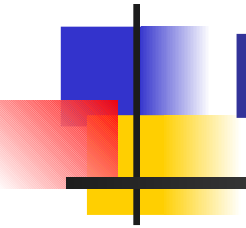
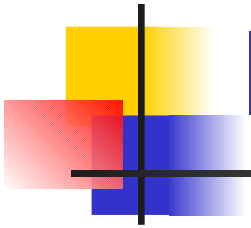


Kerberos and Identity Federations

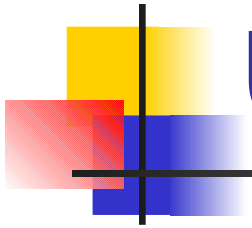
Daniel Kouřil, Luděk Matyska,
Michal Procházka, Tomáš Kubina

AFS & Kerberos Best Practices Worshop 2008



Identity Federations

- linking services and user management systems
  - standardized protocols
  - home institution keeps the most current data
  - service & identity providers
- services trust clients‘ institutions
  - modified trust model
- suitable for large infrastructure
  - possible decreasing of users‘ credentials
- Shibboleth



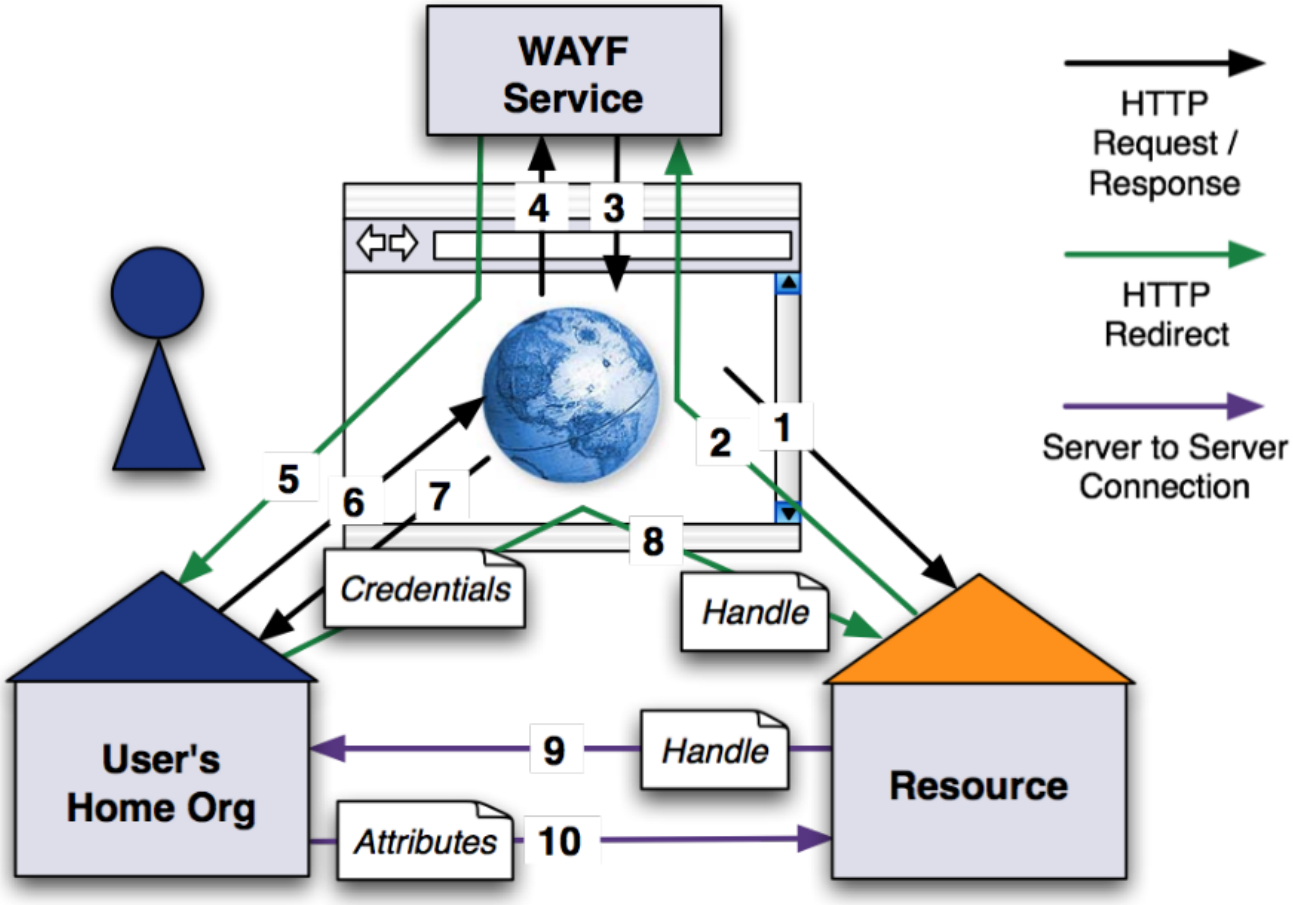
Users‘ attributes

- Additional information published by IdP
  - up-to-date
  - any information from HR databases
    - name, email, affilitation, ...
- allows for sophisticated access control policies
  - groups of students of a course, ...
- pseudoanonymity
- Security Assertion Markup Language

