ATIVIDADES EM MIDDLEWARE DA RNP

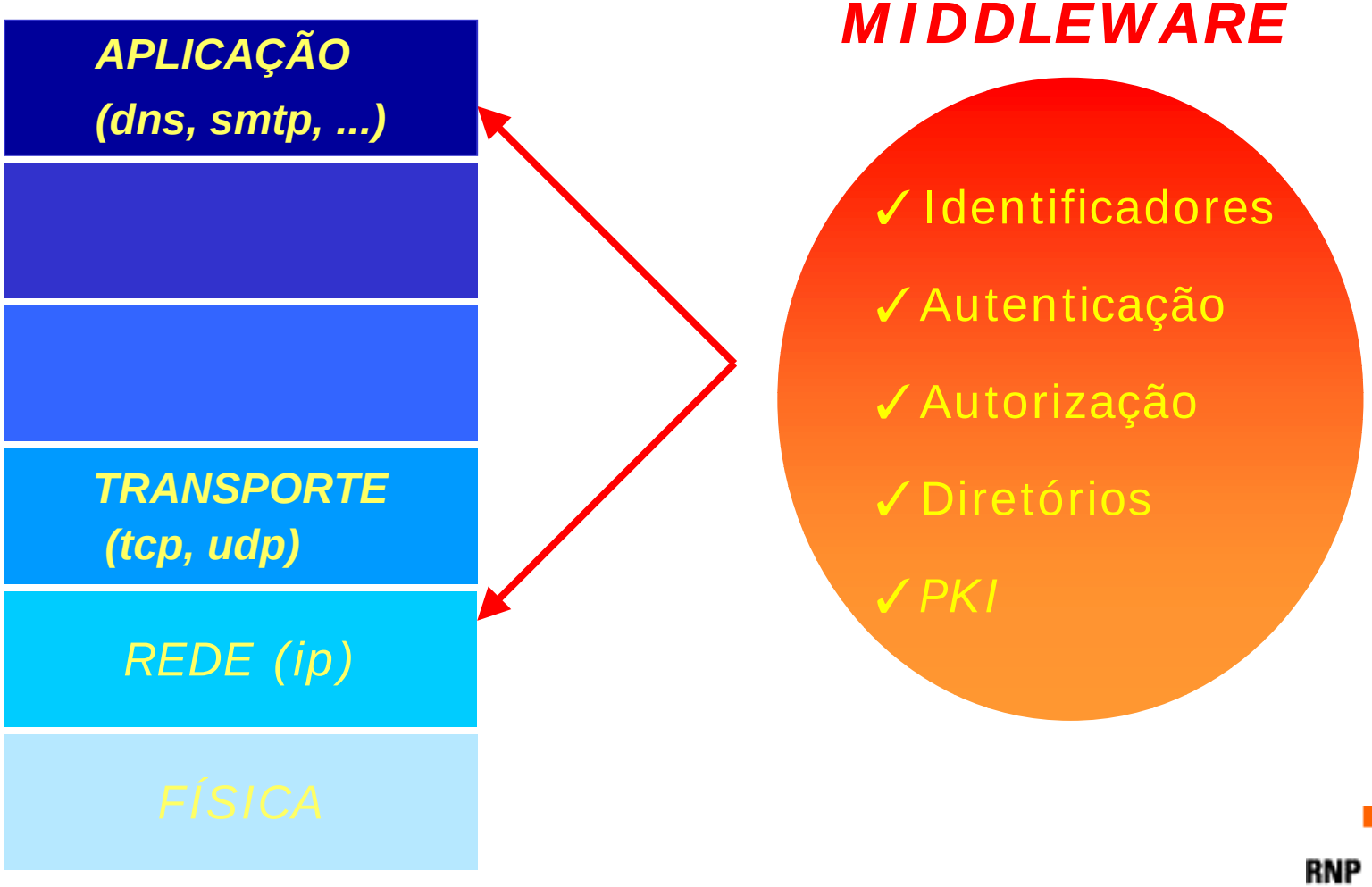
Maria Teresa Moura

Maio 2001

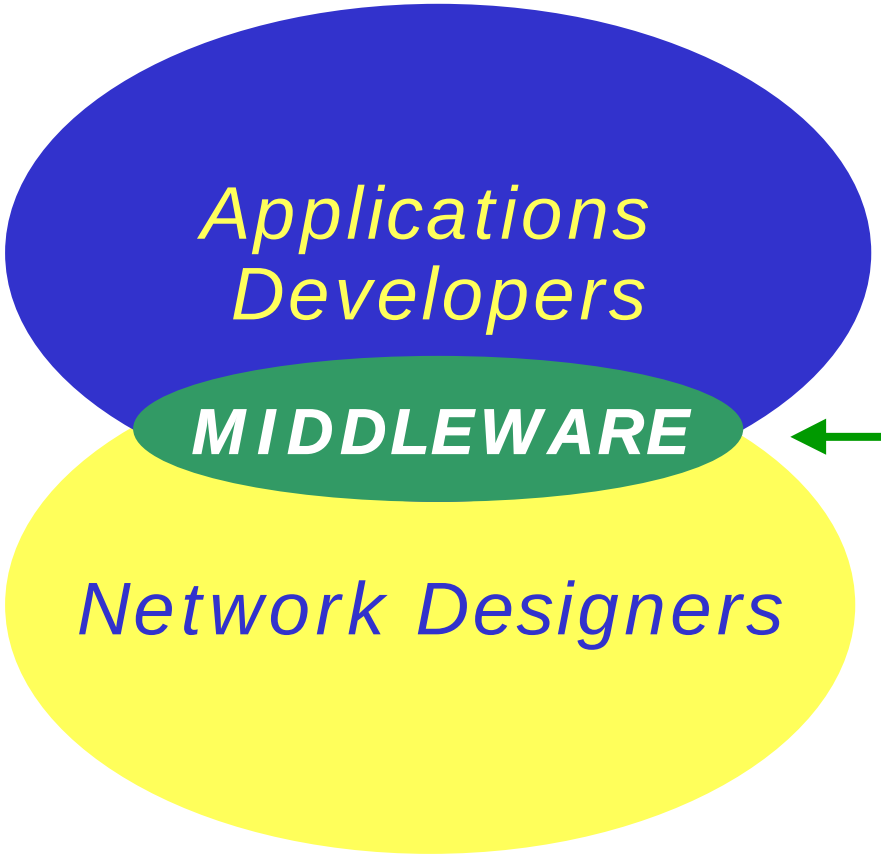
RNP/REF/0236

Índice

Middleware


APLICAÇÃO
(dns, smtp, ...)
TRANSPORTE
(tcp, udp)
REDE (ip)
FÍSICA
MIDDLEWARE
✓Identificadores
✓Autenticação
✓Autorização
✓Diretórios
✓PKI

Middleware



Padronização e
Interoperabilidade

Intranet - características:

- Sistema de informações da RNP
- Apoio às tarefas de gestão
- Melhorar integração da equipe e comunicação com os PoPs
- Módulos de gerência administrativa, de recursos humanos e da informação
- Distribuída: núcleo de coordenação (RJ), núcleos de apoio (RC, CP e DF) e PoPs
- Acesso individualizado

A Experiência da RNP (cont.)

