Authentication and Authorisation for Research and Collaboration

Guidelines for attribute translation to X.509

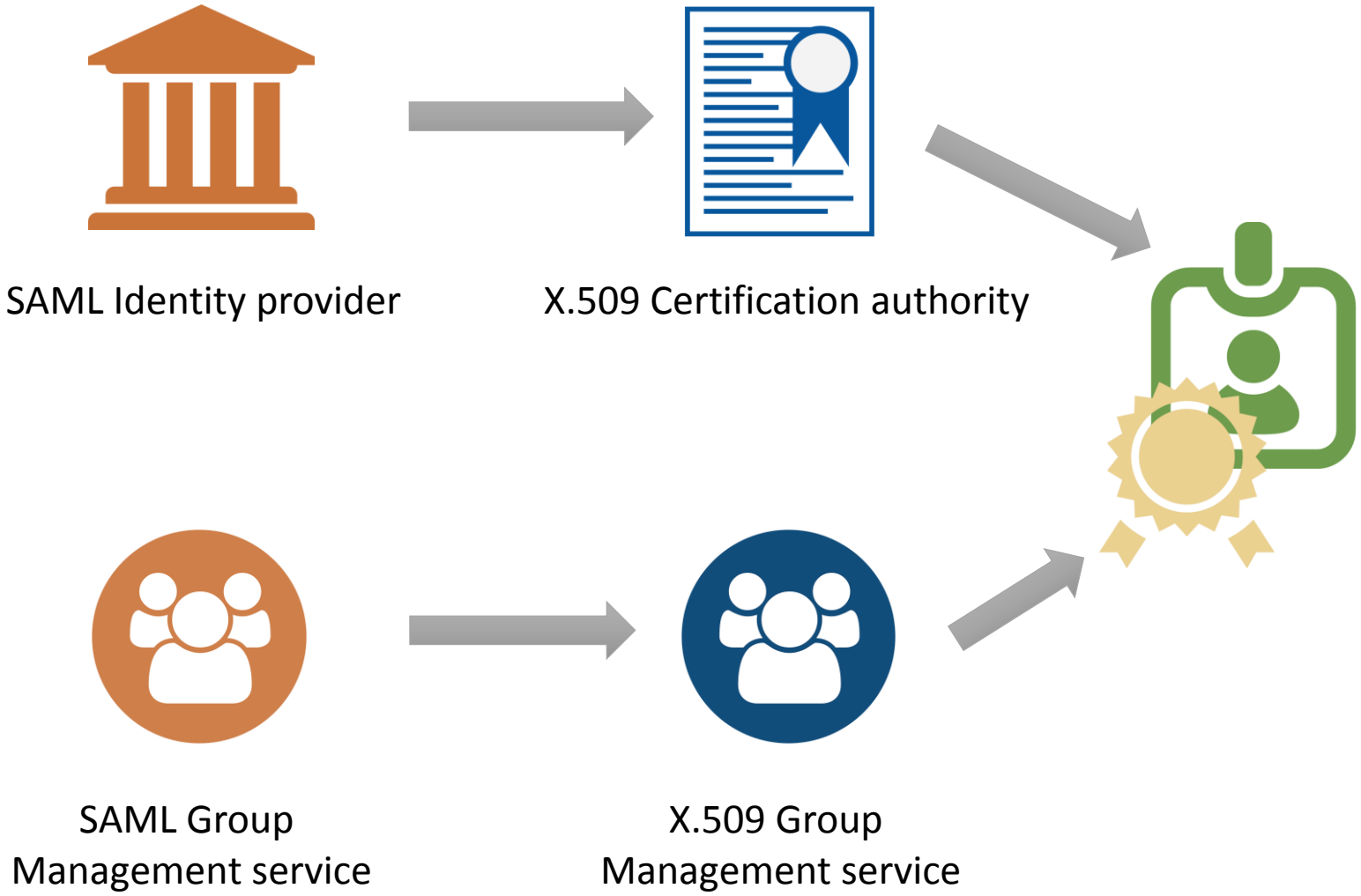
Peter Solagna
EGI Foundation
peter.solagna@egi.eu

AARC 4th General meeting
29 November 2016

Available material

- AARC
  - MJRA1.3: Design for the integration of an Attribute Management Tool
  - DJRA1.4A: Recommendation expression group membership
  - DJRA1.4C: Guidelines on token translation services
- Non-AARC
  - OGF: Interoperable certificate profile

