Introduction to SAML Federations

Milan Sova
CESNET
Czech Republic
SAML?
SAML?

- Security Assertion Markup Language
SAML

- Security Assertion Markup Language
- Security Assertion
  - authentication statement
  - attribute statement
  - authorization decision statement
SAML Protocols

- “packing” of SAML elements
- SAML query
  - authentication query
  - attribute query
  - authorization decision query
SAML Bindings

- map SAML protocol messages onto standard protocols/formats
- SOAP Binding
- HTTP Redirect Binding
- HTTP Post Binding
- ...

...
Towards a federation – the problem

Service

AuthN

Attributes
Legacy approach

Service

AuthN

Attributes

Application itself
Legacy approach

Service

AuthN

Attributes

Service operator Org
Site-centric approach
Guards!

Service operator Org

Site UDB

Attributes

1232 3245 6787 1010

XXX YYY

<<<<<>><><>
Federation approach
Federation approach
Federation approach
Federation trust – How?

- technical means
- policy
Federation trust – Technical means

SAML metadata

Entity
  ID
  Role (SP, IdP, AA...)
Service Location URI
Operator Organization
Public Key(s)
...
Signature
Metadata publisher

• AKA aggregator, issuer, signer...
• verify the Entity metadata
• sign & publish

familiar?
Metadata publisher

- AKA aggregator, issuer, signer...
- verify the Entity metadata
- sign & publish

=> functions of **Certification Authority**
  - same security & trust requirements
SAML metadata security properties

- validUntil
- cacheDuration
- no serial number or time of issuance
  - replay attack
- no revocation mechanism
  - short validity window
  - reliance on access to the publishing point
Federation trust - Policies

- responsibilities of individual parties
  - all
    - key protection
  - IdP
    - data accuracy
  - SP
    - data protection
  - metadata publisher
    - metadata verification
Use of SAML federations in grids

- Mainly web-oriented
- Credential conversion
  - federated CAs
- Access to grid portals
- Attributes to access control
- ...

...