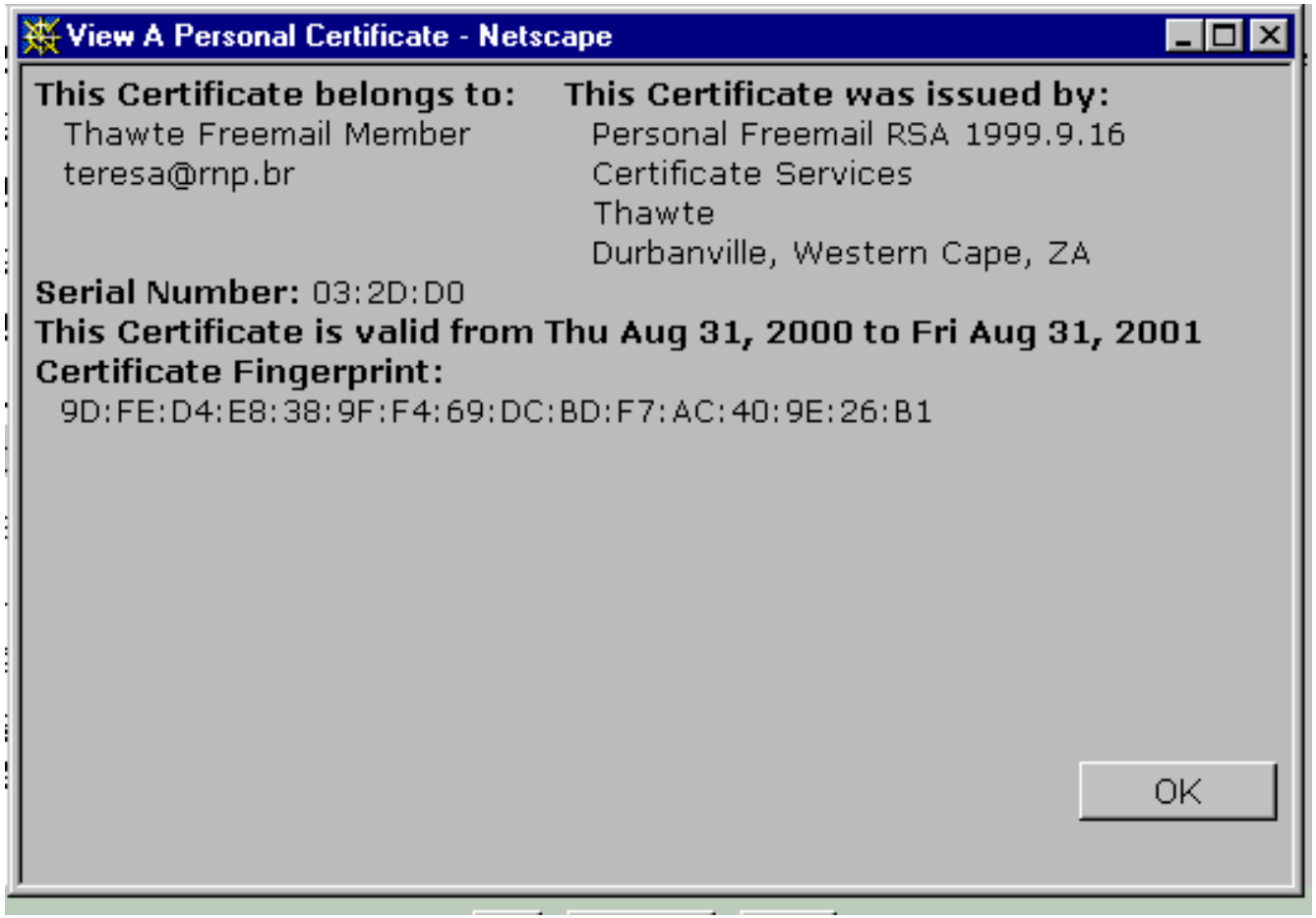
- Aplicação de recursos de *middleware* para suporte aos serviços de identificação, autenticação e autorização segura:

Certificado digital (PKI) e Diretórios (LDAP)

Utilização de certificado digital:

- Alternativa para autenticação por *login* e senha
- Maior nível de segurança em transações pela Internet
- Certificado digital:
  - documento eletrônico de identificação
  - identifica unicamente um usuário
  - pode ser armazenado em disco rígido, disquete ou *smartcard*
  - formado por um par de chaves: pública e privada
  - emitidos e mantidos por uma CA (*Certificate Authority*)
- Utilização para autenticação de clientes web

