Identidade, Privacidade e Autorização

Federações e Organizações Virtuais

Noemi Rodriguez
PUC-Rio
noemi@inf.puc-rio.br

FORUMRNP | e-Saúde dias 2 a 4 de setembro de 2014 | Hotel San Marco | Brasília | DF

Gestão de Identidade

- autenticação e autorização
- certificados garantem que usuário é aquele que diz ser
  - confidencialidade
  - não repudiação

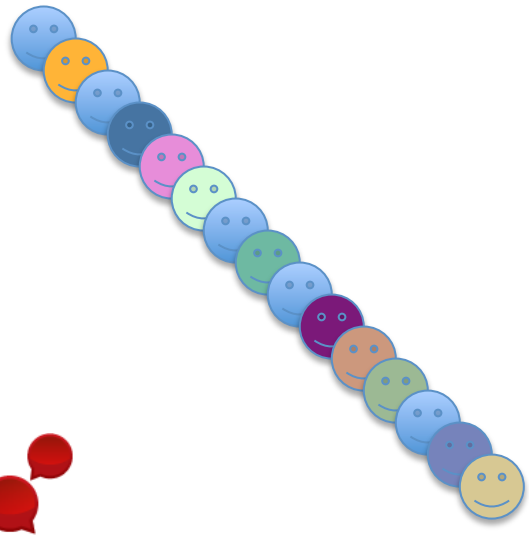
  - mas será que sempre queremos que se saiba quem é o usuário...?

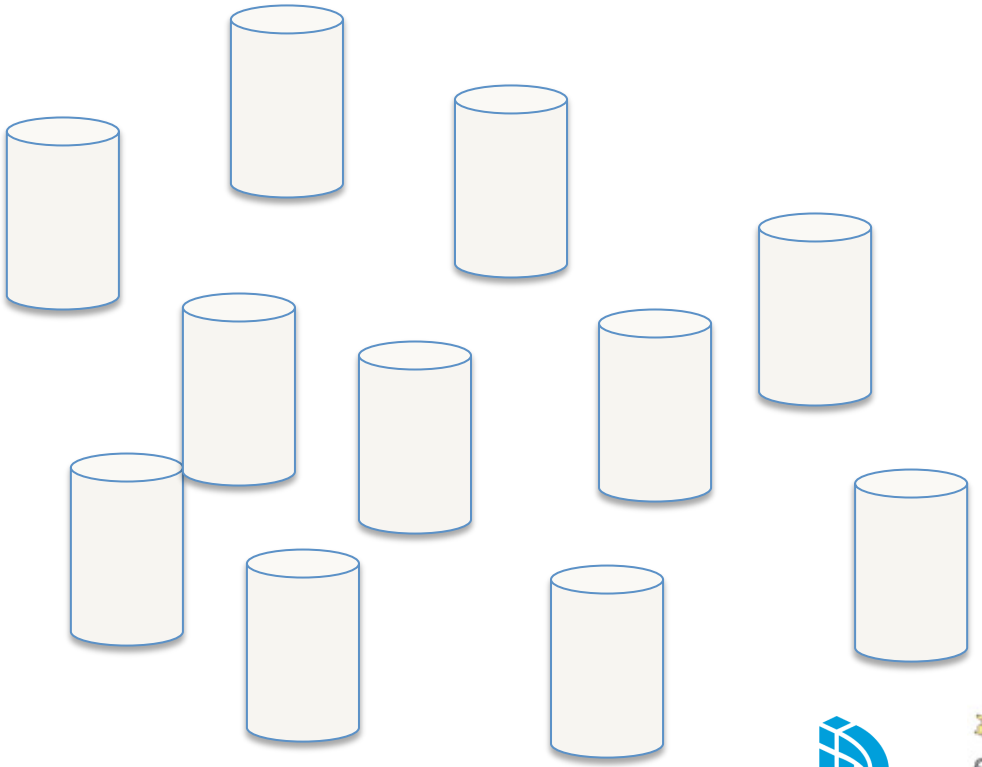
sobrecarga

- sistemas usados por muitos usuários precisam conhecer TODOS?
  - descontos para estudantes e professores

autorizações individuais

- mapeamento de identidade a direitos
- dificuldades de gerenciamento
  - escala
  - manutenção



