OpenGridForum
OPEN FORUM | OPEN STANDARDS

Production Grid Infrastructure WG

Work towards common security profiles

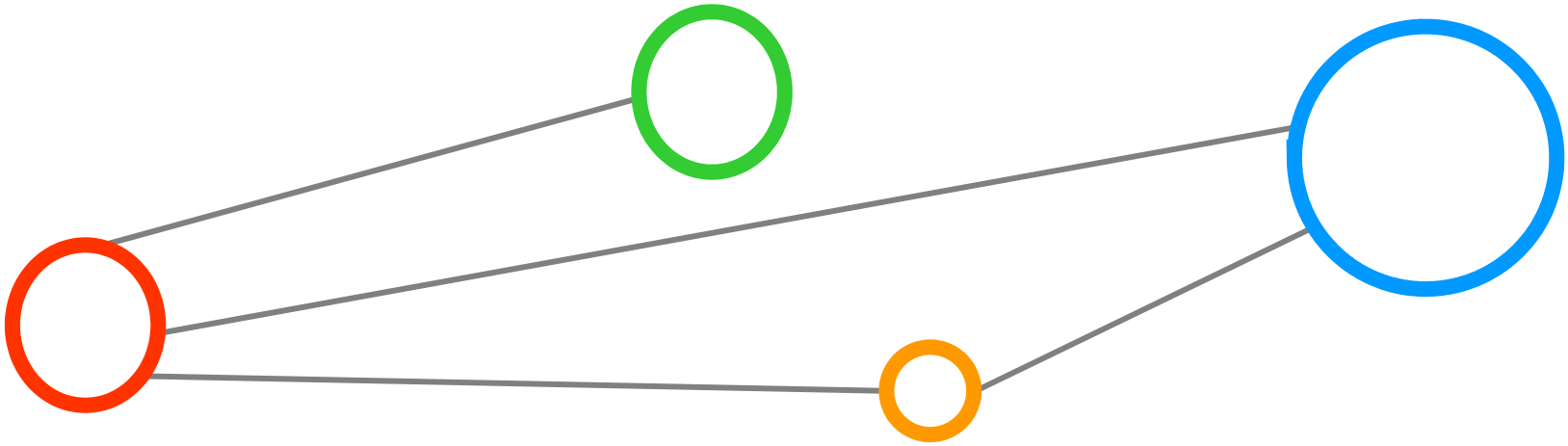
Morris Riedel (Jülich Supercomputing Centre & DEISA)
PGI Co-Chair

OGF IPR Policies Apply

- "I acknowledge that participation in this meeting is subject to the OGF Intellectual Property Policy."
- Intellectual Property Notices Note Well: All statements related to the activities of the OGF and addressed to the OGF are subject to all provisions of Appendix B of GFD-C.1, which grants to the OGF and its participants certain licenses and rights in such statements. Such statements include verbal statements in OGF meetings, as well as written and electronic communications made at any time or place, which are addressed to:
  - the OGF plenary session,
  - any OGF working group or portion thereof,
  - the OGF Board of Directors, the GFSG, or any member thereof on behalf of the OGF,
  - the ADCOM, or any member thereof on behalf of the ADCOM,
  - any OGF mailing list, including any group list, or any other list functioning under OGF auspices,
  - the OGF Editor or the document authoring and review process
- Statements made outside of a OGF meeting, mailing list or other function, that are clearly not intended to be input to an OGF activity, group or function, are not subject to these provisions.
- Excerpt from Appendix B of GFD-C.1: "Where the OGF knows of rights, or claimed rights, the OGF secretariat shall attempt to obtain from the claimant of such rights, a written assurance that upon approval by the GFSG of the relevant OGF document(s), any party will be able to obtain the right to implement, use and distribute the technology or works when implementing, using or distributing technology based upon the specific specification(s) under openly specified, reasonable, non-discriminatory terms. The working group or research group proposing the use of the technology with respect to which the proprietary rights are claimed may assist the OGF secretariat in this effort. The results of this procedure shall not affect advancement of document, except that the GFSG may defer approval where a delay may facilitate the obtaining of such assurances. The results will, however, be recorded by the OGF Secretariat, and made available. The GFSG may also direct that a summary of the results be included in any GFD published containing the specification."

- OGF Intellectual Property Policies are adapted from the IETF Intellectual Property Policies that support the Internet Standards Process.

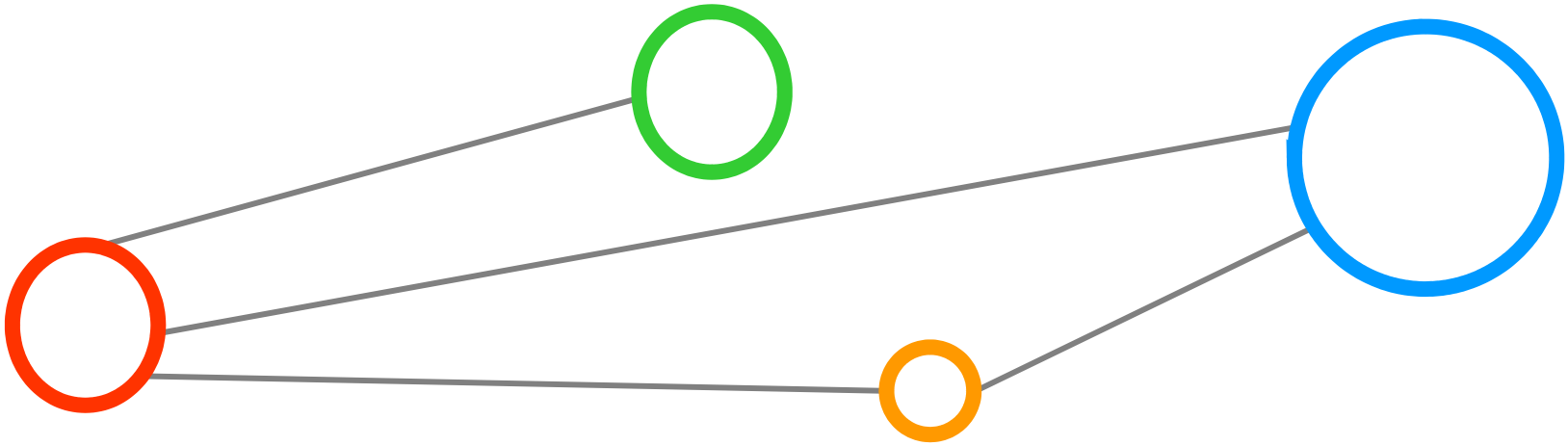
Outline



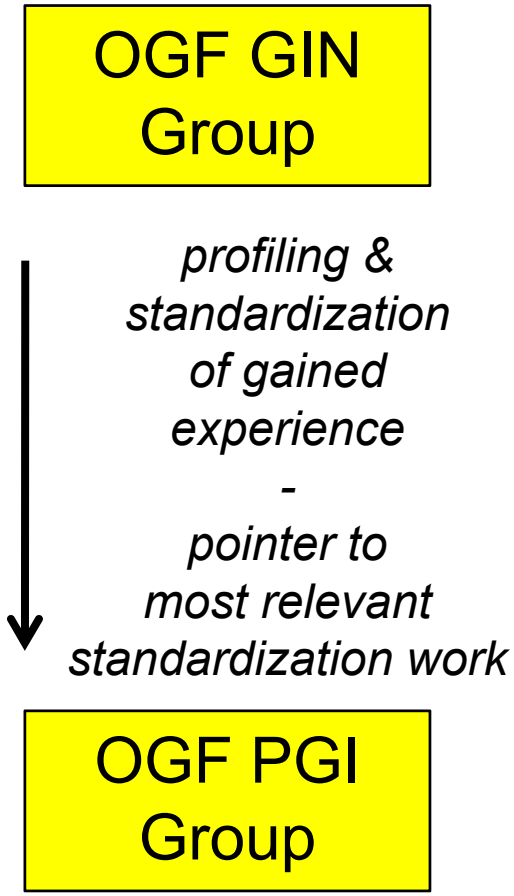
Outline

- OGF PGI 101
- 3 ‚Plumbings' for Authentication & Message Layer
- 2 ‚Plumbings for Attribute-based Authorization
- Common attributes
- Constraints/restrictions
- Out of Scope
- EMI in Context
- Conclusions

