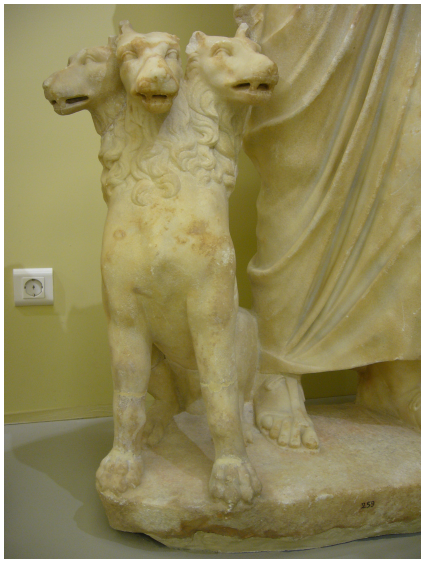
Connecting Web and Kerberos Single Sign On

Rok Papež
ARNES
aaa-podpora@arnes.si

Terena networking conference
Malaga, Spain, 10.6.2009

Kerberos

- Authentication protocol
  - (No) authorization
- Single Sign On (SSO)
- Cerberus
  - Greek and Roman mythology
  - 3 headed dog guarding the gates of Hades
- MIT Project Athena
  - Versions 1-3 internal only
  - Version 4 – 1989 (public software release)
    - DES only, Protocol flaws, End of life
  - Version 5 – 1993 (RFC 1510)
  - GSS-API – Generic security services API
  - IETF Kerberos working group



Kerberos implementations

- MIT Kerberos
  - Krb5-1.6.3
  - Krb5-1.7 beta (22.4.)
  - Most popular
  - Subject to USA cryptography export regulations

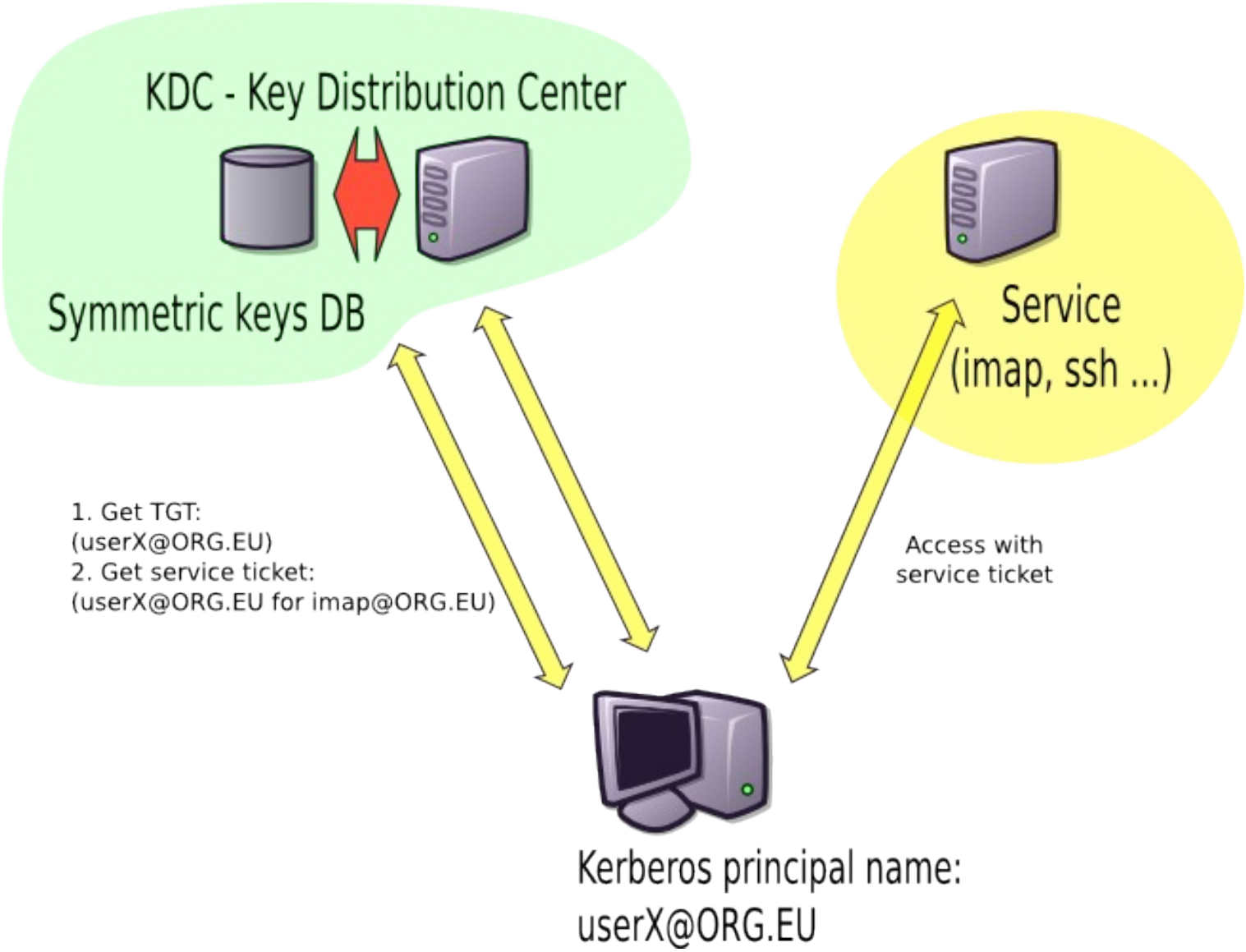
- Heimdal
  - Heimdal-1.2.1
  - Developed in Sweden
  - Better security track record
  - More features

