Framework for non-Web application integrations
CAT

Michal Procházka, Daniel Kouřil, Tomáš Kubina
Masaryk University in Brno
Outline

- Introduction
- SSO options
  - PKI
  - Kerberos
  - Federation
- CAT
  - Credential transformation
  - Network Identity Manager
  - Sample applications
- Demo
Introduction

- More and more services are deployed in the campuses
- Services require authN/authZ
  - Personalization
  - Consumes personal data
- Services in different domains => different authN mechanisms
- We want SSO ...
Deploying new service (SSO)

- Service supports authN mechanism used in the campus
- or
- Service needs to be extended to support that authN mechanism
- or
- Keep service as is and equip users with authN credential which is supported by the service – automatically by the authN translation
SSO - PKI

- Pros
  - Decentralized management
  - Supported by web servers and other applications
  - Side effect: signing and encryption

- Cons
  - User is required to maintain credentials
  - Need functional infrastructure (CA, RA, CRL, …)
SSO - Kerberos

Pros
- Centralized management
- Used in Microsoft domain system
- Easy to use by the users

Cons
- Centralized management
- Closed infrastructure
- Not widely supported by the applications
SSO - Federation

- **Pros**
  - No changes required on the client side
  - Easy to deploy on the service side
  - Connected to the IdM

- **Cons**
  - Centralized management of the Metadata
  - Supported only in the web environment
Credential transformation

- Kerberos ticket → X.509 certificate
  - Using MyProxy in CA mode
  - KCA
- Federated identity → X.509 certificate
  - Federated OnlineCA
  - Web based
  - Using Internet Explorer and Netscape API to generate keys inside the browser
- X.509 certificate → Kerberos ticket
  - PKINIT
  - Support for MS Windows (Heimdal)
Credential transformation
- Common Access Toolkit
- Set of applications and scripts which eases managing user's credentials
  - Easy to use
  - Support for variety of authN mechanisms/credentials
    - Hides technical aspects of the authN mech. from the user
- Actual version is only for Windows OS
- Will be ported to the Linux and Mac OS
Network Identity Manager 2.x

- Desktop application for managing user's credentials
- It supports any type of credentials (provided by the plugins)
- Manages an identities and associated credentials
- Maintained by Secure Endpoints
- Will be ported to the Linux and Mac OS
Plugins

- **NIM X.509**
  - Creates X.509 proxy certificate from the certificate which is stored in Windows CertStore or on the Smart Card
  - Supports PKINIT – Retrieve Kerberos ticket from KDC
- **NIM Fed**
  - Gets X.509 certificate from federated OnlineCA
  - Generated X.509 certificate contains SAML response from the IdP
  - Stores the certificate into the Windows CertStore
  - Using build-in Internet Explorer
Login script for Windows

- Getting certificate from MyProxy server
  - MyProxy issues new certificate after successful Kerberos authentication
  - It can be integrated with common Windows login to make these steps automatically and transparently from the user
  - New certificate can be stored to the file or to the CertStore
Sample applications

- Web applications supporting PKI
- Aleph – Integrated Library System
- Samba storage from different domains
- OpenVPN
- VNC over Stunnel
Demo

- Getting X.509 certificate from the federated OnlineCA
  - User can choose CA
  - Private/public keys are generated at the client
  - New certificate is stored in the CertStore
- Access Aleph library system
- Access VPN service
Obtain new credentials

Kerberos 5

Federation Certifica...

CA Name:

OnlineCA mizar
CA2
Obtain new credentials

OnlineCA mizar

X509 Certificate Identity


czTestFed

O federaci : Politika : Kontakty : Nápověda

Zvolte Vaši domovskou organizaci

Přístup ke zdroji na serveru 'mizar.ics.muni.cz' vyžaduje autentizaci.

Masarykova univerzita

Zvolit

Uložit tuto volbu do ukončení relace prohlížeče.

Finish  Cancel

Make this the default identity
Conclusion

- NIM 2.x is still under development
- Our goals:
  - Easy to use for the client
  - Integrates several authN mechanisms into the NIM
  - Transparent security for the use
Acknowledgement

The project is funded by Masaryk University, CESNET and CESNET Development Fund (253R1/2007)
Thank you ...