OGF PGI 101



GIN & PGI Groups



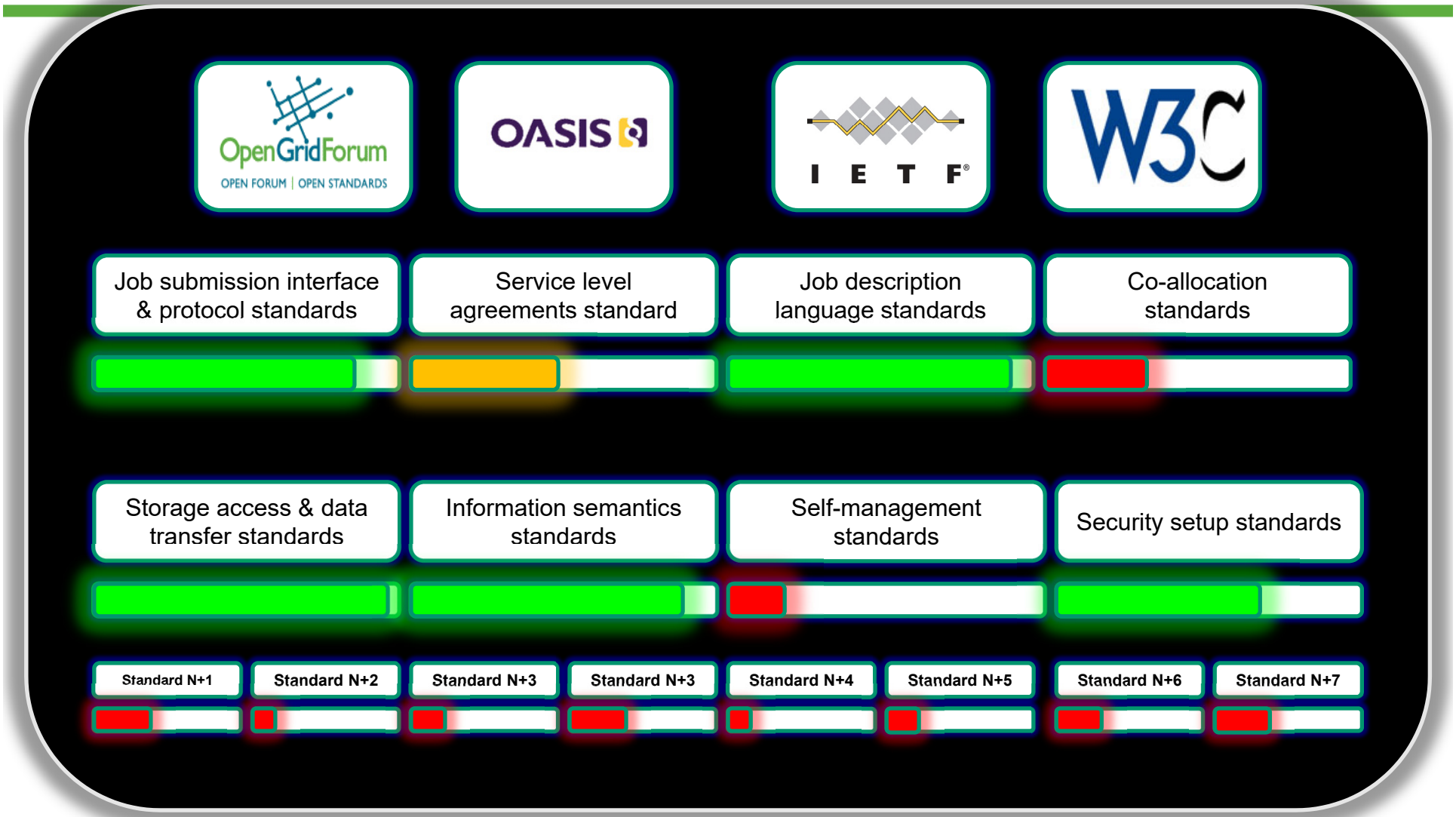
- OGF Grid Interoperation Now (GIN) Community Group
  - Cross-Grid use case applications that require resources in more than one Grid
  - (Often HTC and HPC interoperability)
  - Interoperation of multiple Grid infrastructures based on workarounds and small hacks / modifications
  - E.g. WISDOM, EUFORIA, VPH,…
- OGF Production Grid Infrastructure (PGI) Working Group
  - Takes gained experience from production interop of GIN into account
  - Standardization of a suitable set of standards based on lessons learned
  - Tunings, re-definition & focus on missing links between open standards

Scope

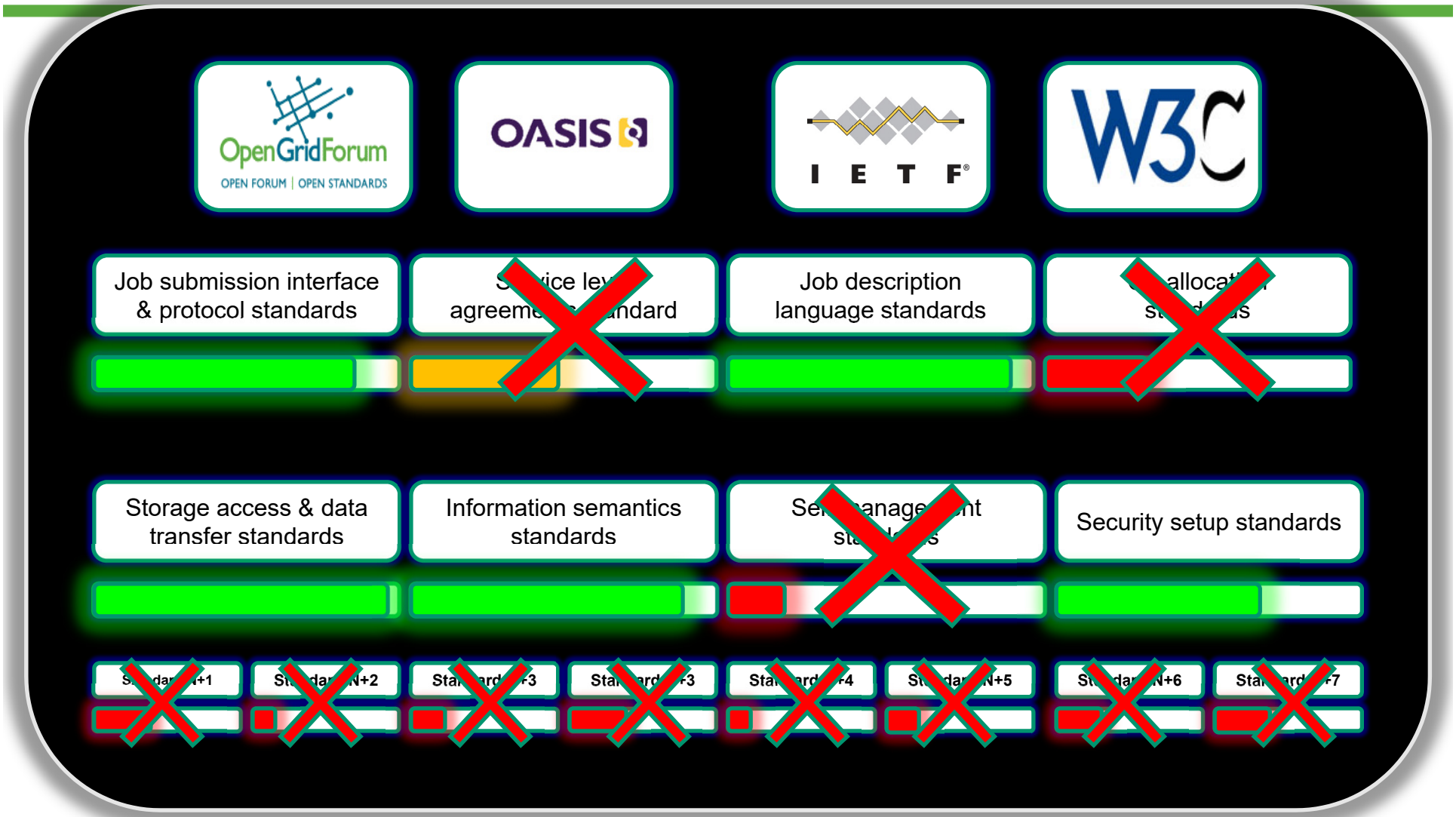
- Identified Basic Use Case
- Only matured specifications
- Specification adoption exist in production middleware systems
- Experience exists in production infrastructures
- Interoperability tests have been performed
- Real scientific use cases require these standards
- Refinements necessary and not complete spec. re-definitions

→ 'Low hanging fruits'