SAML assertion example

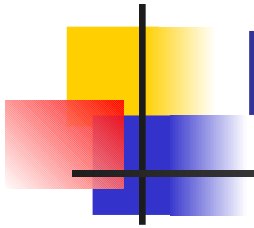
urn:mace:dir:attribute-def:cn	Daniel Kouřil
urn:mace:dir:attribute-def:givenName	Daniel
urn:mace:dir:attribute-def:sn	Kouřil
urn:mace:dir:attribute-def:o	Masarykova univerzita
urn:mace:dir:attribute-def:ou	Wplace-31200;Wplace-924000;Facult-1433
urn:mace:dir:attribute-def:eduPersonPrincipalName	1388@muni.cz
urn:mace:dir:attribute-def:eduPersonAffiliation	member;student; employee
urn:mace:dir:attribute-def:mail	1388@mail.muni.cz
http://www.mefanet.cz/mefaperson/	false

Federations in web world

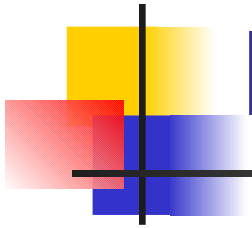


schema from SWITCH AAI

Federation in non-web world



- no redirect mechanism
- PKI and federated certificates
  - transporting IdP‘s assertions
- VPN-based solution as general infrastructure
- obtaining certificates
  - explicit logging into federation