Keep separated authorization and authentication information



Attributes in the EEC as foreseen in the OGF/IGTF policies

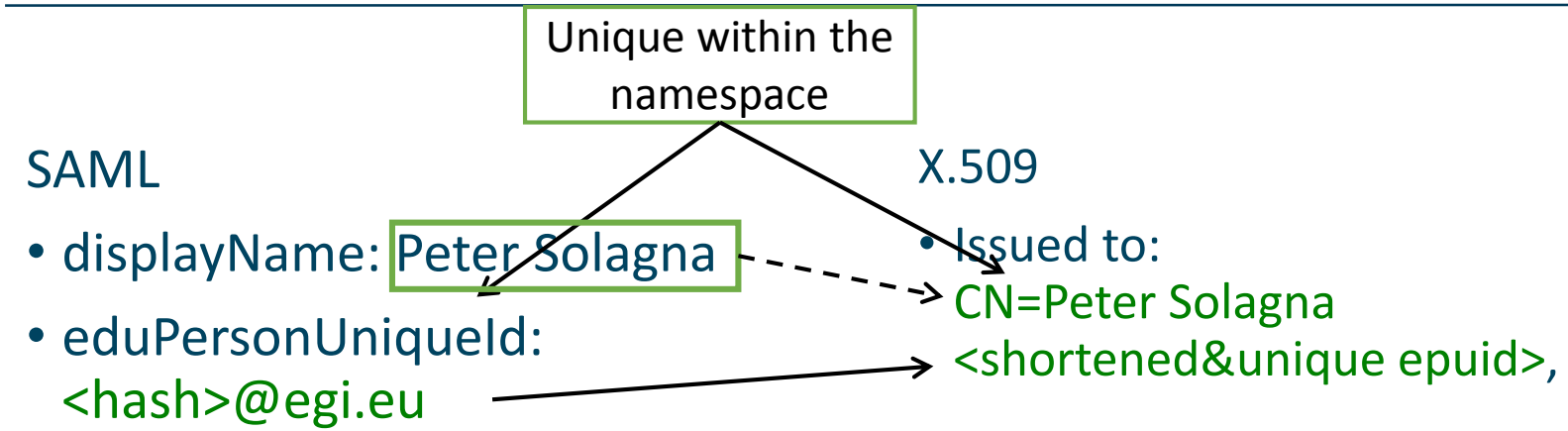
- DC: Domain
- C: Country
- L: Locality
- O: Organization
- CN: Common name

- Real life example:

/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth

/O=dutchgrid/O=users/O=egi/CN=Peter Solagna

How RC Auth translates information from SAML IDPs to X.509



eduPersonUniqueId
Or
eduPersonPrincipalName
Or
eduPersonTargetedID

Requested →

Suggested - - - - - - →

How RC Auth translates information from SAML IDPs to X.509 (2)

SAML Options

- schacHomeOrganisation
- organisationDisplayName
- domain name of the IdP entity ID URL

X.509

- O=egi,
  O=users,
  O=dutchgrid

- Issued by:
  Certification authority DN

Group information, AARC general recommendation

- DJRA1.4A Recommendation
  1. Centralised harmonisation of group membership information
  2. Compatibility with existing group information models
  3. Scoping of group membership information
  4. Use of **eduPersonEntitlement** attribute
  5. Use of valid URIs either URLs or URNs