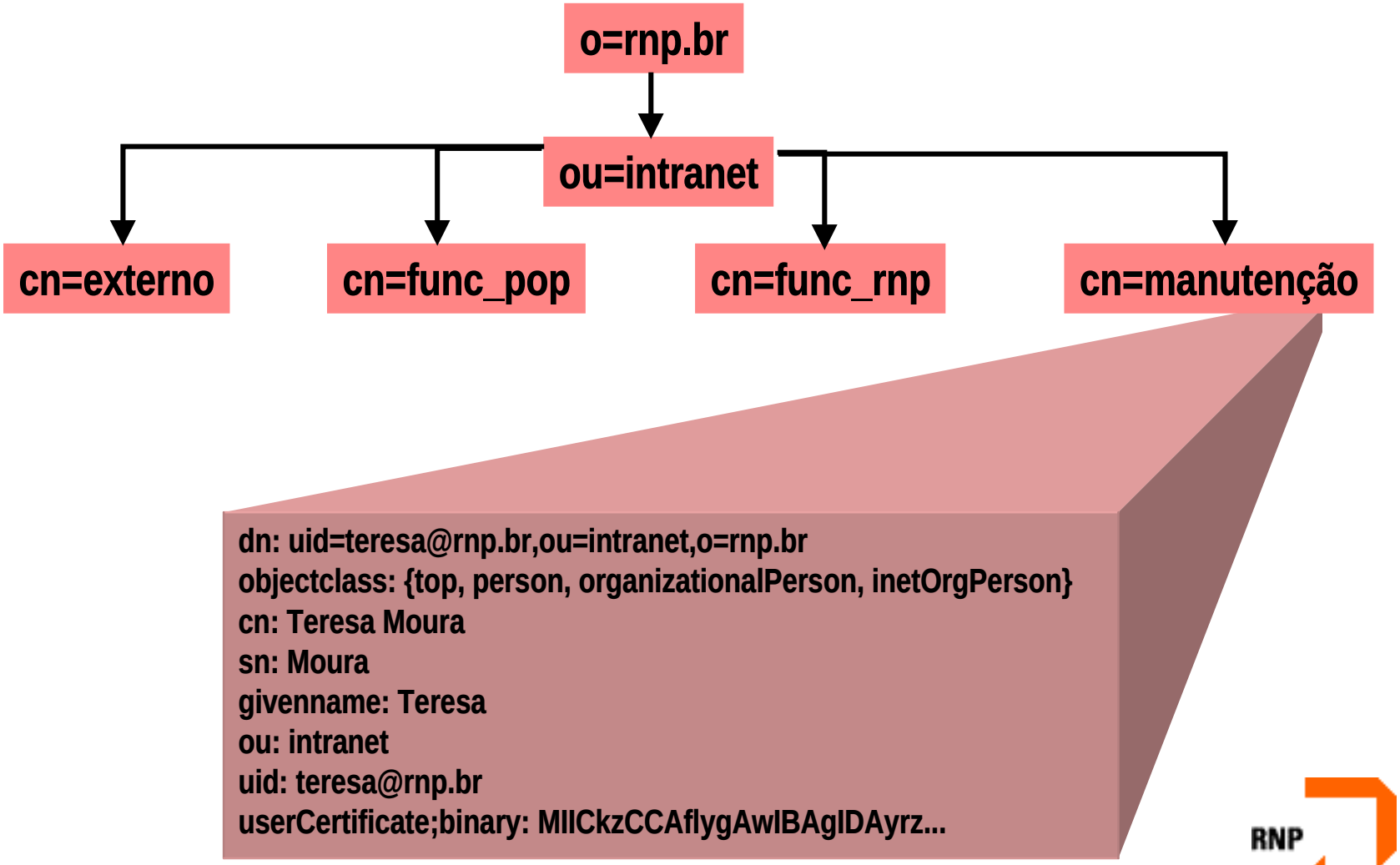
Exemplo de certificado:



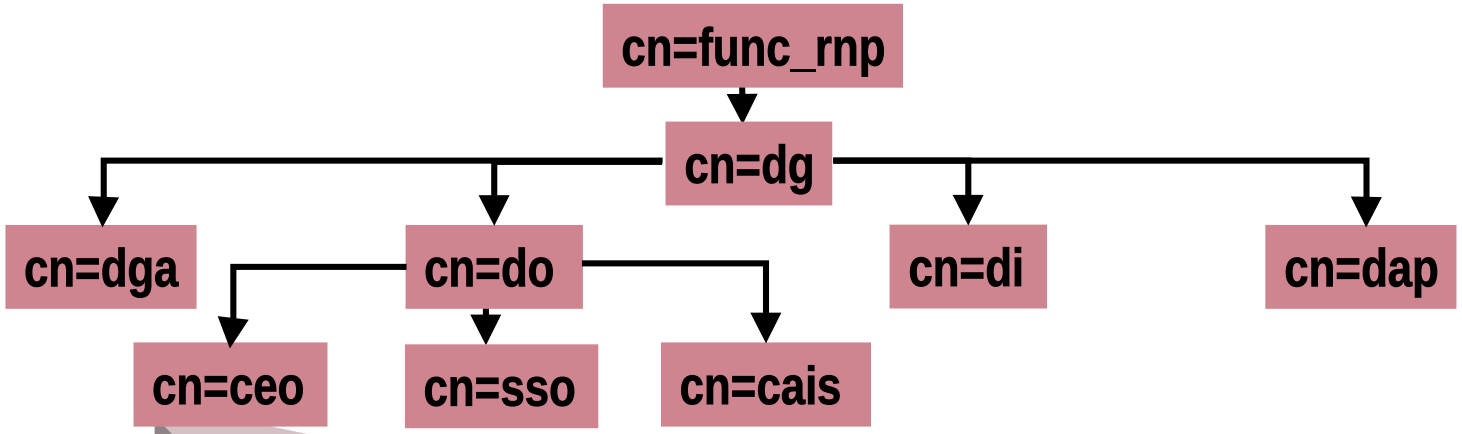
Utilização de Diretório (LDAP)

- Banco de dados especializado para armazenamento de informações em uma organização
- Principal suporte para a maioria dos serviços de *middleware*
- LDAP - Lightweigh Directory Access Protocol:
  - Protocolo para acesso a informações de diretório
  - Suporta TCP/IP