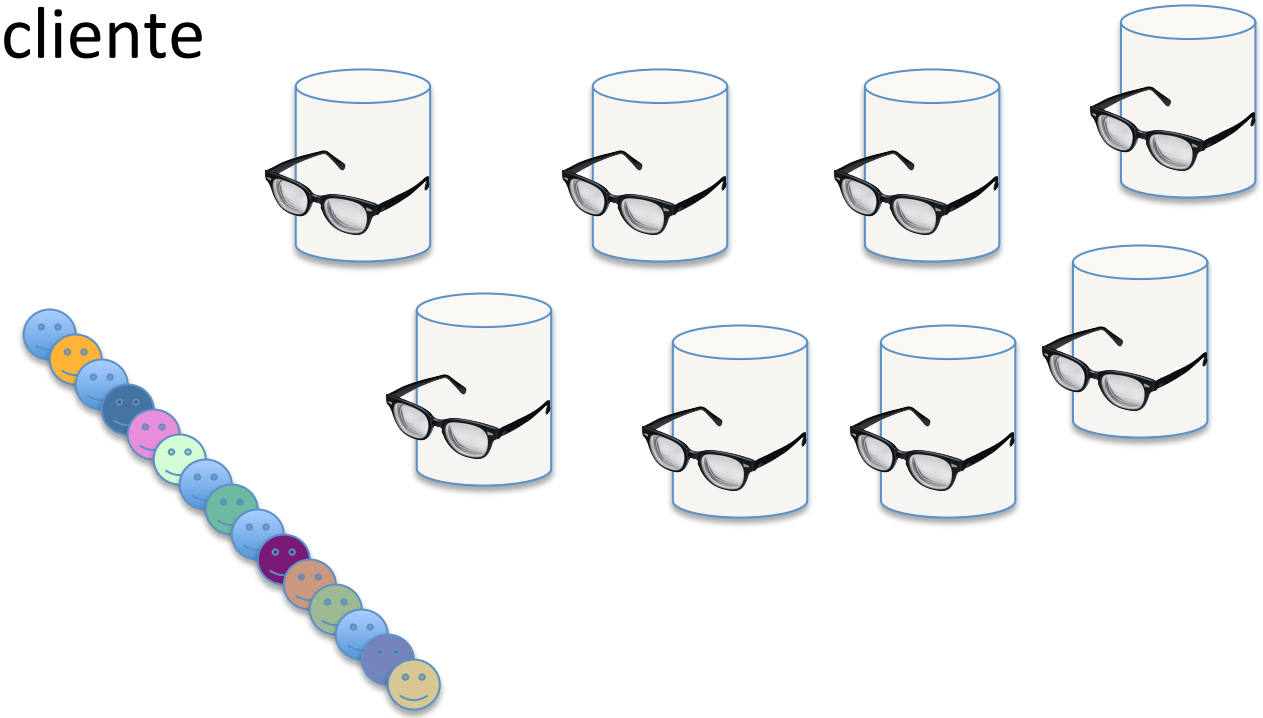


necessidade de privacidade

- para usuário, muitas vezes não é interessante ter que revelar identidade para obter autorização
  - paciente que quer participar de pesquisa sem sofrer retaliação ou preconceito
  - médico que quer consultar prontuários antigos para comparar casos