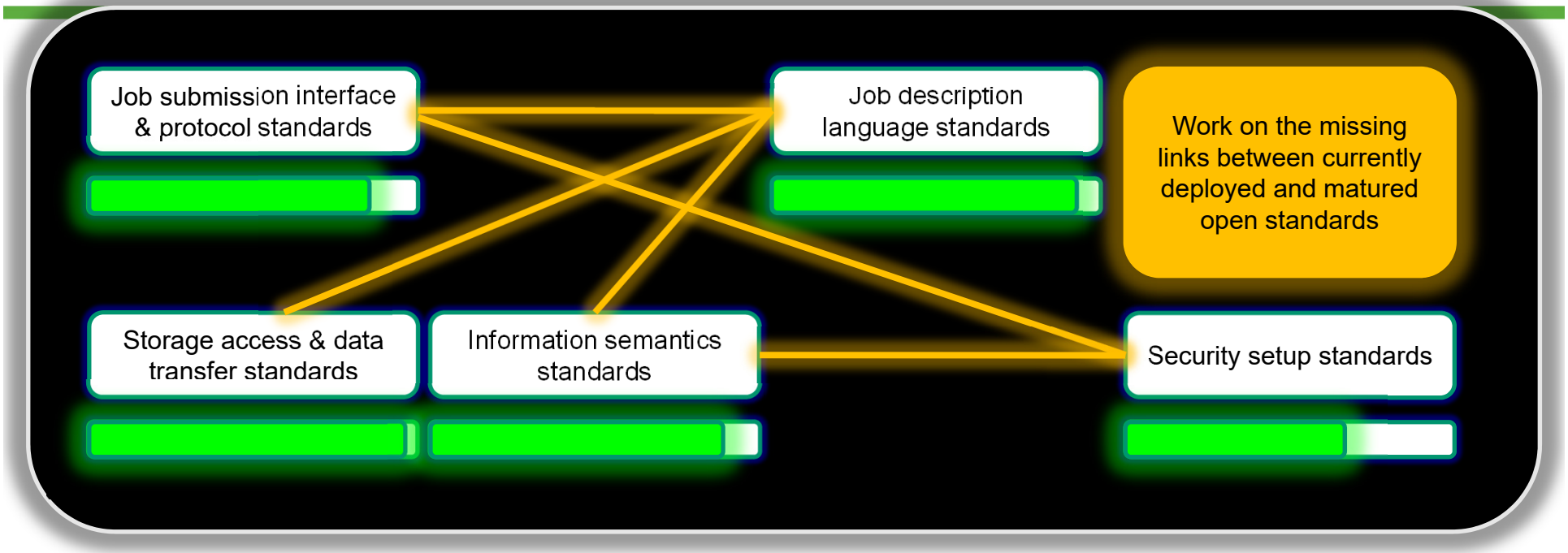
OGSA Standards



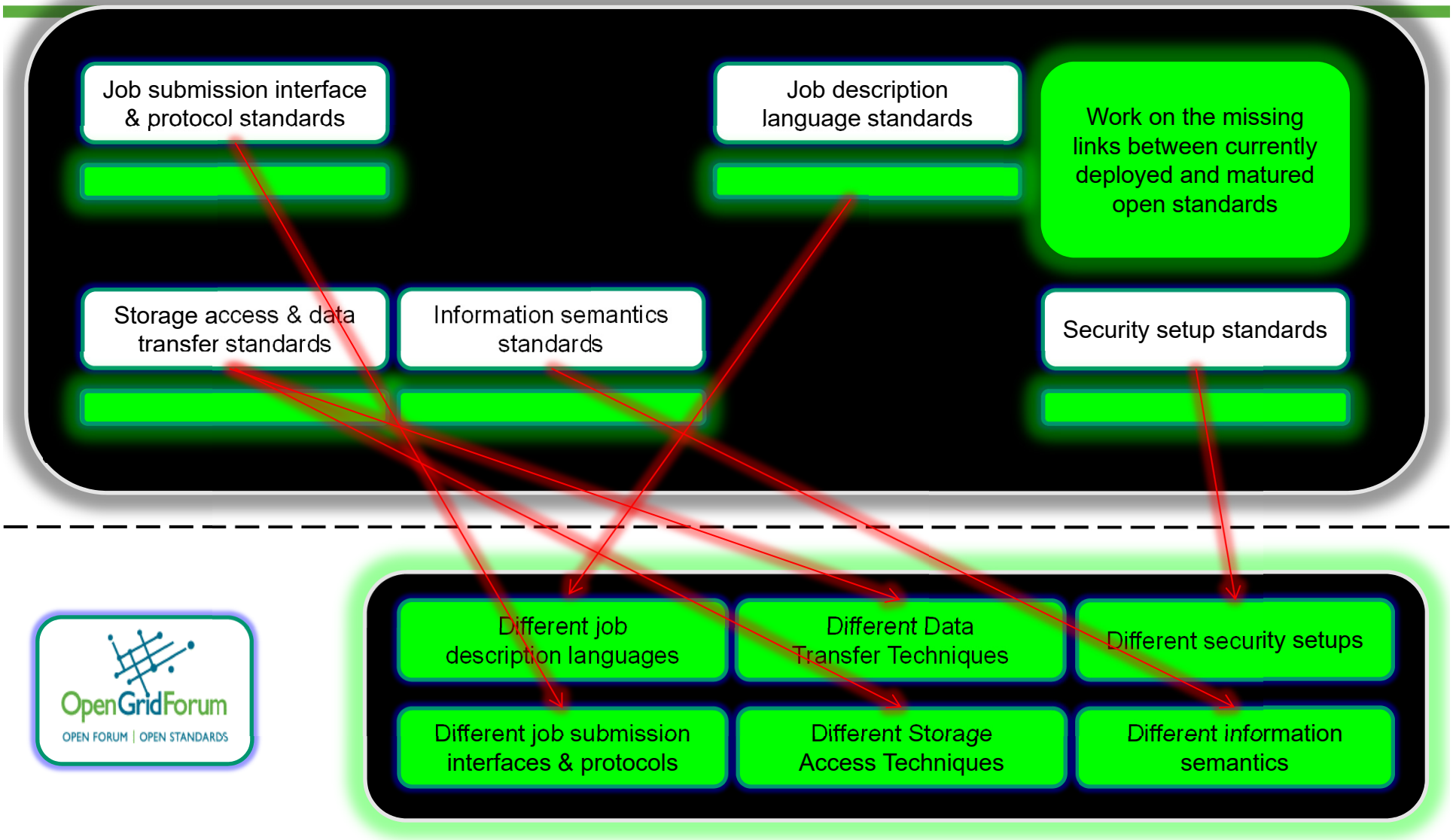
GIN Production Experience



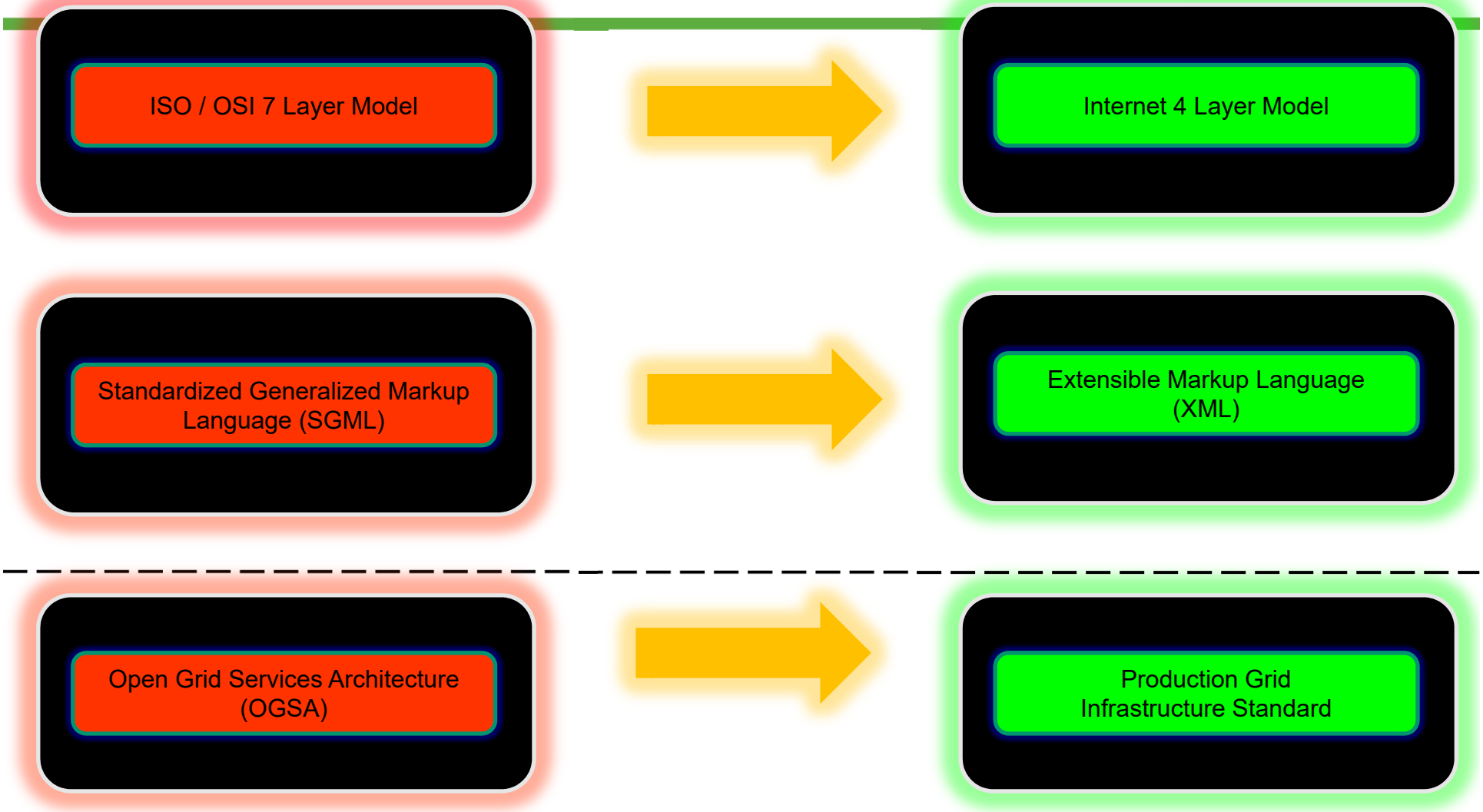
PGI Approach (1)