- Microsoft Windows 2000 and later
  - ActiveDirectory default authentication protocol
  - AuthZ extension: PAC – Privilege Access Certificate

How Kerberos works

- Inband for different protocols
  - IMAP, POP, Telnet, SSH, Cisco routers ...
- 3rd party trust point - KDC
  - KDC – Key Distribution Center
  - Symmetric key cryptography
- Client acquires TGT from KDC
  - TGT - Ticket Granting Ticket
  - Client-KDC trust via shared secret – password
  - User prompted for password!
- Client uses TGT to request Service ticket from KDC
  - User isn't prompted for password
  - KDC issues a time limited Service ticket for ServiceX

Kerberos diagram



Kerberos demo

Video demo!

(screencast of user accessing Kerberos protected resource
and using various tools to display Kerberos tickets)

- Cheat sheet:
  - kinit
  - klist [-v]
  - kgetcred <service>
  - kdestroy [--credential=service]

Kerberos shortcomings

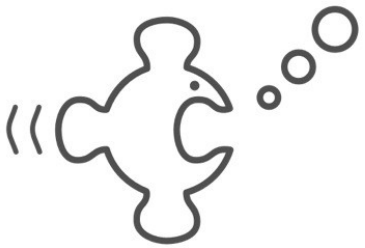
- Bad administrator documentation
- Horrible developer documentation
- Questionable security track record
- Not suitable to run as a „public“ internet service
  - From design-on treated as a **LAN or campus** service
  - Static 2-way or spoke and hub inter-realm trust
  - Always firewalled
- Bad authorization support
  - Kerberos doesn't provide much data
  - Kerberos AutZ in application: check if userID is present
- SPNEGO for web applications
  - Simple and protected GSSAPI Negotiation mechanism
  - Limited to local network use

Distributed AAI using SAML

- SAML – Security Assertion Markup Language
  - Data format / standard
- Web applications
  - Seperate login from application
  - Single Sign On (SSO)
  - User authenticates via „login application“
    - IdP – Identity Provider
  - Authorization data sent to „service application“
    - SP – Service Provider
    - Module in web server
    - Application library
- SAML 1.0 – OASIS standard, 2002
- SAML 2.0 – OASIS standard, 2005

SAML-AAI implementations

- Shibboleth IdP, SP
  - http://shibboleth.internet2.edu/
  - Older
  - Very configurable
  - Java
- SimpleSAMLphp IdP, SP
  - http://rnd.feide.no/simplesamlphp
  - Newer
  - Very easy to use
  - PHP



