

# **PKI in federations**

- **approach to non-web services**

Milan Sova, CESNET  
EuroCAMP, Dubrovnik, 2007

# SAMLized applications

- HTTPS
- web browser

What about

- email access
- network access
- message signing & encryption
- VoIP
- VPN
- ...

# Before SAML: X.509

- CA ... IdP
- AA ... AA
- Relying Parties ... SPs, relying parties
- ...

# X.509

```
{  
  {  
    Issuer,  
    ...  
    Subject,  
    Statement (PK/Attrs...),  
    ...  
  }  
  Signature  
}
```

# SAML

```
<saml:Assertion>  
  <saml:Issuer/>  
  <ds:Signature/>  
  <saml:Subject/>  
  <saml:Statement/>  
  ...  
  ...  
</saml:Assertion>
```

# Why X.509 didn't make it while SAML seems to be succeeding?

- format: binary vs. text
- scope: general vs. specific
- standards: closed vs. open
- community: telcos vs. internet
- assertions: static vs. dynamic
- **trust architecture: root vs. peers**

# Why is X.509 not dead yet?

- **ubiquitous code**
- long-term signing
- document encryption
- authentication
  - TLS servers
  - even (TLS) users!

# X.509 issues

- certificate enrollment
  - identity management
- certificate management
  - by users
    - “private” keys
  - by the relying parties
    - trust anchors
    - CRLs
  - by the infrastructure
    - re-keying, modification, revocation...
- **PKI's not easy... BUT...**

# X.509 and federations

- **federated CA**: certificate enrollment
  - federated identity
  - attributes for authorization
- different CAs for different purposes
- an X.509 certificate does not have to be **heavy**
- an X.509 certificate can be **pseudonymous**

# Possible X.509 applications

- network access (*eduroam*<sup>™</sup>)
  - EAP/TLS
  - authenticate devices not users
- VPN
  - OpenVPN
- SIP?
  - might work (at least for software clients)
- WebDAV?
  - why not? - it's just HTTPS

~~ROCK'S~~  
ROCK'S

NOT DEAD