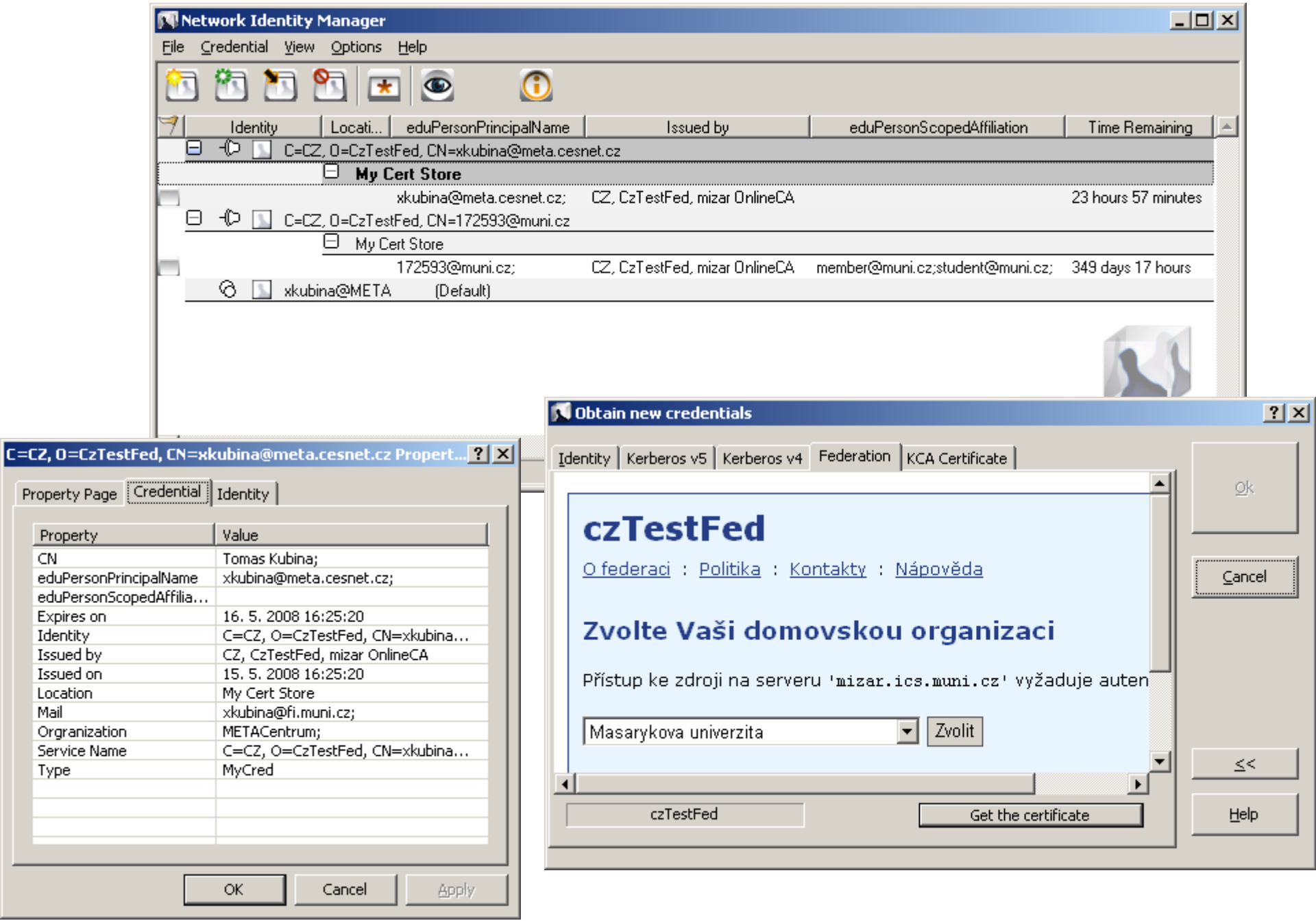


Federated CA

- bridge to non-federative services
- on-line CA running as SP in federation
  - federation-based identity vetting
  - GridShib CA
- key & certificate management done by browser
- certificates contain users attributes
  - X.509 extension

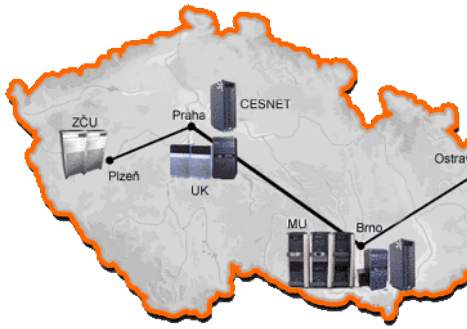
Management of certificates

- browser-based solution not ideal
- GUI and framework desired
  - Network Identity Manager
  - extensible by plugins
- plugin to manage certificate in MS CertStore
  - embedded browser to obtain certificate
- pilot implementation ready
  - scheduled deployment at computer center at MU
- limitation of single identity provider in NIM


Network Identity Manager
File Credential View Options Help
Identity Locati... eduPersonPrincipalName Issued by eduPersonScopedAffiliation Time Remaining
C=CZ, O=CzTestFed, CN=xkubina@meta.cesnet.cz
My Cert Store
xkubina@meta.cesnet.cz; CZ, CzTestFed, mizar OnlineCA 23 hours 57 minutes
C=CZ, O=CzTestFed, CN=172593@muni.cz
My Cert Store
172593@muni.cz; CZ, CzTestFed, mizar OnlineCA member@muni.cz;student@muni.cz; 349 days 17 hours
xkubina@META (Default)
C=CZ, O=CzTestFed, CN=xkubina@meta.cesnet.cz Propert...
Property Page Credential Identity
Property Value
CN Tomas Kubina;
eduPersonPrincipalName xkubina@meta.cesnet.cz;
eduPersonScopedAffilia...
Expires on 16. 5. 2008 16:25:20
Identity C=CZ, O=CzTestFed, CN=xkubina...
Issued by CZ, CzTestFed, mizar OnlineCA
Issued on 15. 5. 2008 16:25:20
Location My Cert Store
Mail xkubina@fi.muni.cz;
Orgranization METACentrum;
Service Name C=CZ, O=CzTestFed, CN=xkubina...
Type MyCred
OK Cancel Apply
Obtain new credentials
Identity Kerberos v5 Kerberos v4 Federation KCA Certificate
czTestFed
O federaci : Politika : Kontakty : Nápověda
Zvolte Vaši domovskou organizaci
Přístup ke zdroji na serveru 'mizar.ics.muni.cz' vyžaduje auten
Masarykova univerzita Zvolit
czTestFed
Get the certificate
Ok
Cancel
<<
Help

Kerberos and federations

- many identity federations emerging
  - local NRENs in Europe
- METACentre project in CR
  - serving users from many institutions
  - Kerberos
- Easy access for new users
  - at least from selected institution
  - registration and further access
- Utilizitation of federations



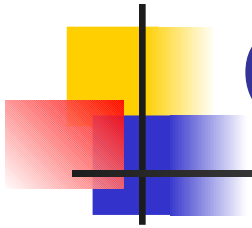
Kerberos and federations

- several ways possible
  - KAML group
- no changes to infrastructure, easiness of use for end-users
  - authorization data field for SAML
  - transformation of federated certificates to tickets
- PKINIT + KDC modified to retain SAML
  - simple, easy to implement
  - SAML is copied from X.509 to TGT as authZ data
    - all derived tickets will inherit the assertion
- Similar to MS PAC
  - not signed currently
  - SAML artifacts

SAML on Application Server

- authorization based on SAML attributes
  - policy language
- authZ decision made by application or third-party component
  - XACML Query/Response protocol
  - components from Grid world „available“

```
krb5_recvauth (....);
krb5_ticket_get_authorization_data_type(
    context,
    ticket,
    KRB5_AUTHDATA_SAML,
    &saml_data);
process_saml_data(saml_data);
```



Conclusion

- Simple integration easy to done
  - KDC, users-side tools, application server-side code & authZ service
  - Kerberos as transport mechanism
- NIM plugin
  - logging into federations
  - useful for other environment as well
    - collaborative systems, videoconferencing