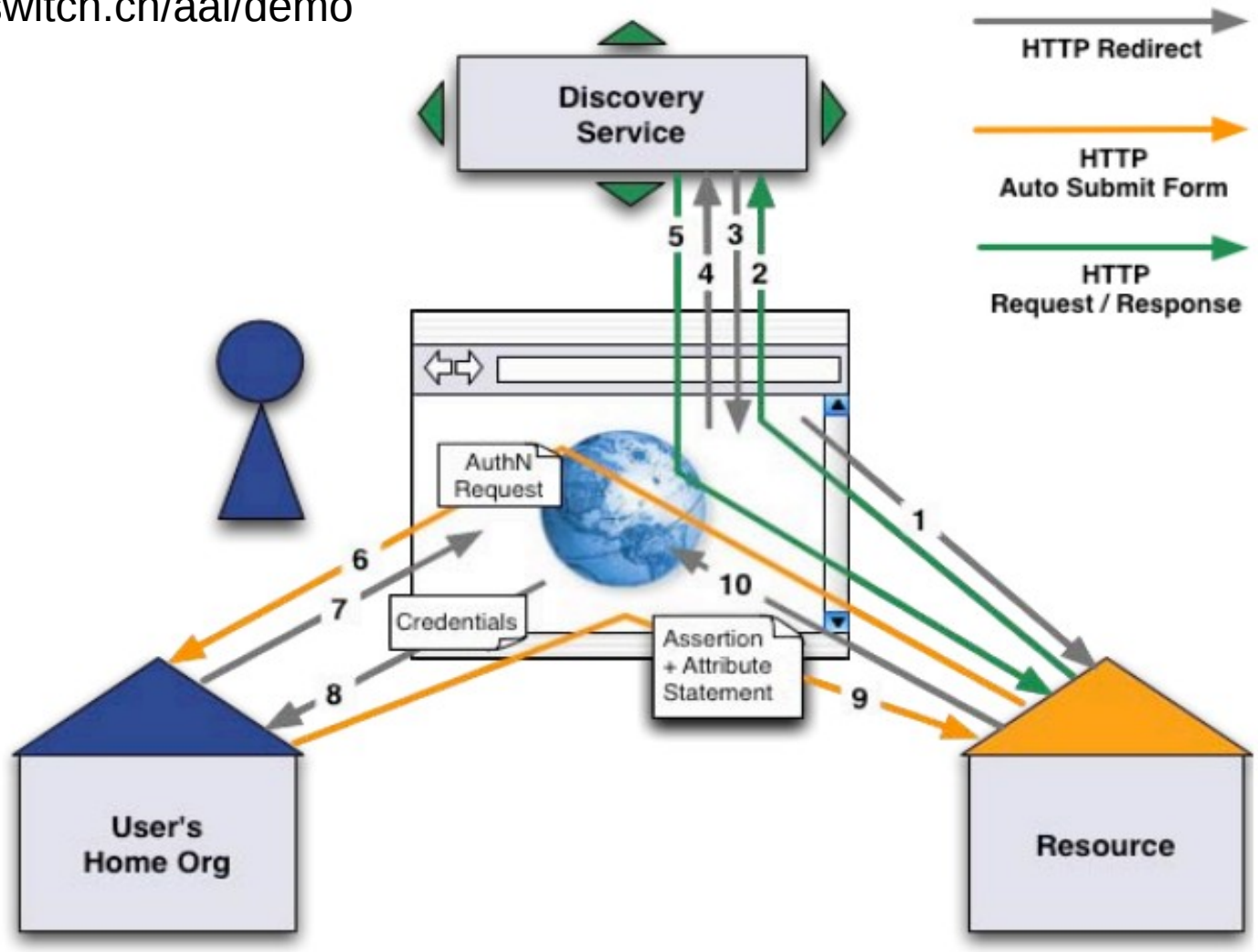
How SAML-AAI works

- 3rd party trust point
  - Metadata distribution point (Web server URL)
  - X.509 public key cryptography
- Web browser redirects
  - WAYF/DS – Where Are You From/Discovery Service
- Auto-submit forms
  - IdP sends authorization data from LDAP to SP
- Cookies for SSO session at IdP

SAML-AAI Diagram

Akademska in raziskovalna mreža Slovenije

http://www.switch.ch/aai/demo



SAML-AAI demo

Akademska in raziskovalna mreža Slovenije

Video demo!

(screencast of user accessing Adobe Connect PRO and Foodle aplication,
web server with integrated Shibboleth 2.1 SP,
login via SimpleSAMLphp IdP)