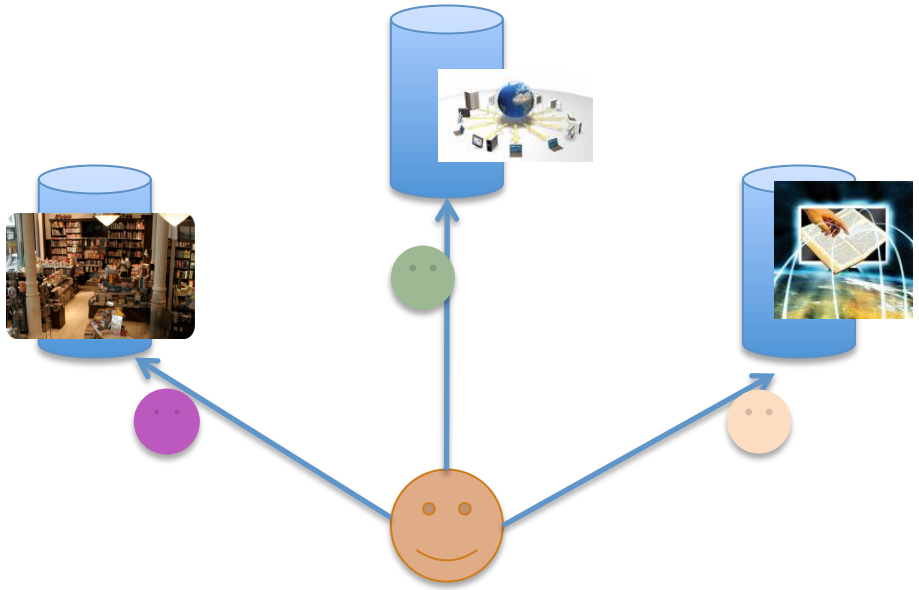
autorizações individuais

- privacidade
  - cada serviço conhece TODAS as requisições de cada cliente

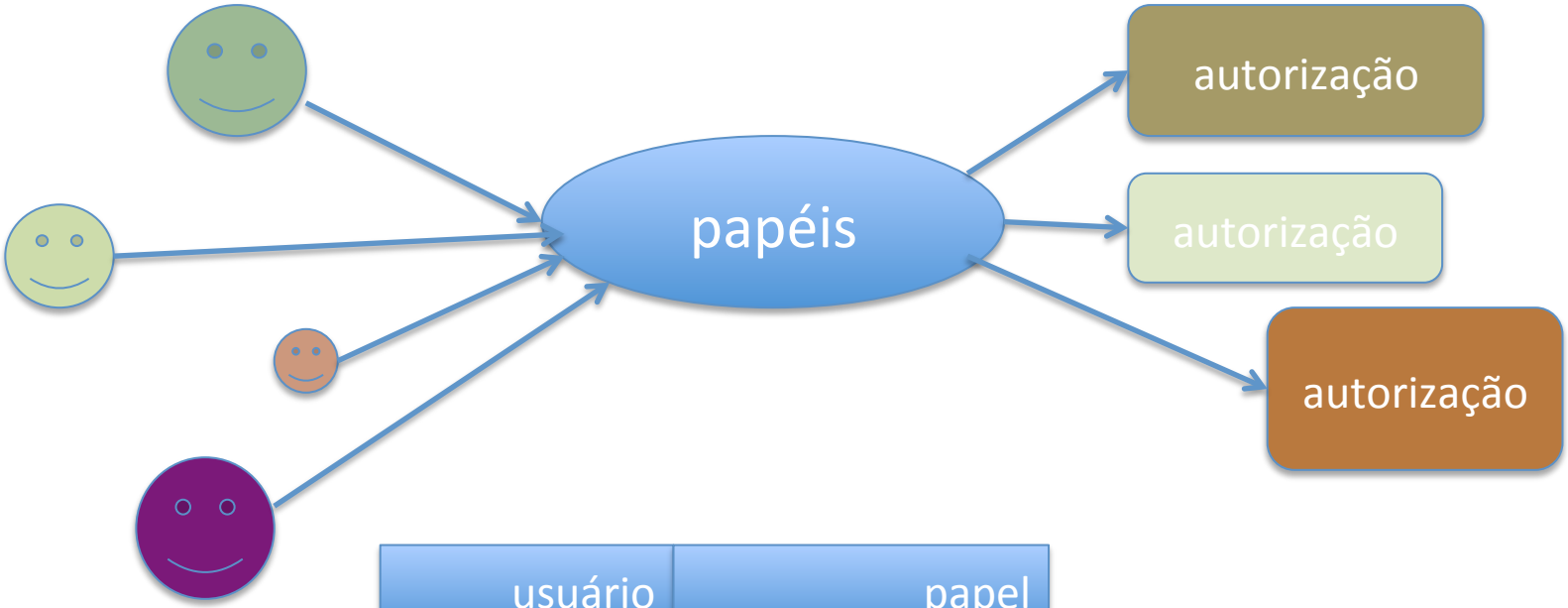


autorização baseada em papéis

- usuários e papéis
  - estudante
  - membro de comunidade (depto, organização, ...)
  - diretor de departamento
  - ...



autorização baseada em papéis



usuário	papel
fulano	professor
sicrano	estudante

RBAC e ABAC

- autorização baseada em papéis:
  - usuário pode assumir papéis diferentes em momentos diferentes
  - modelo um pouco complexo
- autorização baseada em *atributos*:
  - modelo mais estático onde atributos determinam privilégios

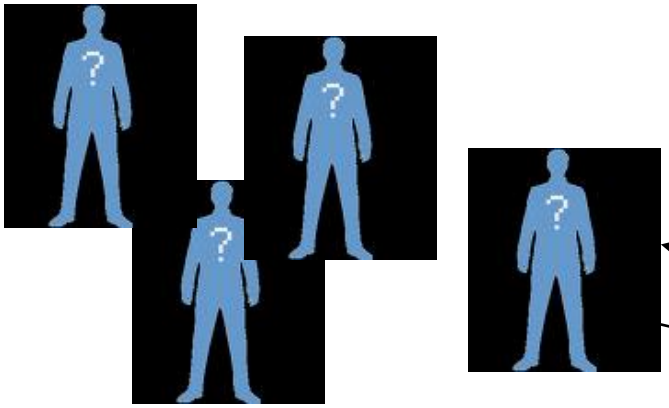
como implementar

- certificados de atributos - ACs
  - certificado garante que usuário tem determinada propriedade
    - normalmente indicado para atributos de vida longa
      - graduado na instituição abc?
- assertivas sobre atributos - federações
  - entidade fornece informações sobre usuário em tempo real
    - atributos de vida curta
      - matriculado em disciplina xyz?

federações de a&a

- autenticação de usuário por *provedor de identidade*
- *provedor de serviço* recebe uma garantia de autenticação
- provedor de serviço pode requisitar *atributos* do usuário para controle de acesso
  - relação com papéis
  - preocupação com privacidade

federações de a&a



provedores de identidade

autenticação
atributos

serviço

rede de confiança entre provedores de serviço e provedores de identidade!!

federações acadêmicas

- redes de confiança:
  - universidades e outras instituições de ensino e pesquisa
    - atuação como provedores de identidade e como provedores de serviço
  - editoras e outras
    - atuação como provedor de serviço

exemplo serviço CAFe: atlas de imagens histológicas de alta resolução
atlases.muni.cz

