Digital Identity Management and RNP

Noemi Rodriguez

RNP, PUC-Rio
RNP (Rede Nacional de Ensino e Pesquisa): non-profit private organization
  ▶ under contract by Brazilian government to manage national academic network
  ▶ more than 300 connected organizations
    ▶ around 130 universities
    ▶ 30 private and public research centers
RNP Activities

- network infrastructure
- services
- research and development:
  - fostering the use of new technologies
- training
Network infrastructure: the Ipe backbone

- hybrid architecture, supporting routed IP and e2e circuit traffic
- last mile: optical metropolitan networks
RNP Services

- voice over IP
- webconf
- video streaming
- video distribution
- federated authentication
- public key infrastructure
- ...
New Technologies

- advanced networking
  - tools for hybrid architectures
  - testbeds for protocols and network technologies
- middleware
  - basic services: authentication and authorization, circuit reservation, ...
  - building blocks for other applications
- applications
  - education and research-related network-based applications
Working Groups

- RNP has lifelong informal collaboration with academic community
- formal WG program started in 2002
- open call once a year
- surveyed or developed technologies may lead to services offered by RNP
  - fone@rnp
  - video services
  - distance learning tools
  - authentication and authorization
Efforts in Digital Identity

- working groups on identity-related issues started in 2002
- currently two RNP services for research and higher ed organizations:
  - ICPEDU – PKI
  - CAFe – federated authentication and authorization
- role of RNP (www.rnp.br/servicos/):
  - dissemination
  - management of centralized parts of service/procedures
  - support for institutions wishing to adhere
- software and hardware developed in WG program
  - hardware is currently used also in ICP-Brasil
- root authority maintained in UFSC
- CAs are universities and research centers (20)
- certificate emission at no cost
- main applications:
  - email
  - electronic signature
  - SSL
  - electronic forms
  - grids: brgridca.ic.uff.br
CAFe – Comunidade Acadêmica FEderada

- applications
  - integrated learning programs (multi-institutional)
  - access to digital libraries
- exchange of SAML assertions
  - authentication at home institution
  - predefined attributes released to service for authorization
- ideas from Incommon and european federations (refeds)
- recommended configuration for internal data organization
  - large number of institutions with little technical expertise
CAFe recommended configurations

- use of shibboleth software
- authentication and attribute data from LDAP repositories
  - brEduPerson schema for LDAP
  - tools for populating LDAP with institutional data
brEduPerson schema

- Object classes: inetOrgPerson, brPerson, schacPersonalCharacteristics
- Attributes:
  - uid: S12345678
  - brcpf: 12345678900
  - brpassport: A23456
  - schacCountryOfCitizenship: Brazil
  - telephoneNumber: +55 22 81389199
  - Mail: silvana@...
  - homePostalAddress: ...
  - cn: Silvana
  - cn: Silvana Rossetto
  - sn: Rossetto
  - userPassword: silvana
  - schacDateOfBirth: 19000523
  - schacGender: 2

- EduUsers:
  - braff: 01, uid=S12345678, ou=people, dc=uff, dc=br
    - braff: 01
    - brafftype: student
    - brEntranceDate: 20070205
  - braff: 02, uid=S12345678, ou=people, dc=uff, dc=br
    - braff: 02
    - brafftype: faculty
    - brEntranceDate: 20070205
    - braff: 02
    - brafftype: student
    - brEntranceDate: 20070205

- EduVoIP:
  - brvoipalias=2345, uid=S12345678, ou=people, dc=uff, dc=br
    - brvoipalias: 2345
    - brEduVopIPtype: celular
    - brEduVopIPadmin: uid=A34344340, ou=people, dc=uff, dc=br
    - brEduVopIPcallforward: +55 22 3418 9199
    - brEduVopIPaddress: 200.157.0.333
    - brEduVopIPexpiryDate: 20081030
    - brEduVopIPbalance: 295340
    - brEduVopIPcredit: 300000

- EduVoIP:
  - brvoipalias=5020, uid=S12345678, ou=people, dc=uff, dc=br
    - brvoipalias: 5020
    - brEduVopIPtype: pstn
    - brEduVopIPadmin: uid=A34344340, ou=people, dc=uff, dc=br
    - brEduVopIPcallforward: +55 22 3418 9199
    - brEduVopIPaddress: 200.157.0.333
    - brEduVopIPexpiryDate: 20081030
    - brEduVopIPbalance: 295340
    - brEduVopIPcredit: 300000
Current Status

- ICPEDU and CAFé in operation as services from 2010
- around 15 organizations using each service
  - challenge: dissemination
- evolution
  - technical committee: discussion of directions in identity management
Some current issues

- integration of trust infrastructures
  - federations: edugain
- virtual organizations: multiple sources of attributes
  - attribute certificates?
  - attribute aggregation
- working group: integration of different authentication frameworks
  - specific case: bridges such as CILogon
- pilot: eduroam
Thanks!

noemi@inf.puc-rio.br