Production Grid Infrastructure WG
PGI Security Considerations

Thoughts about common security profiles

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

© 2008 Open Grid Forum

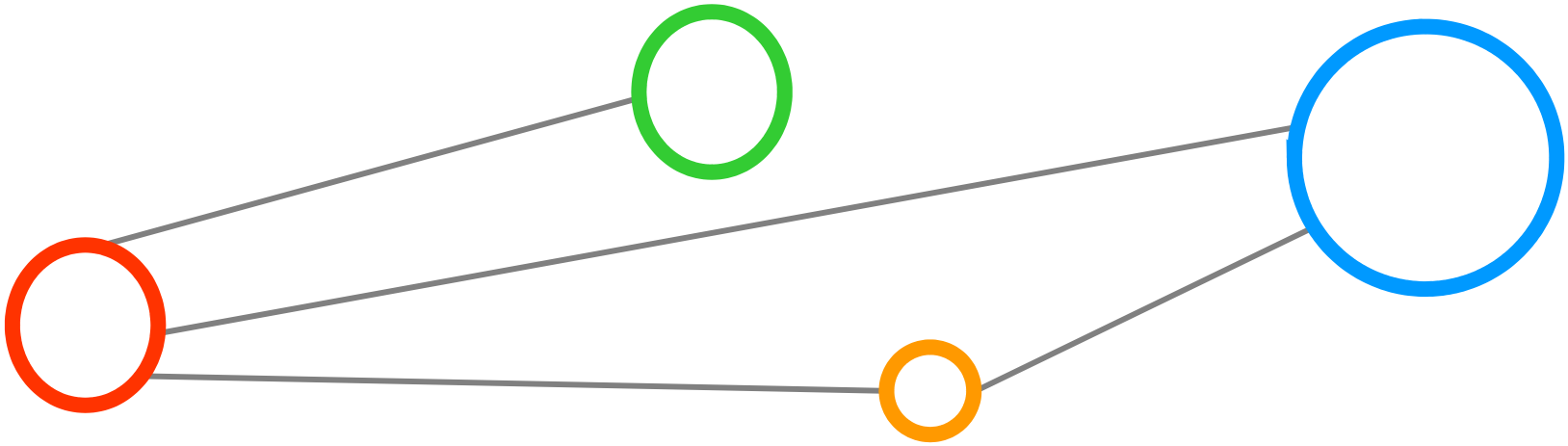
OGF IPR Policies Apply

- "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.

© 2008 Open Grid Forum

Outline



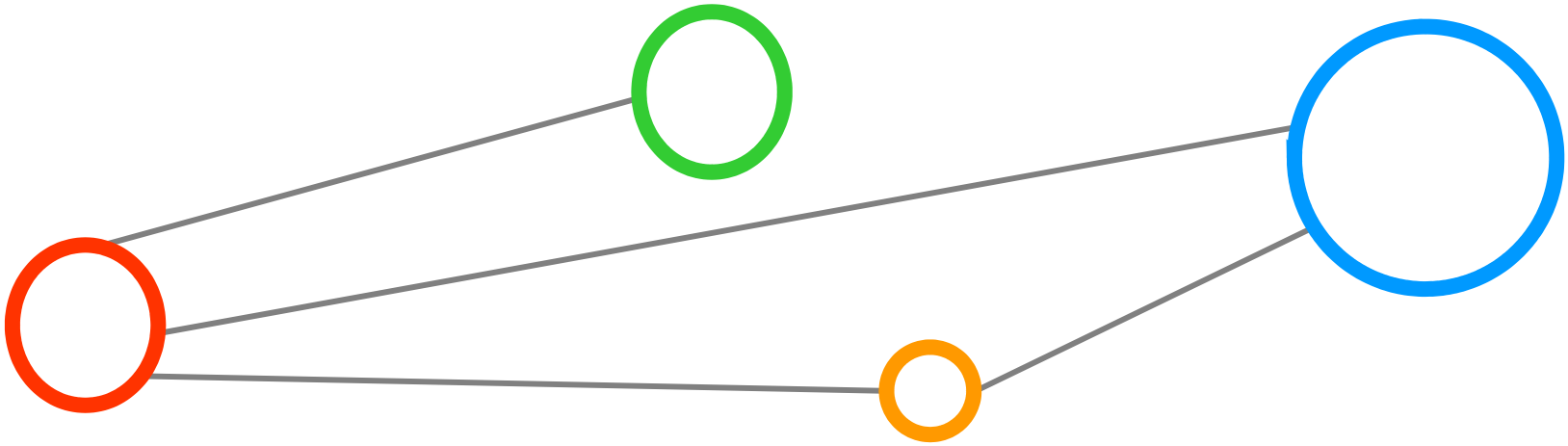
© 2008 Open Grid Forum

Outline

- OGF PGI 101
- 3 ‚Plumbings‘ for Authentication
- 2 ‚Plumbings for Attribute-based Authorization
- Common attributes
- Common constraints/restrictions
- Out of Scope
- Discussions
- Conclusions