➢ certificados garantem comunicação entre parceiros nessas redes!

federações - evolução

- soluções iniciais: protocolos próprios para comunicação entre provedores de serviço e provedores de identidade

- evolução para padronização: SAML

- diversas implementações baseadas ou compatíveis com SAML
  - shibboleth (Internet2)
  - simplesaml
  - outros...

privacidade

- provedor de serviço deve receber o mínimo de informação necessário para estabelecer direitos de acesso
  - “estudante da U1”
  - “professor aposentado da U2”
  - ...
- acordos entre provedores de serviço e provedores de identidade para liberação de atributos
- controle por usuário

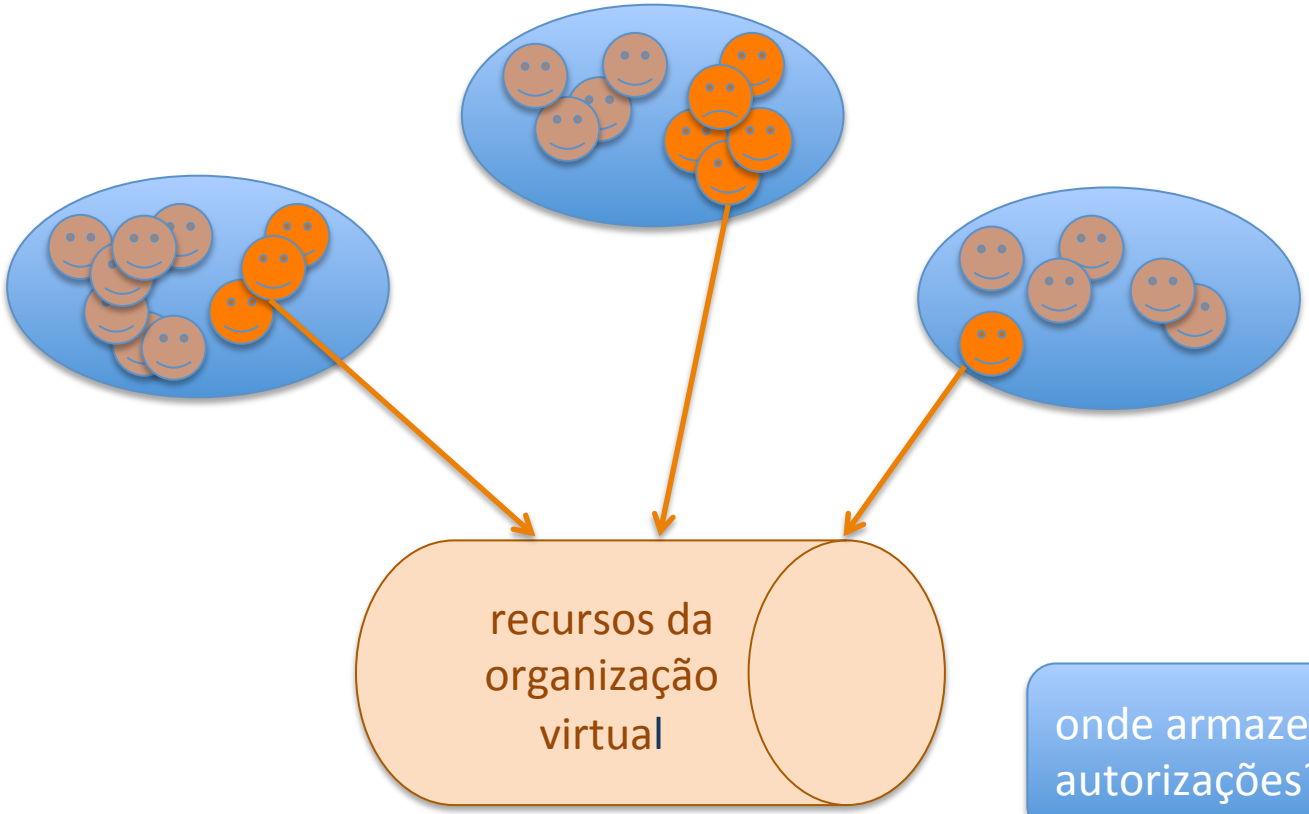
quem emite atributos?

- federações tradicionais:
  - provedores de identidade e de atributos são a instituição do usuário

cada entidade só deve emitir atributos sobre os quais tem autoridade

- como tratar projetos interinstitucionais?
  - conceito de *organização virtual*

organizações virtuais



onde armazenar essas autorizações?

implementação de OVs

- um novo IdP pode ser criado para cada OV...