Best practices in attribute management

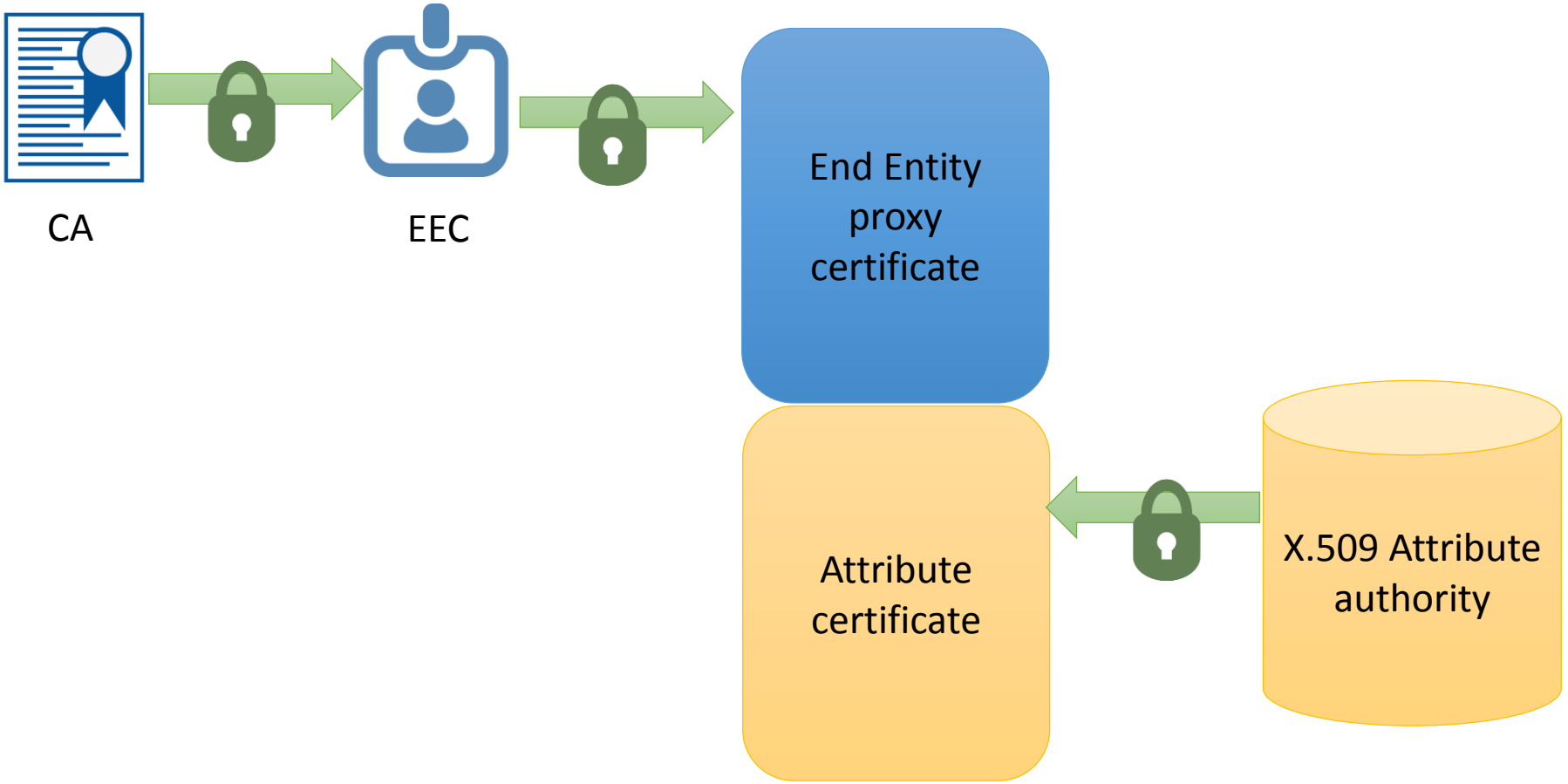
Attributes technical requirements

Example of VO membership as expressed by CheckIn

```
urn:mace:egi.eu:<authority-fqdn>:[<group>[:<subgroup>:…]]:<role>@<vo>
```

- <authority-fqdn> is the FQDN of the authoritative source for the entitlement value
- <vo> is the name of the Virtual Organisation
- <group> is the name of a group in the identified <vo>; specifying a group is optional
- zero or more <subgroup> components represent the hierarchy of subgroups in the <group>; specifying sub-groups is optional
- the <role> component is scoped to the rightmost (sub)group; if no group information is specified, the role applies to the VO

X.509 attribute certificate



Attribute certificates in EGI

subject : /O=dutchgrid/O=users/O=egi/CN=Peter Solagna/CN=<proxy uid>
issuer : /O=dutchgrid/O=users/O=egi/CN=Peter Solagna
identity : /O=dutchgrid/O=users/O=egi/CN=Peter Solagna
type : RFC3820 compliant impersonation proxy
strength : 1024
path : /tmp/x509up_u506
timeleft : 11:59:53
key usage : Digital Signature, Key Encipherment, Data Encipherment

Personal proxy certificate

=== VO dteam extension information ===

VO : dteam
subject : /O=dutchgrid/O=users/O=egi/CN=Peter Solagna
issuer : /C=GR/O=HellasGrid/OU=hellasgrid.gr/CN=voms2.hellasgrid.gr
attribute : /dteam/Role=NULL/Capability=NULL
attribute : /dteam/EGI/Role=NULL/Capability=NULL
timeleft : 11:59:53
uri : voms2.hellasgrid.gr:15004