Estrutura do diretório da Intranet

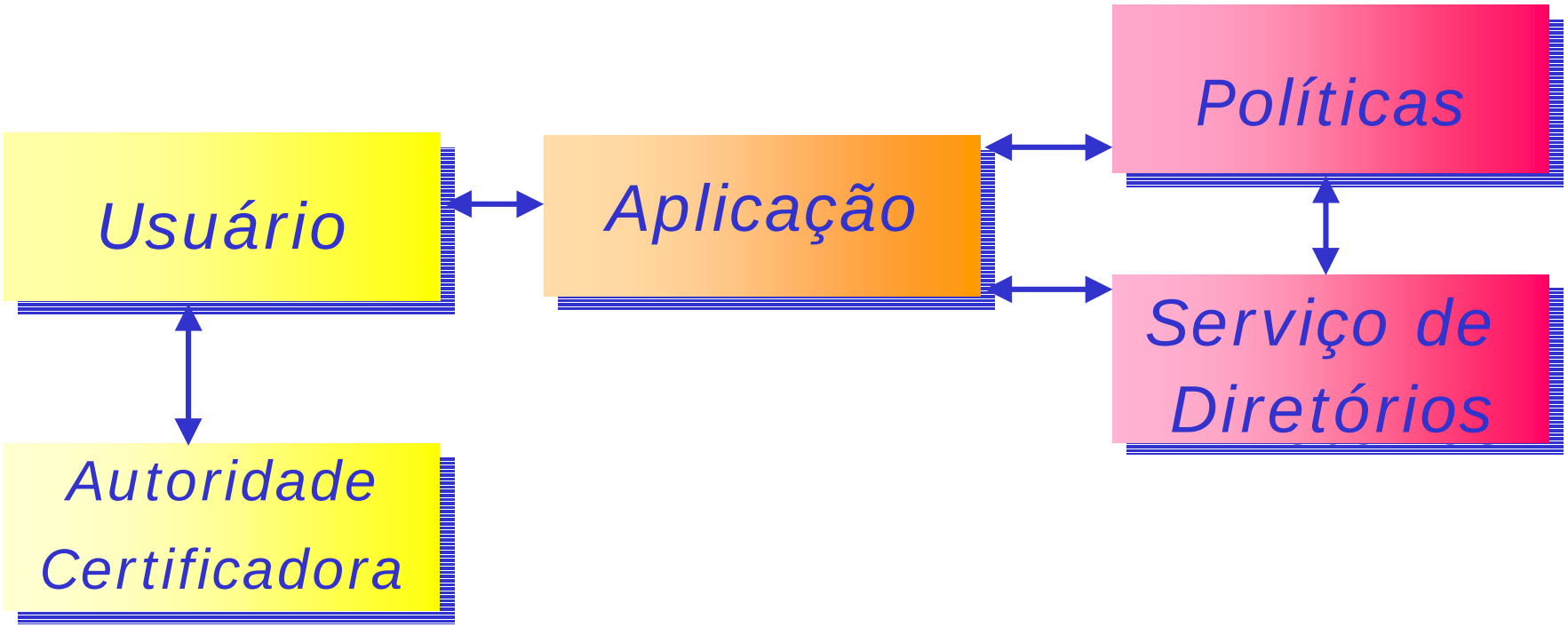


Estrutura do diretório da Intranet




```
dn: cn=ceo, ou=intranet,o=rnp.br
objectclass: groupofuniquenames
cn: ceo
givenname: Centro de Engenharia e Operações
ou: intranet
uniquemember: uid=ari@rnp.br, ou=intranet, o=rnp.br
uniquemember: uid=cybelle@rnp.br, ou=intranet, o=rnp.br
```

Visão geral:


Usuário
Aplicação
Políticas
Serviço de Diretórios
Autoridade Certificadora

Autenticação e autorização na Intranet:

HEPKI: Higher Education PKI

- Esforço conjunto das organizações CREN, Educase/Net@EDU e Internet2 para apoiar o desenvolvimento de PKI para a comunidade científica

- Grupos de trabalho:
  - PAG – *Policy Activities Group*
    - Define como uma CA deve operar
  - TAG – *Technical Activities Group*
    - Pesquisa nas escolas envolvidas sobre estado atual da utilização de ferramentas relacionadas a PKI
    - Aspectos técnicos tais como:
      - Utilização de código aberto ou soluções comerciais para CA
      - Portabilidade de certificados: *smartcards*

- Formas de trabalho:
  - Conferências
  - Troca de email

Situação Atual das Iniciativas da Internet2 (cont.)

EduPerson

- Projeto para definição de uma classe de objetos padrão para um LDAP corporativo da comunidade científica
- Facilitar intercâmbio de aplicações e recursos entre instituições
- Suporte de várias universidades: Wisconsin, Georgetown, Washington, MIT
- Estado atual:

  - Versão eduPerson 1.0 lançada em fev.2001

```
objectclasses: ( 1.3.6.1.4.1.5923.1.1.2
   NAME 'eduPerson'
   SUP  'inetOrgPerson'
   MAY ( eduPersonAffiliation $ eduPersonNickname $
         eduPersonOrgDN $ eduPersonOrgUnitDN $
         eduPersonPrimaryAffiliation $ eduPersonPrincipalName $
        )
```

LDAP Recipe

- Recomendações para configuração e operação de diretórios LDAP
- Garantir que os diretórios sejam configurados e povoados obedecendo a um esquema comum
- Algumas recomendações:
  - Esquema de nomes: dc (*domain component*)
  - Usar eduPerson
  - Usar atributos padrões
  - ...

DoDHE

Situação Atual das Iniciativas da Internet2 (cont.)

DoDHE

- *Directory of Directories for Higher Education*
- Pesquisa e desenvolvimento de um serviço para *directory searching* (*"Web of People"*)
- Não deve impor restrições à política de cada instituição
- Ênfase na cooperação com iniciativas similares
- Problemas a resolver:
  - Crescimento da comunidade Internet2
  - Clientes LDAPv2

Situação Atual das Iniciativas da Internet2 (cont.)

Shibboleth

- Projeto para criação de um serviço para autenticação e autorização na Web
- O problema:
  - Disponibilizar um recurso WWW usando credenciais das respectivas instituições
- Produto principal:
  - Módulo para o *Apache Web Server* que requisita autenticação e autorização remota
- Produtos *open source*