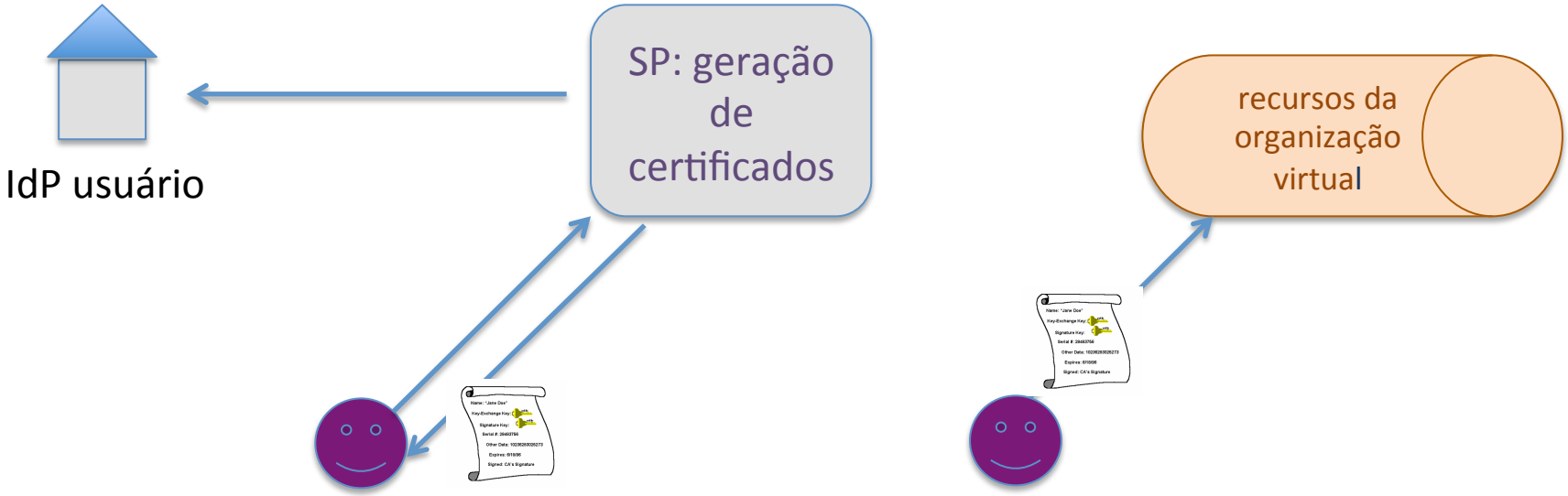
  - atualizações cadastrais em mais um ponto
  - novo conjunto de credenciais
  - dificuldade de capturar dependência com outros dados

implementação de OVs

- certificados gerados por um serviço "intermediário" podem ser usados para acessar recursos da OV