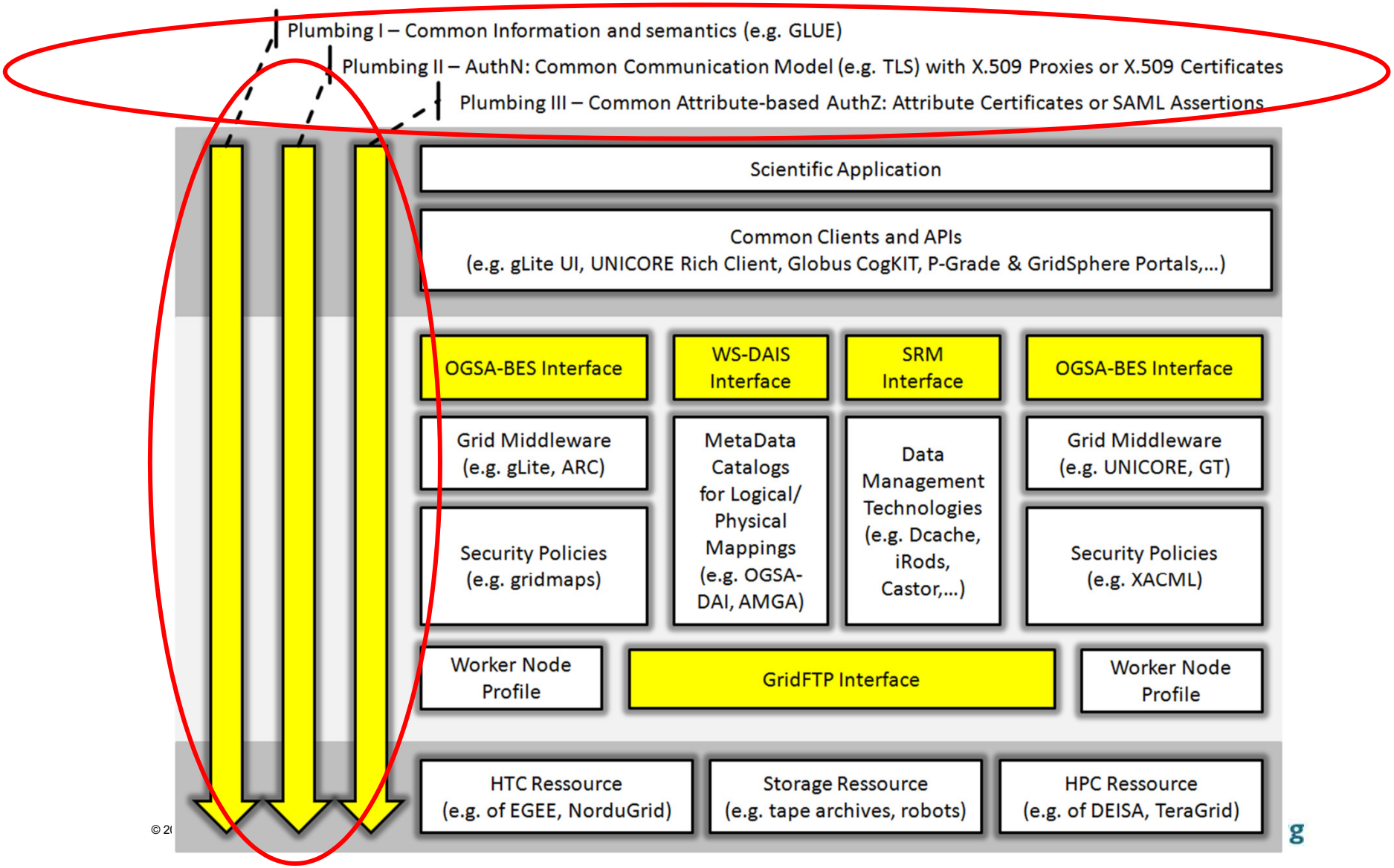
PGI Approach (2)



Compare History of Computer Science



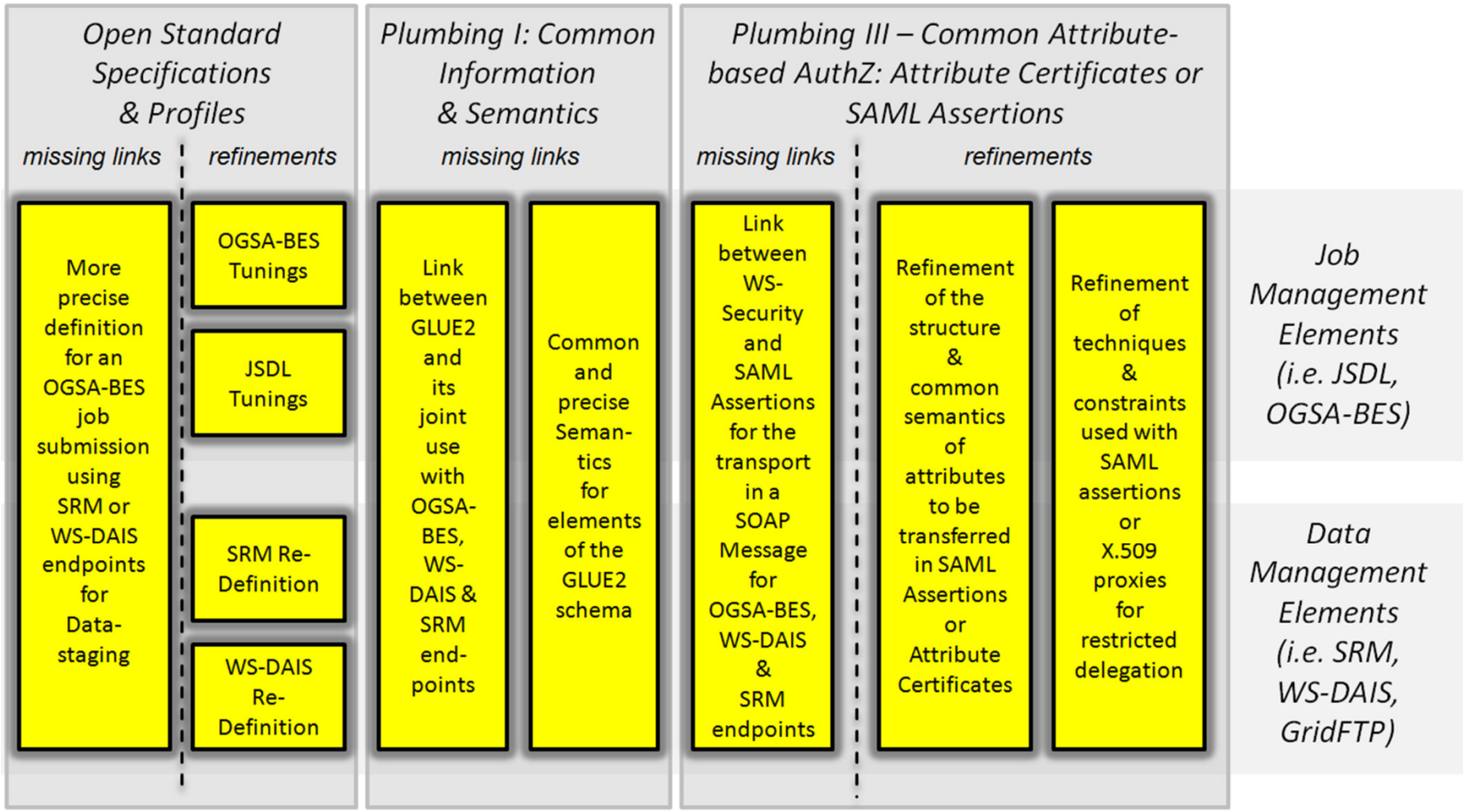
PGI Ecosystem Overview



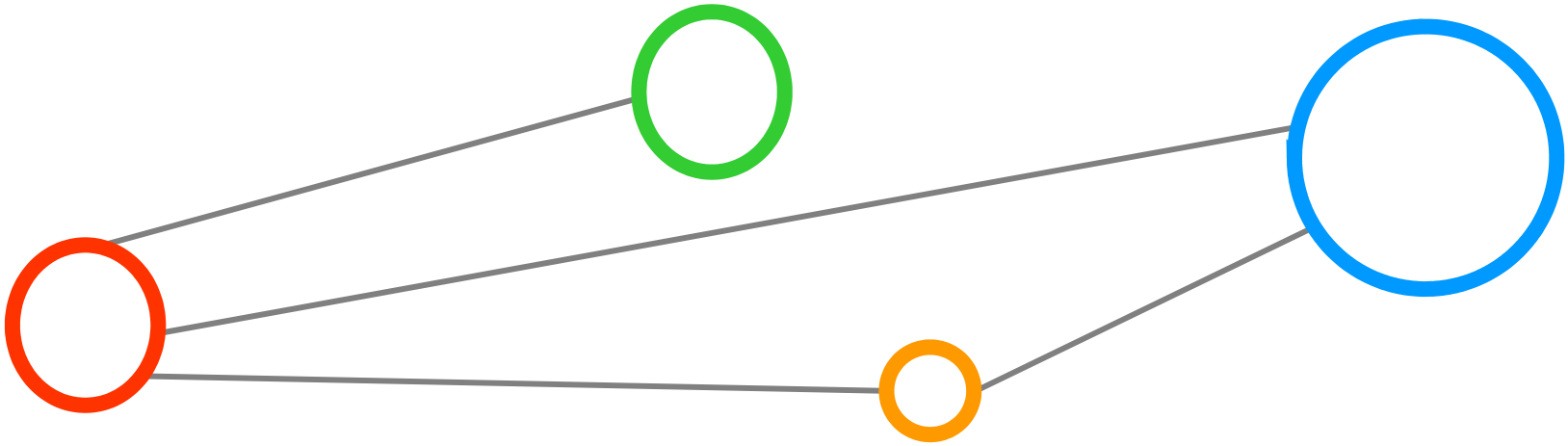
Plumbings Idea

- Plumbings can be used to put different ‚elements' through
  - E.g. warm water (realizing normal OpenSSL-TLS connections) vs. Cold water (realizing GSI connections), depends on deployments
- Many plumbings can be installed in parallel – while not crossing the other plumbings or breaking the plumbings
  - E.g. modern container concepts allow easily addition of n handler that can take care of the elements by n plumbings
- Different plumbings can use the same source and can be sink into the same achievement/functionality
  - E.g. Attribute-based VOMS system vs. SAML-based VOMS system
  - Both based on same VO DBs but convey attributes differently
  - However, authZ decision based on these attributes can be again usable for both approaches (e.g. one XACML policy file)
- Plumbings may be removed over time while new plumbings are already deployed in infrastructures