Comparing SAML-AAI and Kerberos

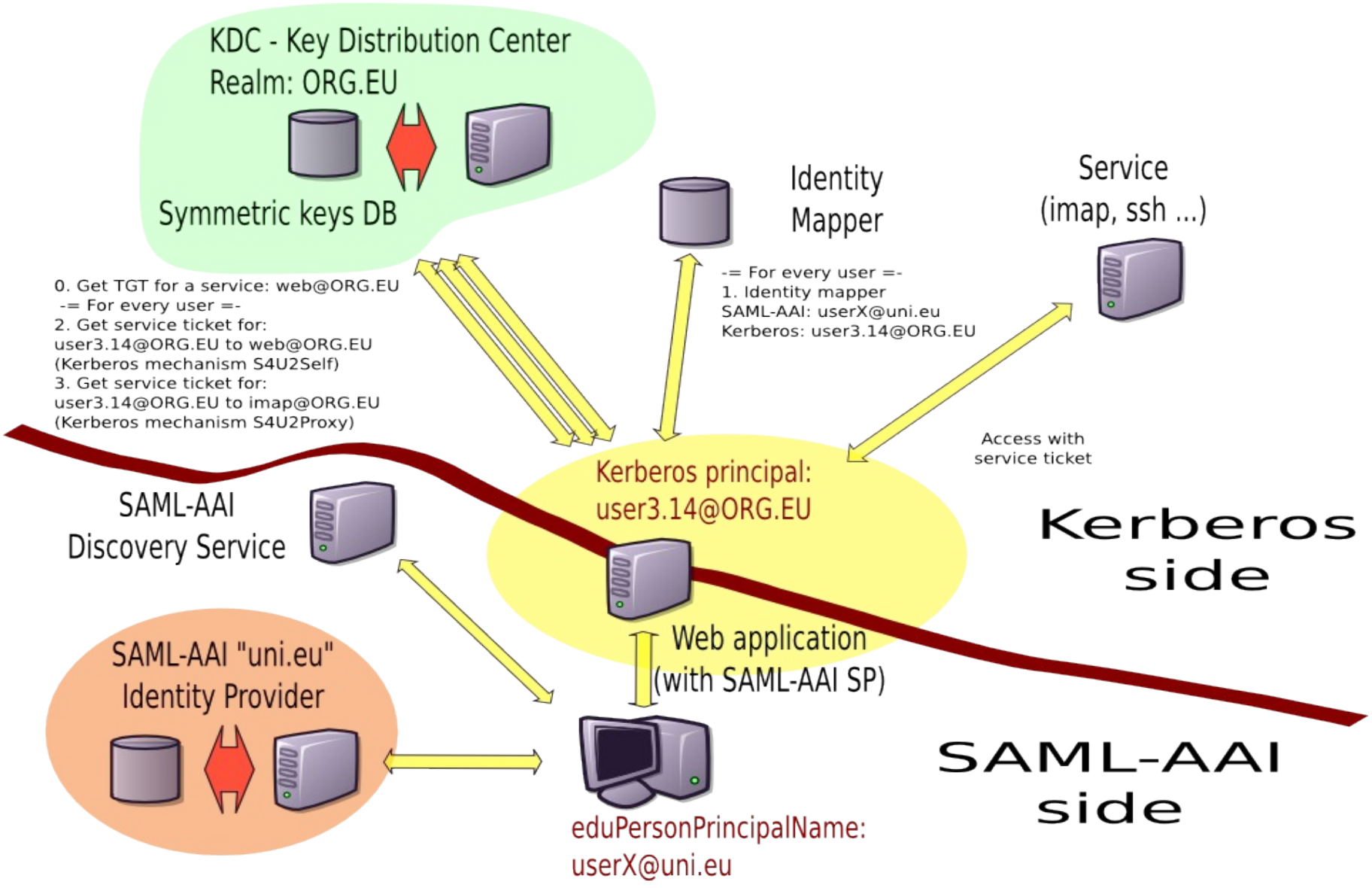
- SAML-AAI
  - Web applications
  - Internet-wide
  - X.509 PKI
  - SAML
  - Authorization data
- Kerberos
  - (Mostly) Non-web applications
  - Local/campus networks
  - (Mostly) symmetric keys
  - ASN.1
  - (Mostly) no authorization data

SAML-AAI and Kerberos are not competing protocols!

Interoperating SAML-AAI and Kerberos

- Hybrid web applications:
  - Web interface
  - Access to backend Kerberos protected services
  - Login via SAML-AAI + get Kerberos ticket
- Problems:
  - Identity mapping
    - Which Kerberos principal name to use?
    - Kerberos principal name: userX@ORG.EU
    - org.eu is Kerberos LAN/Campus realm
    - SAML identity
      - EduPersonPrincipalName: userX@uni.eu
      - EduPersonTargetedId: kl83Hlsnblq Yskgh72Kfqkl
  - User provisioning (new user?!)
  - Getting service tickets from KDC for userX@ORG.EU

Hybrid SAML-AAI with Kerberos diagram



ARNES AAI team

Akademska in raziskovalna mreža Slovenije

- http://aai.arnes.si
- http://www.eduroam.si
- e-mail: aaa-podpora@arnes.si

Questions?