  - uso extensivo dessa solução na área de grids computacionais

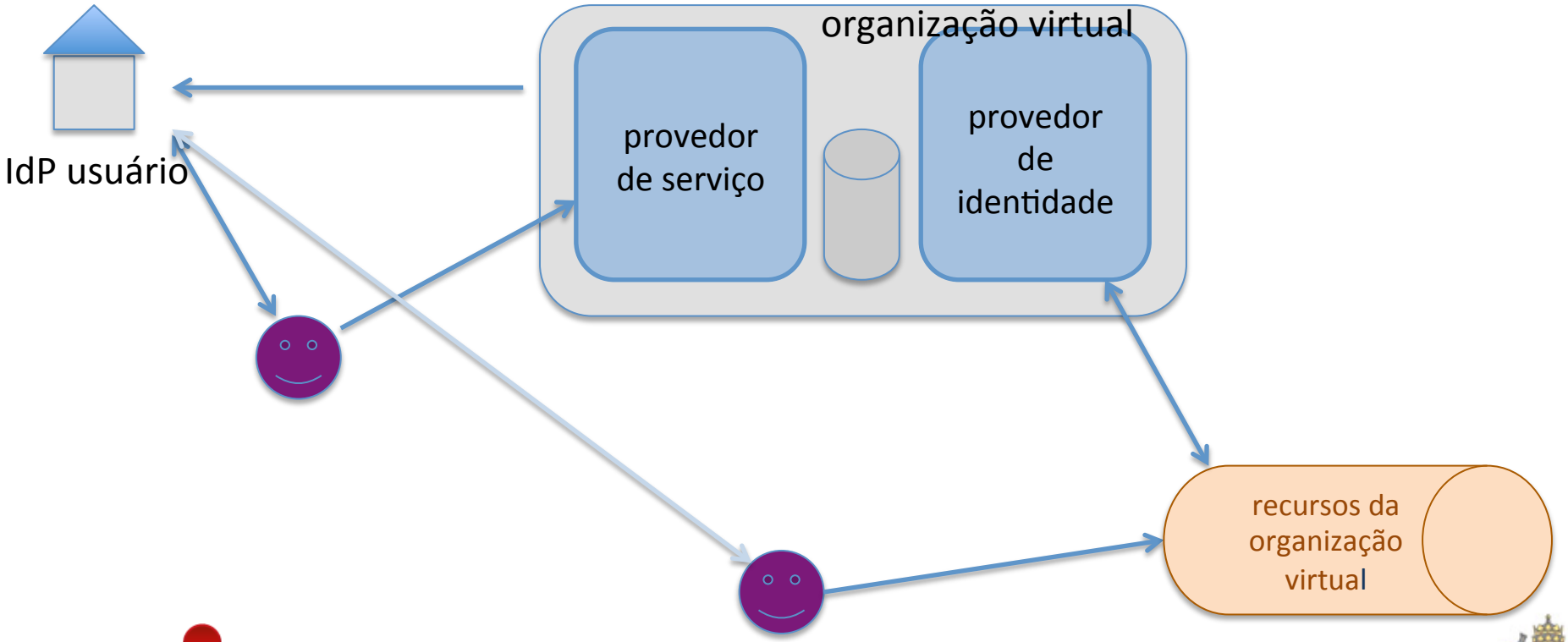
serviços geradores de certificados



- possível processo externo de registro de usuário junto a serviços de OV

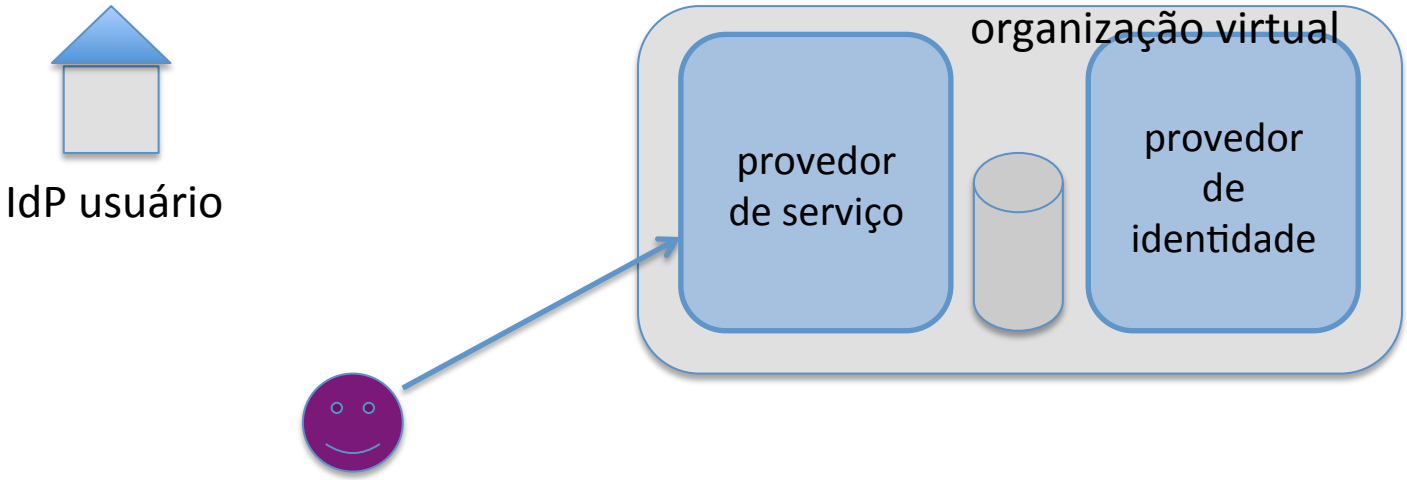
organizações virtuais

- soluções ainda em evolução



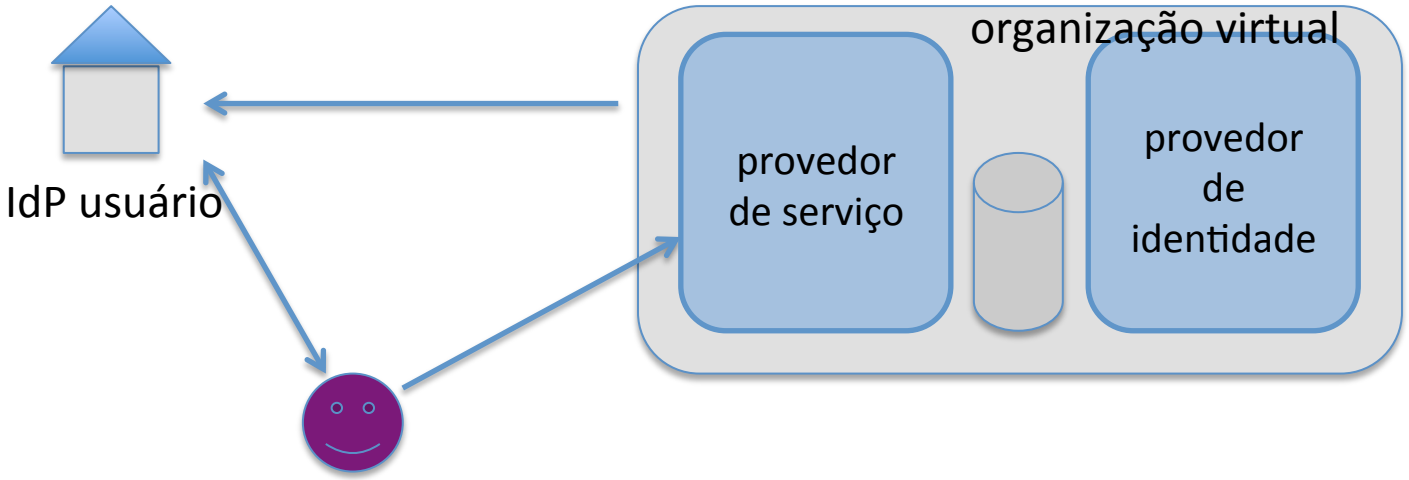
organizações virtuais

- soluções ainda em evolução