Missing Links & Refinements



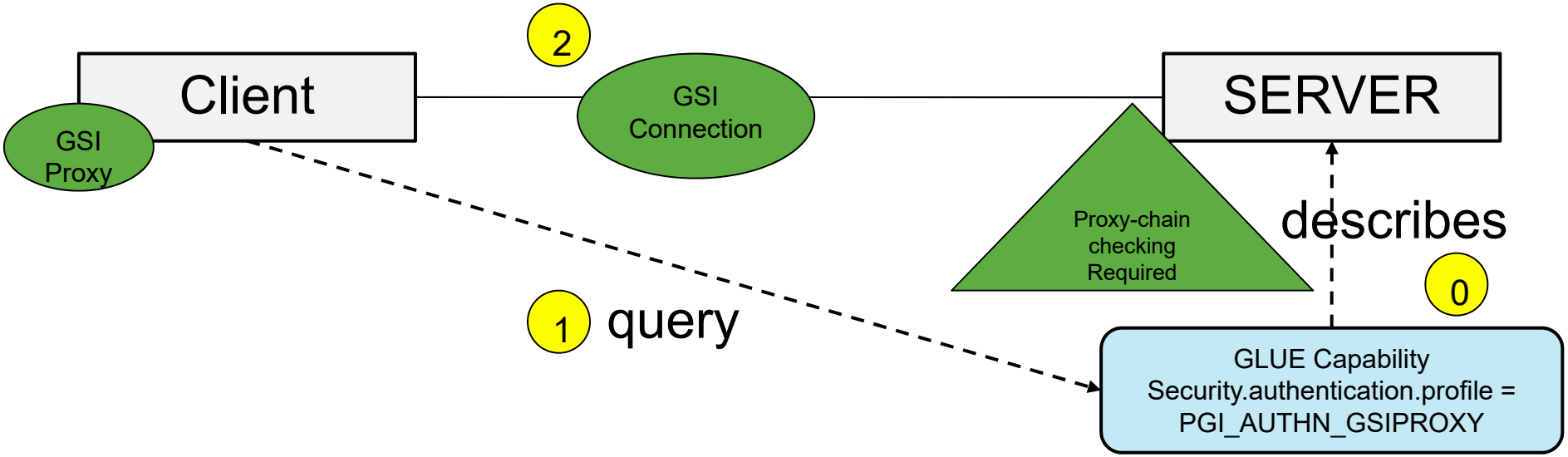
3 Plumbings for Authentication



(1) TLS with GSI Proxies

- General PGI paradigm
  - Move away from Grid Security Infrastructure (GSI) to align with Web-based world
  - Easier tooling, interoperability with Web on transport level
- GSI-based ‚TLS' is not compatible with OpenSSL TLS
  - Possible to make GSI-based TLS be compatible with OpenSSL TLS (GT4 environment variable to switch on compatible TLS)
- Many production systems require still the GSI-based TLS
  - Proxies needed since the data staging might be delegated
  - E.g. OGF Storage Ressource Manager (SRM) interface implementations and OGF GridFTP implementation
  - Changes in all these implementations take time
  - Deployments of these implementations then take more time
  - Idea: GSI plumbing until GSI is deprecated and not used anymore

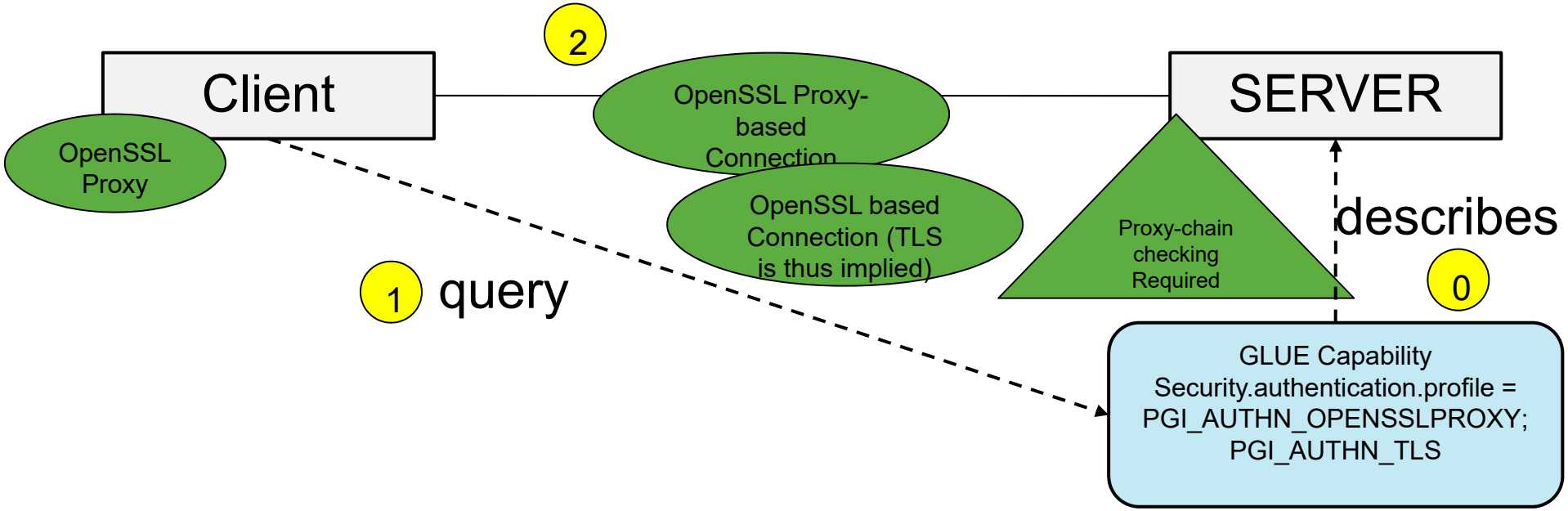
(1) TLS with GSI Proxies



(2) TLS with OpenSSL Proxies

- Components of NAREGI, ARC & gLite require OpenSSL-based Proxies TLS Connections
  - Proxies because a job submit might be delegated
  - Service container could work with non TLS proxies
  - Implies proxy chain checking (well specified in RFC3820)
  - Issues with proxy renewal (MyProxy is a proprietary protocol and thus not inline with a standards approach, but de-facto)
- UNICORE can work with OpenSSL-based Proxies
  - Implements optionally the proxy chain checking for these security setups
  - Proxies not needed for delegation – but used for interoperability

(2) TLS with OpenSSL Proxies



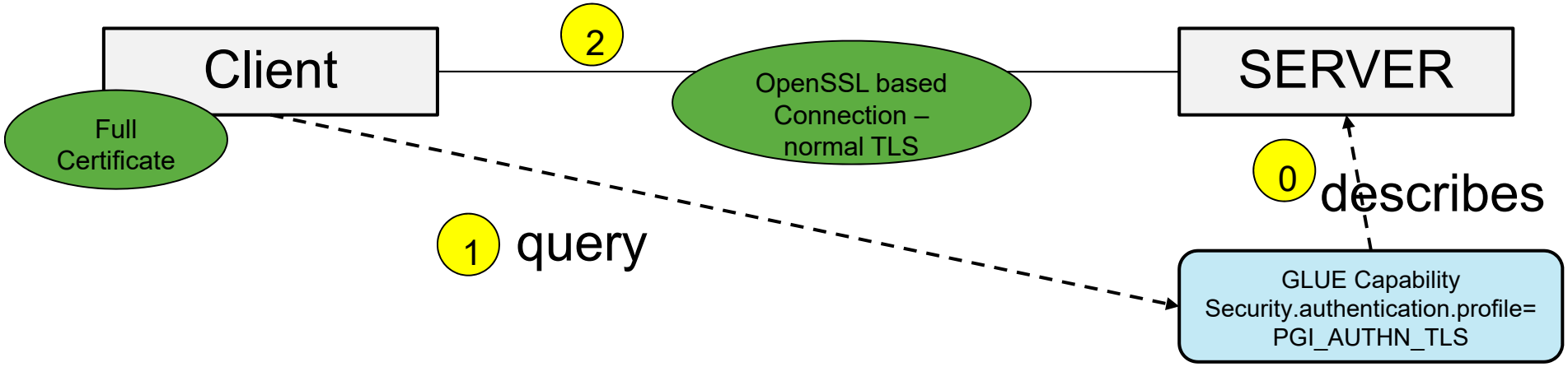
- „Classic VOMS“ supports RFC proxies instead of GSI proxies to generate valid proxies with Acs
  - Medium-term move towards this solution if consumers of ACs support this

(3) TLS with Full Certificates

- Some service container (e.g. UNICORE) required TLS connections using full end-entity certificates
  - Service container could not work with proxies in this setup
  - Proxy chain checking is not required!

