



Easing access to Grids using identity federations

Daniel Kouřil

Terena NREN & Grid Workshop 2008, Dublin



PKI & Grids – what we learnt

- The Grid authentication mechanism
 - A lot of achievements
- Promising principles
 - ... but a lot of details to cope with
 - Revocation checks, private key management, ...
- Security reduced in deployment
 - Easier way of certificate management?



Shibboleth-based Federations

- Linking services and user management systems
 - standardized protocols
 - home institution keeps the most current data
 - services trust clients' institutions
 - eduid.cz in Czech Republic
- SAML assertions
 - Attributes for AuthZ
- suitable for large infrastructures
 - Primarily for web-based applications



Common Access Toolkit for Federations

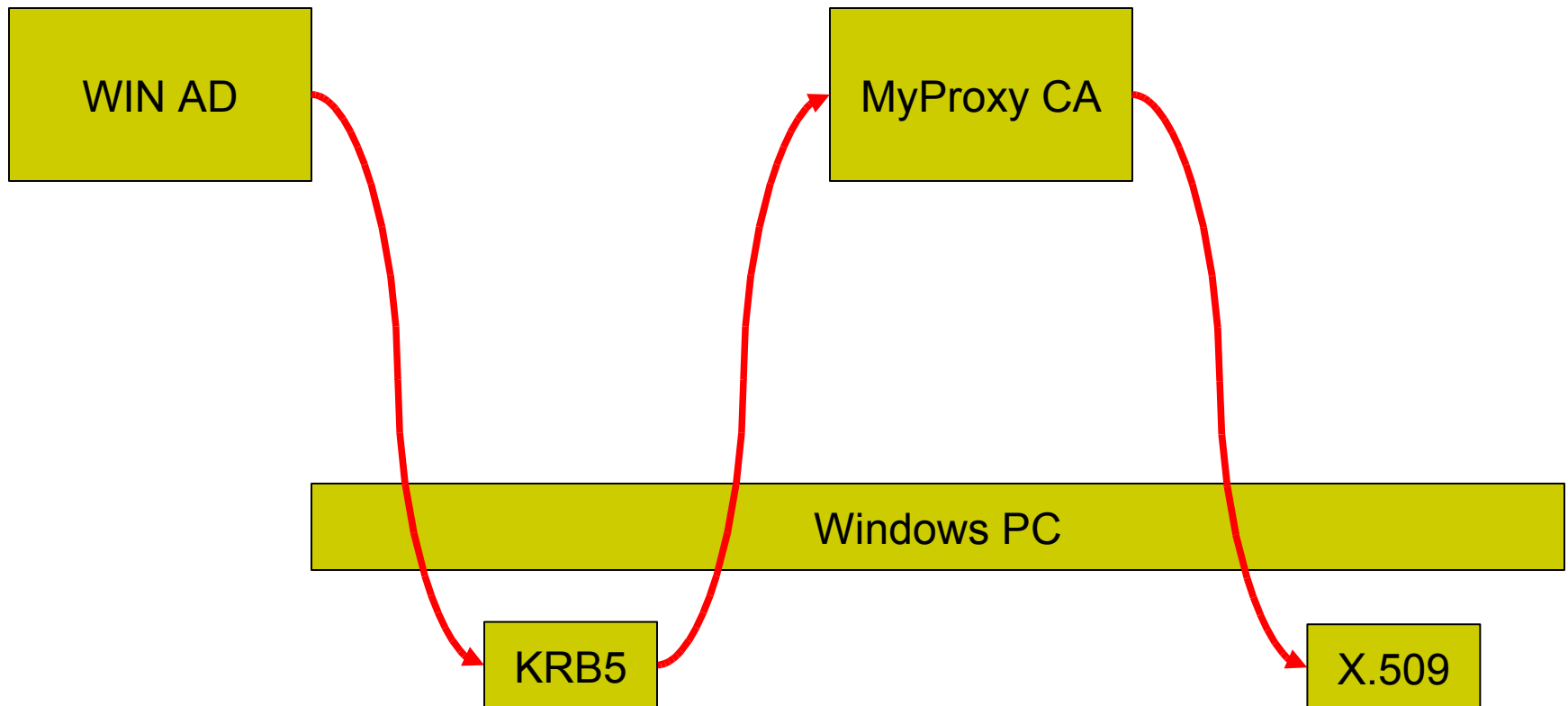
- Project supported by CESNET FD and Masaryk University
- Support for federation concepts in non-web world
 - Collaborative environments
- PKI and „federated“ certificates
 - transporting IdP's assertions
- Framework & user tools
 - OS integration



Transparent PKI at Masaryk University

- University computer hall & faculty facilities
 - Automatical generation of certificates
- Standard Windows authN
 - Kerberos
- Translating mechanism from Kerberos to X.509
 - The same identity, only different format
- Enlarging the SSO area
 - Accessing services without explicit authentication

Credential Translation





Federated CA

- on-line CA running as SP
 - federation-based identity vetting
 - GridShib CA, SWITCH SLCS CA
 - CESNET CA – multiple instances (one to be accredited by IGTF)
- certificates contain users attributes
 - X.509 extension (value or reference)
- key & certificate management done by browser



Management of certificates using CAT

- browser-based solution not ideal
 - No overview of certificates, etc.
- GUI desired
 - Network Identity Manager (NIM)
 - Widely used by Krb5 community
 - extensible by plugins
- Obtaining certificates
 - explicit logging into federation
 - transparently



NIM Plugins

- plugin to manage „federated“ certificates
 - embedded browser to obtain certificate
 - MS CertStore
 - Authentication explicit or transparent
 - Depending on particular CA policy
- Plugin to manage proxy certificates also available
 - Can access CertStore or MyProxy repository

Network Identity Manager

File Credential View Options Help

Identity Location 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 Properties

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;
Organization	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



Conclusion

- Transparent PKI to improve/retain security
 - Focusing on non-web world
- Tools to obtain and manage certificates
 - From both local and federated CAs