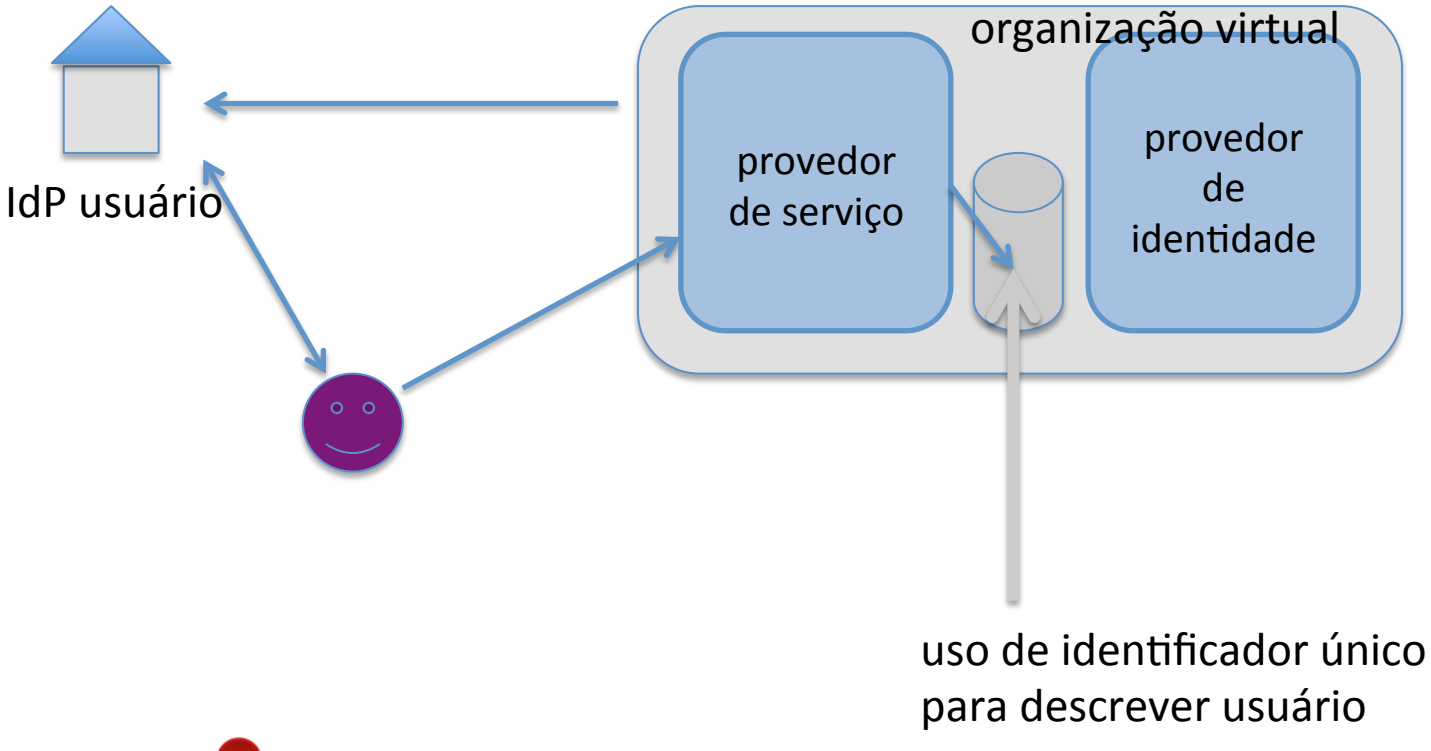
organizações virtuais

- soluções ainda em evolução



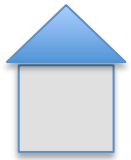
organizações virtuais

- soluções ainda em evolução

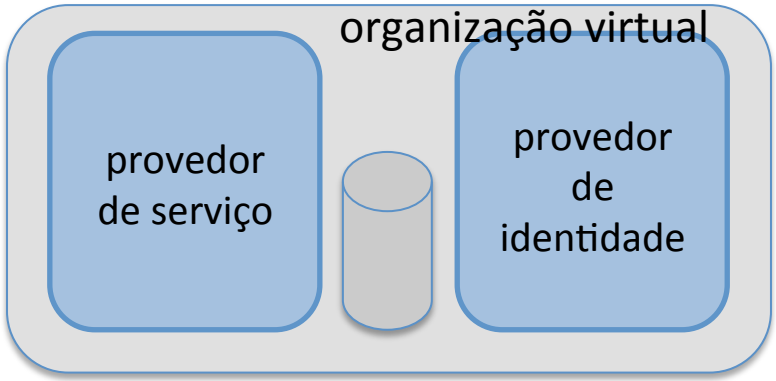


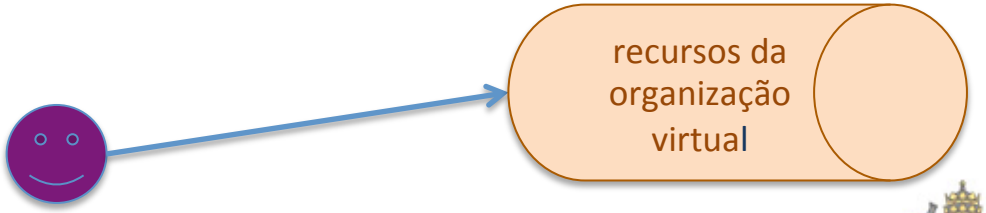
organizações virtuais

- soluções ainda em evolução



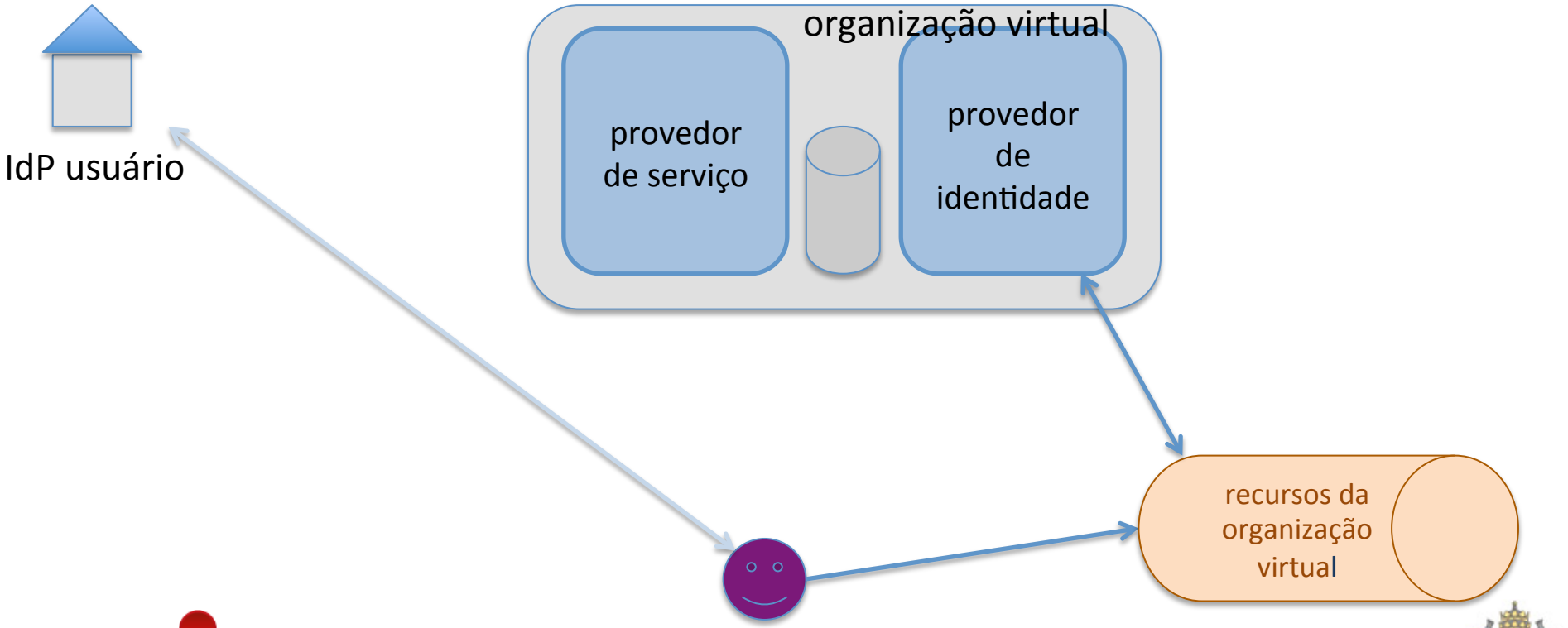
IdP usuário





organizações virtuais

- soluções ainda em evolução



organizações virtuais

- ênfase em conveniência de uso
  - ferramentas de gerência de grupos, convites, etc
  - sem necessidade de suporte de TI

  - fundamentais para colaboração!

- desafios
  - gestão e padronização de atributos

Identidade, Privacidade e Autorização

Federações e Organizações Virtuais

Noemi Rodriguez
PUC-Rio
noemi@inf.puc-rio.br

FORUMRNP | e-Saúde dias 2 a 4 de setembro de 2014 | Hotel San Marco | Brasília | DF