- But(!) it can exist in parallel to Plumbing (2) in the same container
  - When moved away from GSI connections, TLS is interoperable
  - Proxy chain checking does not break the acceptance of full end-entity certificates since all are X.509 certificates
  - Both plumbings can exist smoothly in parallel and deployment of solution is subject to policy decisions on the infrastructures

(3) TLS with Full Certificates



Message layer Authentication (1)

- Numerous WS-Security Specifications
  - UsernameToken profile
  - X.509 Token profile (Can be directly generated if a X.509 credential is possessed)
  - SAML Token Profile
    - A third-party authority is required to issue SAML Token
    - Should be considered together with the SAML attribute assertion used for attribute-based AuthZ
    - SAML Token includes <saml:Subject> and <saml:Attribute>
    - The UVOS and VOMS SAML Service might be enhanced to support this profile

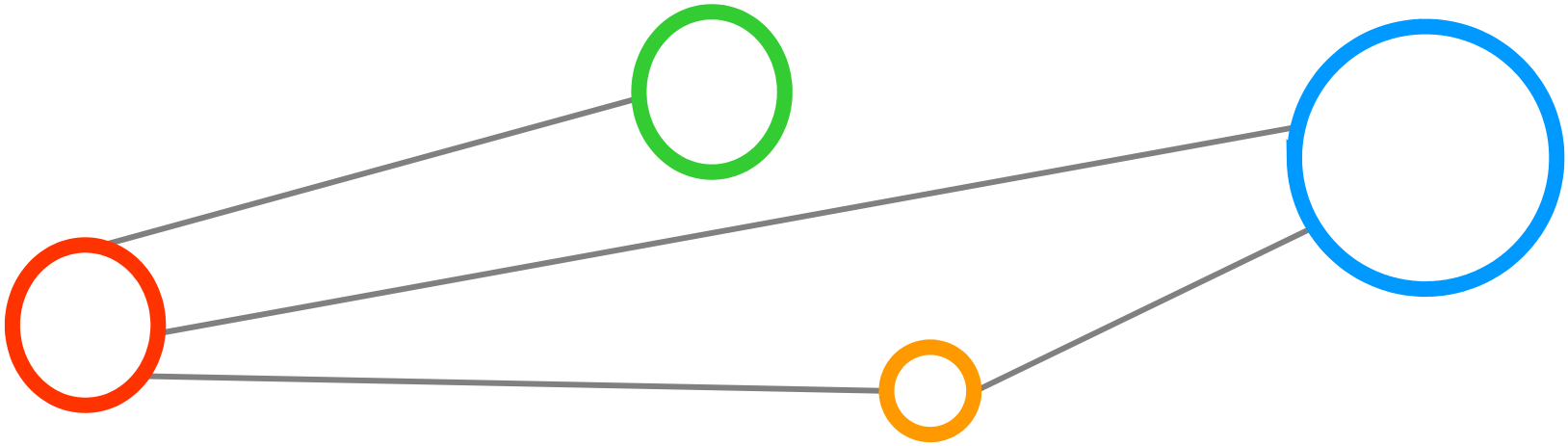
SAML Example

```
<saml:Assertion
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier NameQualifier="www.example.com" Format="...">
    uid=joe,ou=people,ou=saml-demo,o=grid.org
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
        </saml:ConfirmationMethod>
        <ds:KeyInfo>
          <ds:KeyValue>...</ds:KeyValue>
        </ds:KeyInfo>
      </saml:SubjectConfirmation>
    </saml:Subject>
  <saml:Attribute AttributeName="MemberLevel"
AttributeNamespace="http://www.oasis.open.org/Catalyst2002/attributes">
    <saml:AttributeValue>gold</saml:AttributeValue>
  </saml:Attribute>
  </saml:AttributeStatement>
  <ds:Signature>...</ds:Signature>
</saml:Assertion>
```

Message layer Authentication (2)

- WS-Trust Discussions
  - Define primitives and extensions for security token exchange
  - Enable the issuance and dissemination of credentials within different trust domains
  - Can be used for defining the token exchange: e.g. getting SAML Token by providing X.509 Token, etc.

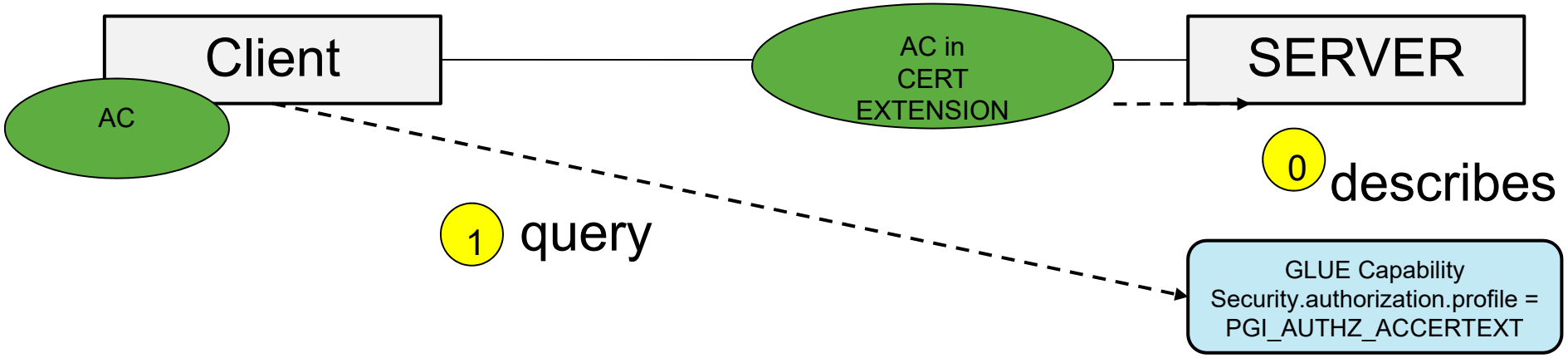
2 Plumings for AuthZ



(1) AC Certificates in Extensions

- Supporting „Classic VOMS“ exposing ACs
- Normally ACs are shipped via certificate extensions
- But since the ACs are bound to end-entity certificates, they may be shipped as alternative to SAML assertions in SOAP headers
- Plumbing might be removed in a few years when SAML became majorly used
  - PGI pushes the use of SAML, respecting production AC setups

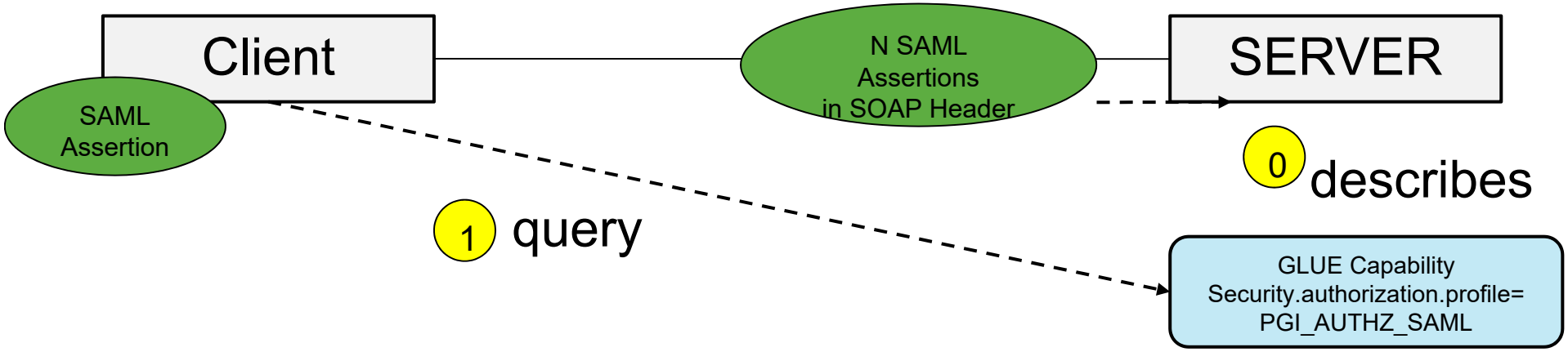
(1) AC Certificates in Extension



(2) SAML Assertions in SOAP Header

- Move towards SAML is pushed by PGI as a long-term goal while still respecting the production legacy setups
- Supported SAML-based VOMS or UVOS exposing SAML assertions (Attribute Authorities)
- n SAML assertions can be shipped in SOAP headers
  - Being careful: SAML assertions should be bound to a subject identity, otherwise each hop can „hi-jack“ the assertion for further usage (i.e. by other subjects)
  - But in general much more flexible as the AC approach