Propostas da RNP

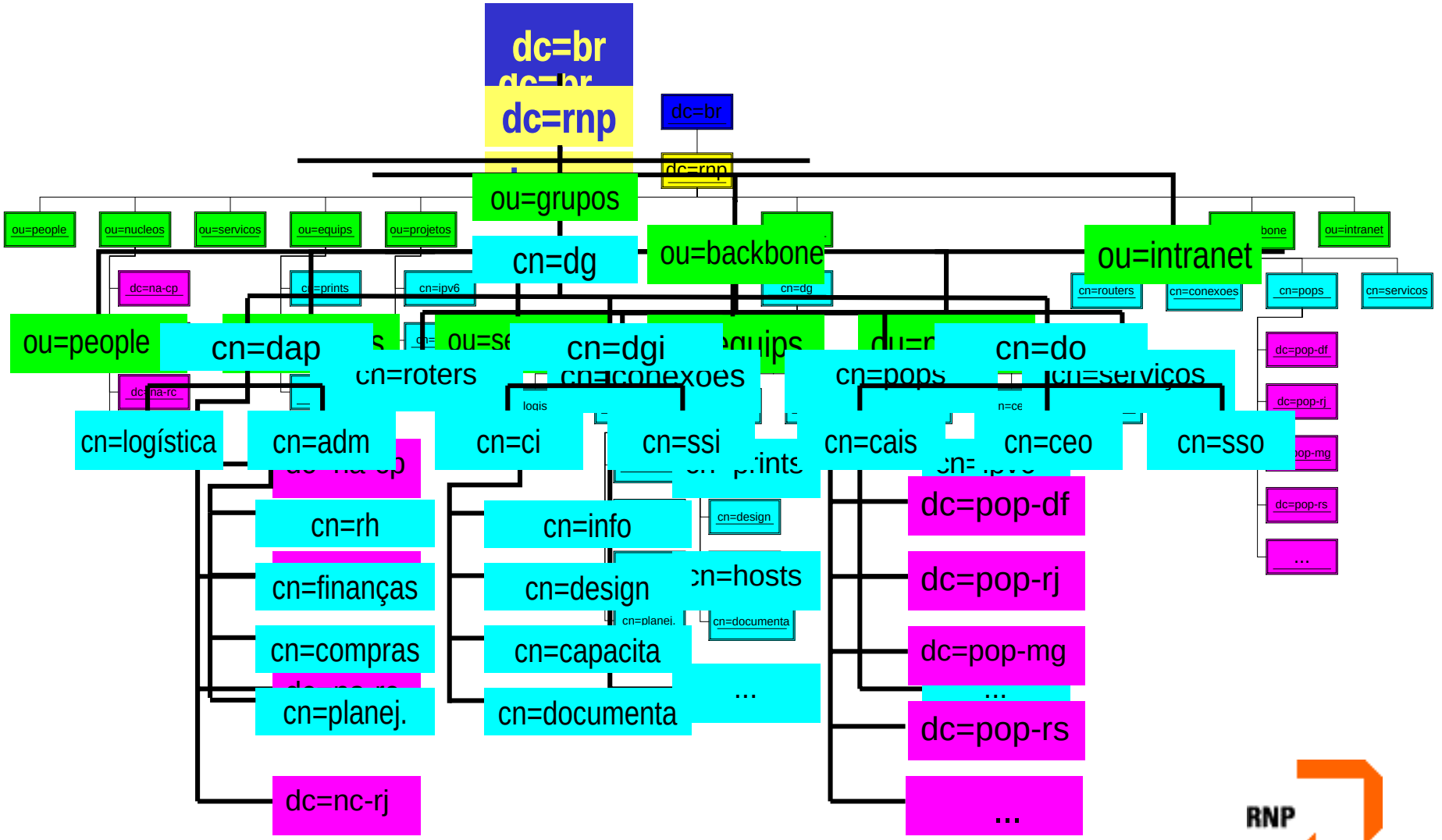
- Projeto Serviço de Diretórios:

  - Estudar os padrões vigentes, levando-se em conta as tentativas internacionais e padronização dos atributos de usuários

  - Definir uma árvore de diretório LDAP para a RNP e implantar um serviço de diretórios na RNP

  - Propor um modelo de dados para diretório LDAP da comunidade de pesquisa

Propostas da RNP



Propostas da RNP

- Iniciativa nacional de PKI para a comunidade de pesquisa:

"Participation in the middleware arena will achieve high visibility and technology return, given that this area will enable the applications of the "next generation Internet" for usability between corporations as well as consumers. We believe this area of development may actually be the enabler of Internet technologies to the masses, and is likely to be a very hot area of research and development in the next 2 to 3 years."

http://middleware.internet2.edu