Current Status of Blueprint AARChitectures

Marcus Hardt
Task JRA1.2
KIT

EGI-CF, Bari
12, Nov 2015
Feedback and questions

• Google doc for feedback (especially for correcting errors in the architectures)
• http://tinyurl.com/qfv8kod
• Just drop your comments (it’s anonymous...)
eduGAIN Federations & RC & e-Infrastructures
eduGAIN Federations & RC & e-Infrastructures
e-Infrastructure Deployments

• We analysed several e-Infrastructures
  • EUDAT
  • DARIAH
  • ELIXIR
  • UMBRELLA
  • WebFTS
  • EGI
  • INDIGO
• Sorry for the amount of pictures
VO Management and FIM in DARIAH

DARIAH LDAP
- ou = people
- ou = shibpeople
- ou = groups

DARIAH IdP

Registration SP
- Attributes + Entitlements

Campus IdP
- ePPN + Attributes

Attributes+

write

Redirect2

Attributes

Redirect2

Aggr. Attr. Resolver

Resource SP
- Attribute Checker

DARIAH Resource

Admin Portal

Permissions

Ext Attributes Authentication LoA Proxy Token Translation Service Provider
Image courtesy of M. Van Daalen, PSI, 2014
INDIGO AAI

Login Service
- Identity management
- SAML SP & X.509
- Session Database
- OAuth2.0 server & client
- Identity Harmonisation

Group Membership Service
- Group management
- OAuth2.0 server & client

Scientific Gateway
- Web portal
- OpenID Connect Token
- Access Token

Token Translation Service
- Service Plugin
- Service Plugin
- Internal VOMS

DFN federation
eduGAIN
Google

Ext Attributes Authentication LoA Proxy TokenTranslation Service Provider
dCache
OpenStack Keystone
OneData
SSH
Grid-Ftp
AAI: The e-Infrastructure view

What is happening on top of existing Federation infrastructures today

ELIXIR

National federations (eduGAIN)

Social

eGoV-ID

Other

Step up AuthN

The authenticated user can go:
- Directly to the service
- Authenticate via Proxy
- Use Token Translation

AARC

https://aarc-project.eu
AAI: The e-Infrastructure view
What is happening on top of existing Federation infrastructures today

User

National federations (eduGAIN)

X.509

OIDC

SAML

eGovID

Other

Step up Audit

The authenticated user can go:
- Directly to the service
- Authenticate via Proxy
- Use Token Translation

Reputation Service

Token Translation Service

Site Token Services

Possible flows of additional attributes:
- Directly to the service
- via the Proxy / TTS

Attribute Authorities

AA: SAML

AA: eGov

AA: VOMS

Addressed via Attribute Authorities:
This is still unclear

Ext Attributes
Authentication
LoA
Proxy
Token Translation
Service Provider

End Services

Three options to authenticate at a service:
- Directly
- Via Proxy
- Via Token Translation

Attribute Flow
Unauthenticated User
Authenticated User
Thank you

Any Questions?

hardt@kit.edu