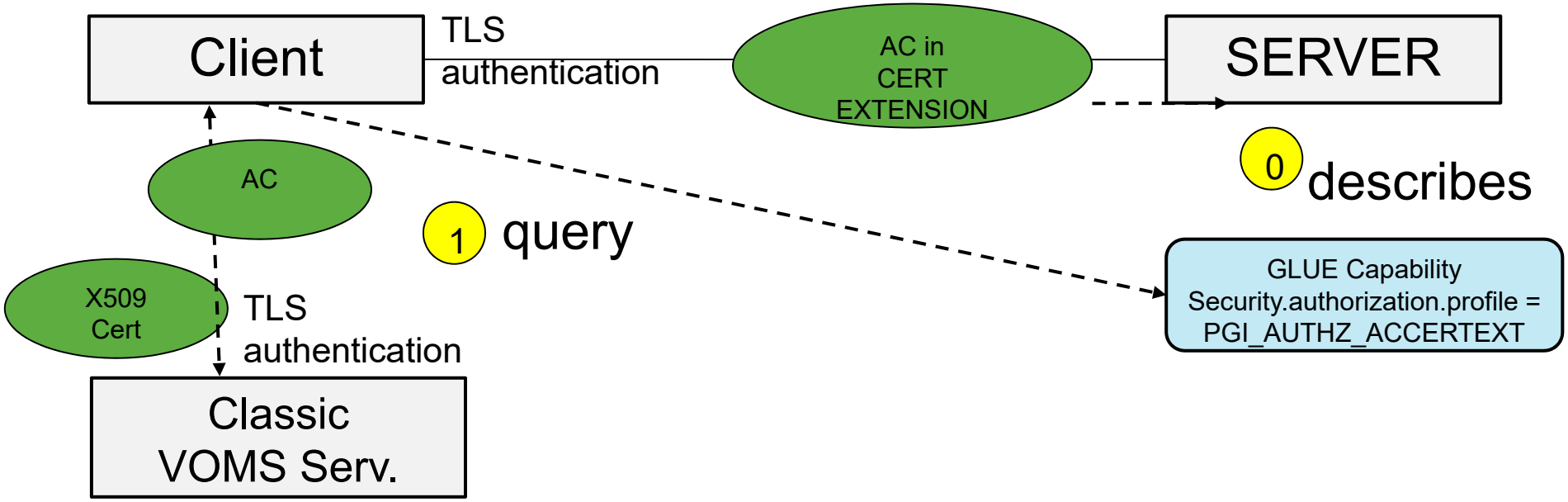
(2) SAML Assertion in SOAP Header



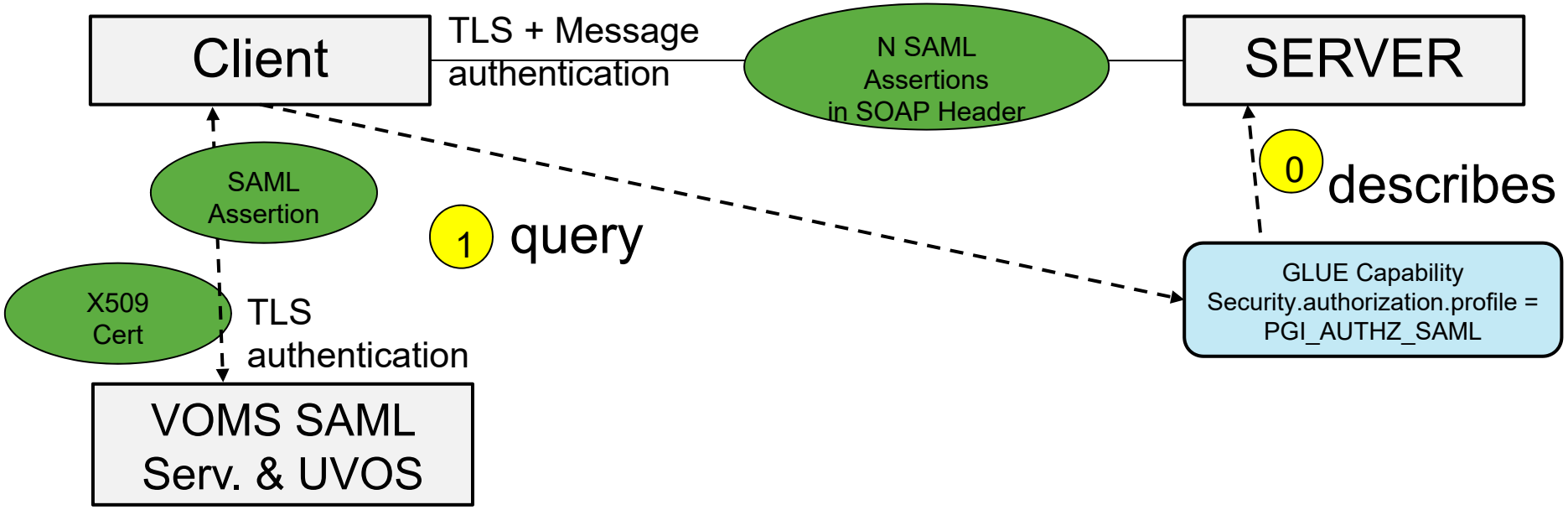
Two profiles for attribute based AuthZ

- Attribute Certificate (AC) – „Classic VOMS“ mechanism
  - Proxy certificate for transport layer authentication
  - One AC carried by proxy certificate
  - Third-party authority needed for AC issuing
  - Interface to „Classic VOMS“ is unfortunately proprietary
- SAML (Attribute) Assertions carried by SAML Tokens
  - SAML Token for message (SOAP) layer authentication
  - Third-party authority needed for SAML assertion issuing
  - If message layer authentication needs to be achieved, the SAML assertion should include <saml:Subject/> for subject confirmation
  - VOMS SAML service can be extended to support this profile by providing 'SAML Token profile' compliant SAML Token
  - Interface to UVOS/SAML-based VOMS is standard (SAML)

AC Certificates in Extension



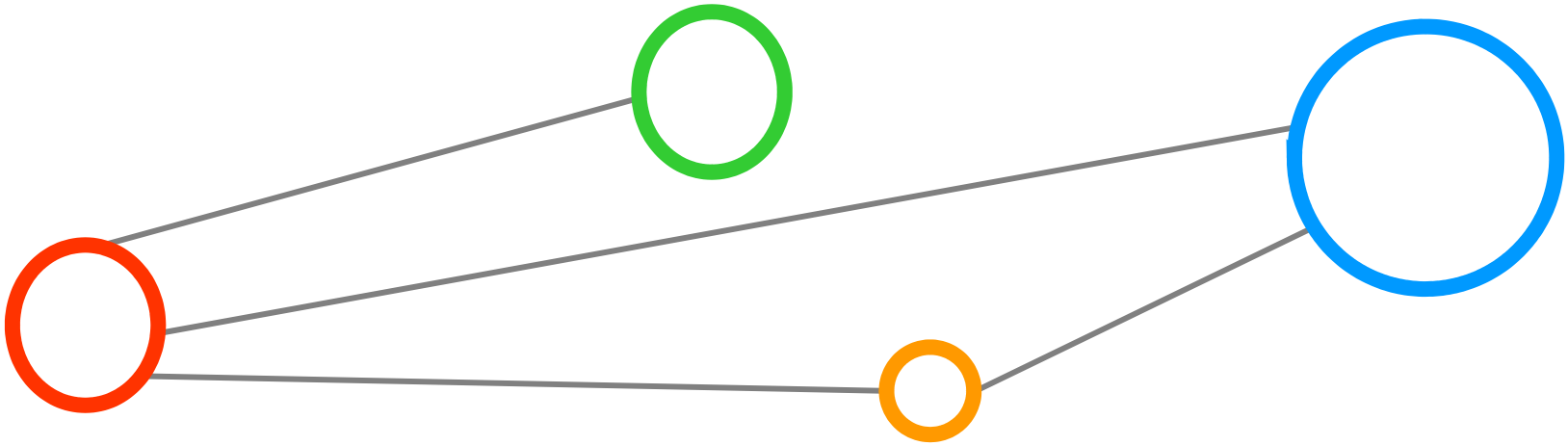
SAML Assertion in SOAP Header



Combination of Both

- PGI mandates to use at least one of the AUTHZ plumbings
  - Ensures a better interoperability then before (although not completely interoperability coverage)
- In principle we can apply (2) and (3) both together
  - UNICORE implements (2) with openssl proxies and (3) SAML assertions in one container (AC support planned)
- So using jointly the plumbings where necessary
  - PGI_AUTHZ_ACCERTEXT together with
  - PGI_AUTHZ_SAML

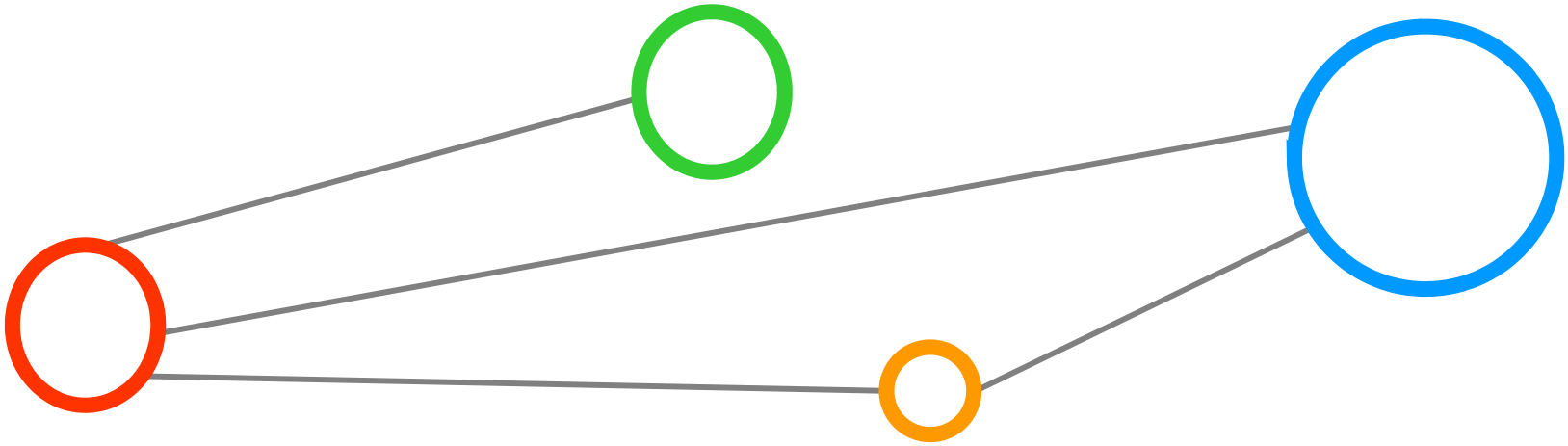
Common Attributes



Common Attributes

- Goal: common understanding and agreement of syntax and semantics of attributes between Grids
  - Technically oriented – does not deal with usage policies, etc.)
- Aspects of mapping between EGEE VOs and DEISA DECI Projects have been partly done also in JSPG
  - Open questions are virtual communities (Fusion, Virtual Physiological Human, etc.) that are different from DECI projects
- VOMS Format defines one possible FQAN syntax & semantics
  - No official standard document for it yet – work in progress…
  - Focussed on needs of EGEE and NDGF, some work has to be done to map needs of other infrastructures (i.e. DEISA, PRACE)