Attribute certificate

Attribute certificates in EGI -2-

VO : dteam

subject : /O=dutchgrid/O=users/O=egi/CN=Peter Solagna

issuer : /C=GR/O=HellasGrid/OU=hellasgrid.gr/CN=voms2.hellasgrid.gr

attribute : /dteam/Role=NULL/Capability=NULL

attribute : /dteam/EGI/Role=NULL/Capability=NULL

timeleft : 11:59:53

uri : voms2.hellasgrid.gr:15004

R3: One attribute certificate per VO
VO name: unique within the infrastructure

Signed by the X.509 attribute authority

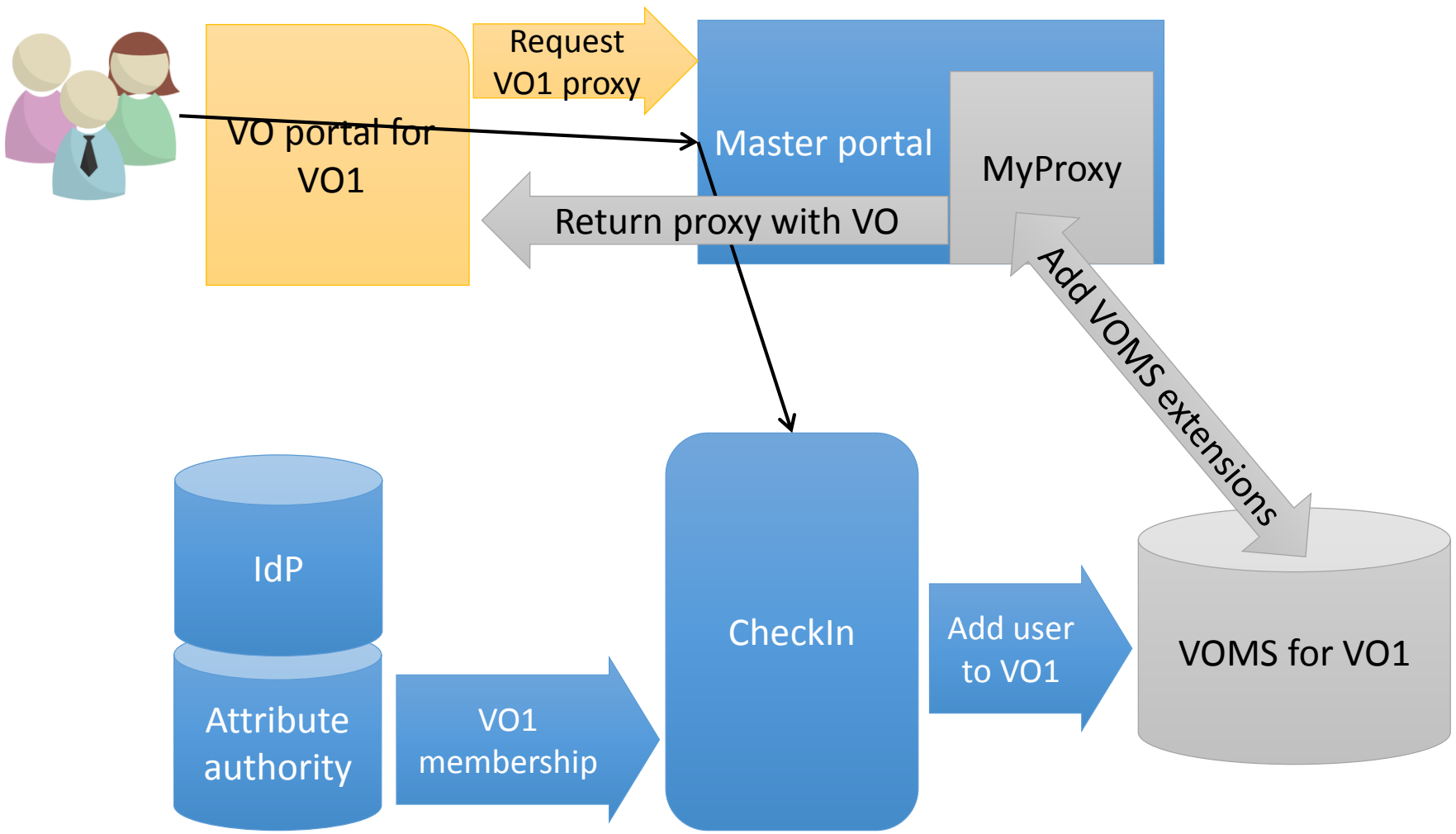
Groups, sub groups, membership, and roles within the group

R5: Valid URI. Constant for all certificates released through the translation service

Possible AARC recommendation for group membership translation to X.509

- Group membership information should be translated into an attribute certificate (AC) separate from the EEC. AC should be included in a EE proxy certificate
  - RFC3820
  - RFC3281
- One AC should contain information about a single virtual organization
- Groups, sub-groups and roles within the group should be expressed in the form:
  - /<vo>/<group>/<sub-group/../Role=<role>
  - Optional?
- AC should be short-lived: max 24h

Pilot for attribute translation from SAML to X.509



Thank you

Any Questions?

karl.meyer@geant.org

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).