atributos
- implementar com diretórios de borda, ou ACLs dentro do diretório da empresa, ou com diretórios proprietários

O que ainda falta...

- Políticas de Certificados, e Declarações de Práticas de Certificados
- Estruturas de confiança entre domínios
- Mobilidade

Políticas de Certificados (CP)

- Políticas: responsabilidades e riscos legais (questões de compensação)
- Operação de sistemas de gerência de certificados
- Espera-se manter quase uniformidade dentro da comunidade
- Níveis de confiabilidade - varia de acordo com processos I/A e outros fatores operacionais

Declarações de Práticas de Certificados (CPS)

- Práticas - detalhes específicos ao local de conformidade operacional com uma política de cert
- Uma Autoridade de Gerência de Políticas (PMA) determina se um CPS é adequado para uma dada CP.

Componentes do modelo de confiança entre domínios

RNP

- verificação de confiabilidade entre remetente-receptor através de uma entidade comum confiável aos dois
- precisa atravessar caminhos ramificados para estabelecer caminhos de confiança
- necessário usar CRLs, etc., para validar confiança
- se políticas nos certs, validação complexa

Componentes do modelo de confiança entre domínios

- delegação torna o trabalho ainda mais difícil
- Hierarquias X Pontes
  - questões de filosofia e implementação
  - em jogo: transitividade e delegação
  - hierarquias contam com um modelo de confiança comum
  - pontes usam acordos bilaterais s/ modelos de confiança e mapeamento de políticas

Opções de Mobilidade

- cartões inteligentes (smart cards)
- USB dongles
- senhas para recuperar de um depósito ou diretório
- esquemas proprietários de “roaming” são comuns - Netscape, VeriSign, etc.
- GT SACRED criado dentro da IETF
- Dificuldade de integrar certs de múltiplos depósitos (HD, diretório, dispositivo, etc.)

Vai funcionar?

- Bem, ele tem que funcionar...
- Escalabilidade
- Desempenho
- “Com força suficiente, qualquer coisa voa”

Leitura adicional

- Internet2
  http://middleware.internet2.edu
- Houseley e Polk, “Planning for PKI”, Wiley, março de 2001