Constraints/Restrictions



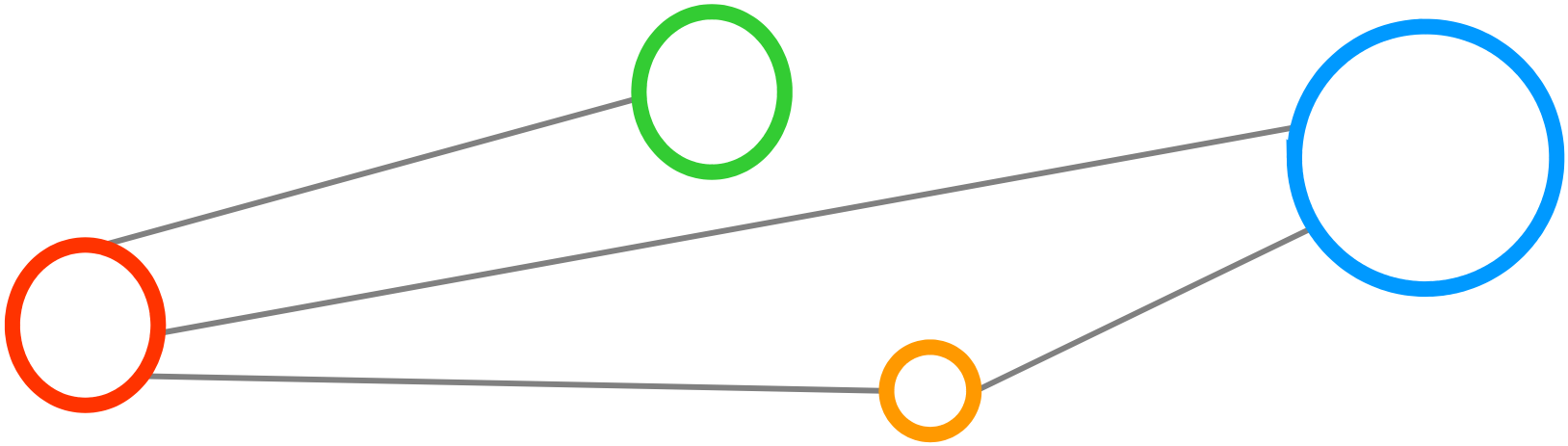
Constraints/Restrictions (1)

- SAML assertions with constraints
  - Initial experience with UNICORE (could be more)
  - Got feedback that the medical work in hospitals also rely on SAML → Here security is the most important aspect for patients
- Work from S.Cantor et al. „SAML 2.0 Single Sign-On with Constrained Delegation“
  - The person that delegates put in SAML Assertion:
    <saml:SubjectConfirmation> → Name, KeyInfo, etc. of him (aka ‘WHO delegates’)
  - The person additionally put in the SAML Assertion:
    <saml:AudienceRestriction> → used to indicate for what the assertion is actually used for AuthZ/AuthN or to whom further delegation can be performed
    - Maybe even ‘Grid actions’ can be put: Read/Write Data, Job Submission only, etc. or even specific endpoints can be mentioned
  - Plus: Attributes allows for fine-tuning about the assertion

Constraints/Restrictions (2)

- Proxies with Restrictions
  - Many different working aspects can be found it this context
  - All use the extensions in proxies for definitions
  - Globus does also work on this topic a long time ago
- Why was this never considered for production?
  - Why it is not supported? → Never had strong user requirements
  - Not in EGEE3 lifetime – maybe later?! Matter of priorities…
  - A matter of priorities and not many resource providers require it
  - Manpower issues, also it should be clarified if resource owners would like to do this
  - Hurdle to implement this is very high (for each application in VO)
- PGI common way of defining restrictions across Grids (?)

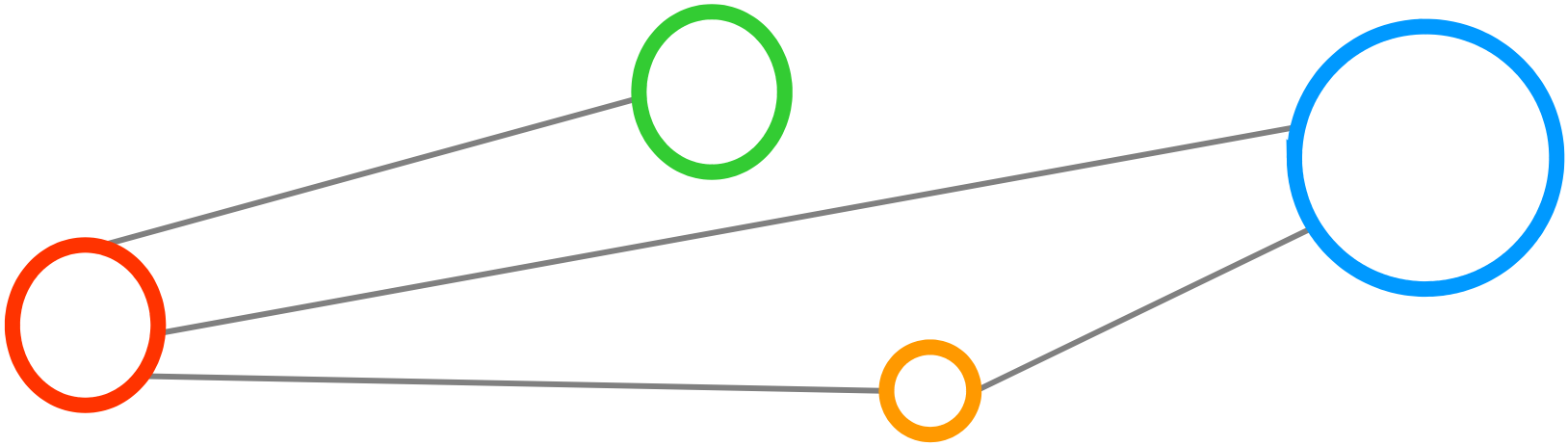
Out of Scope



Out of Scope

- Standardization on profiles that retrieve attributes from Attribute Authorities (AAs)
  - How end-users obtain there attributes is out of scope of PGI
  - Nevertheless we seek to use standard interfaces here (e.g. SAML)
- Specific policy technologies and definitions
  - How specific policies, (e.g. XACML policies) are defined is out of scope of PGI, but in general push standards where possible
- Ressource usage policy of production infrastructures
  - The policy of how and if end-users can use cross-Grid resources is out of scope of PGI (political level rather then technical level)

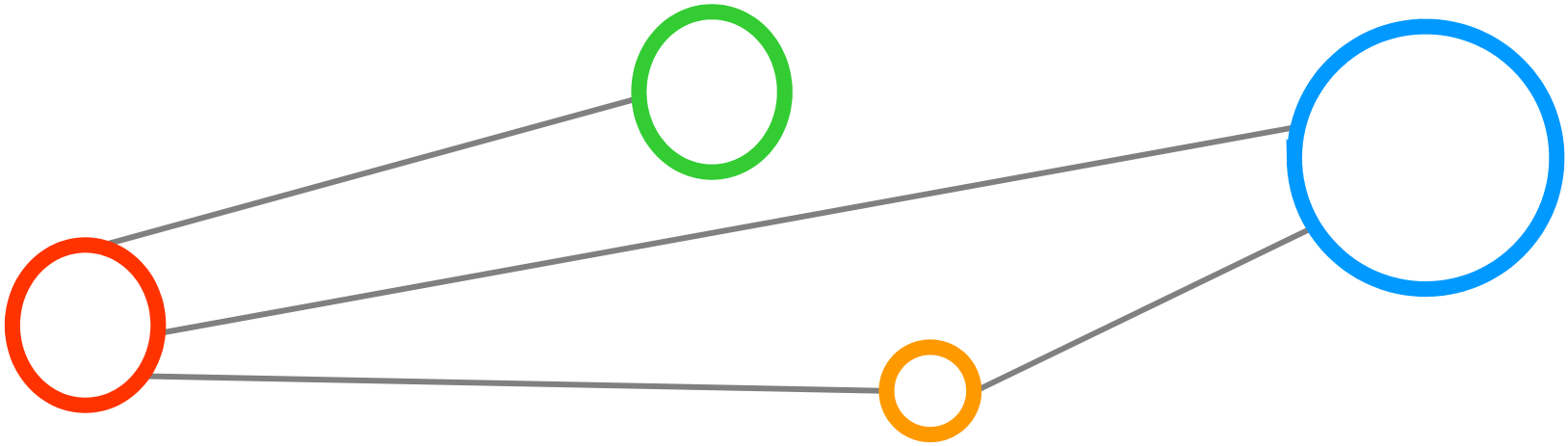
EMI in Context



EMI in Context

- European Middleware Initiative (EMI) Project Proposal
  - → Visit our EMI sessions on Thursday at EGEE 2009!
- gLite, ARC, UNICORE and other middleware already work closely together in EMI
  - First agreements on how a future common PGI security standard should look like, aligned with compute, information, data, …
- EMI will try to leverage and drive the PGI activities
- Major difference between PGI and EMI: in OGF PGI we have „no money“, but EMI has „a little bit of money“
- E.g. „little“ change picture: Some SRM implementations will be PGI-compliant moving away from GSI, hopefully forcing other SRM implementations to follow

Conclusions



Conclusions

- Changes in Security Models take a very long time
  - Compare to switch from GLUE information models → years!
- We basically more or less survey what security setups is used in production Grids currently
  - We thus not define a large security framework
  - We focus on elements used in production already or (very soon in production) with a general move away from GSI and to SAML
- The main achievements in our group is agreement about certain important elements / standards
  - E.g. BES, SRM, GridFTP, GLUE, JSDL, etc.
  - Work on missing links between them
  - Work on tunings / refinements of them
  - Pushing back elements back to the open standards itself

Full Copyright Notice