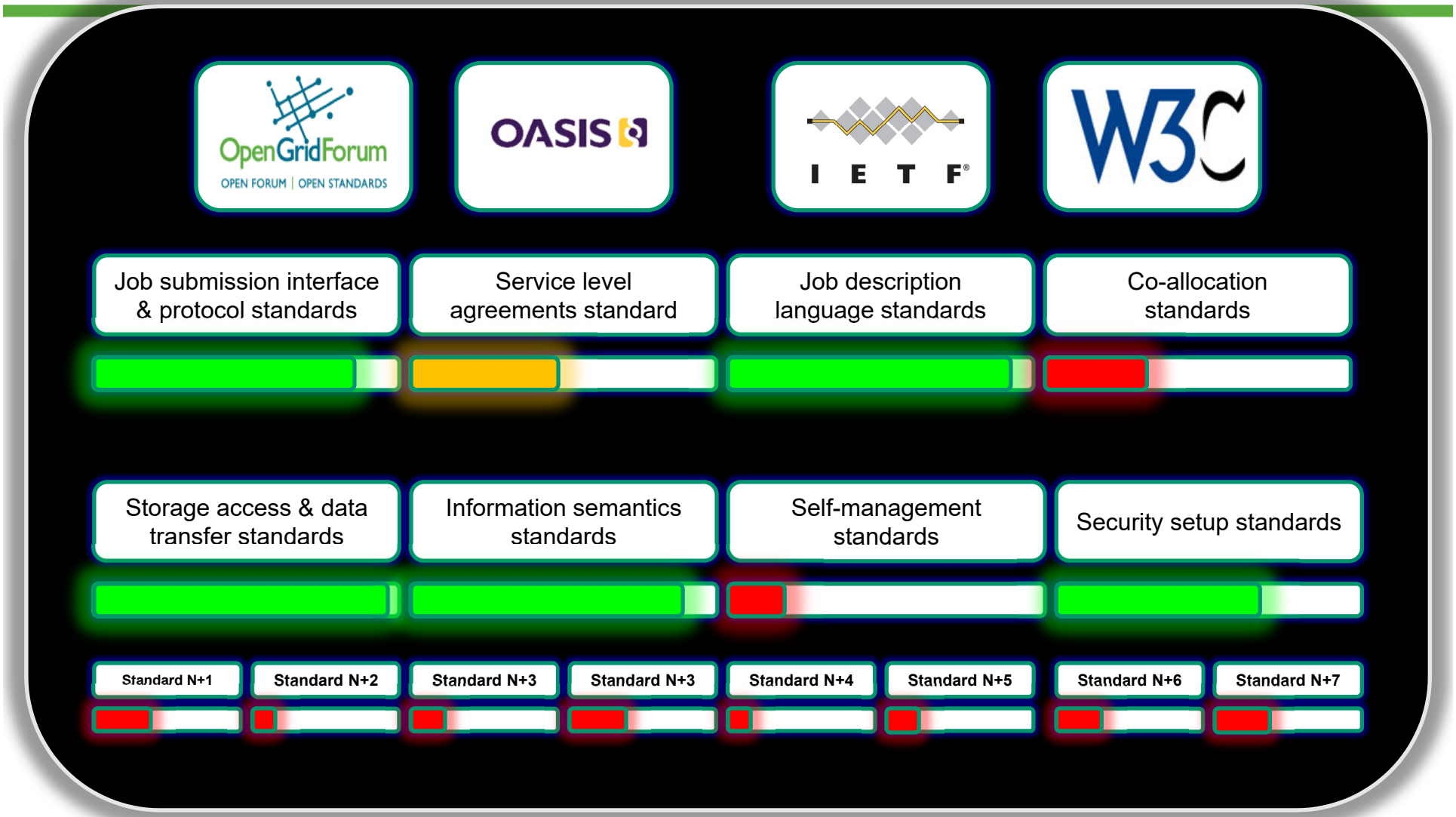
© 2008 Open Grid Forum

OGF PGI 101



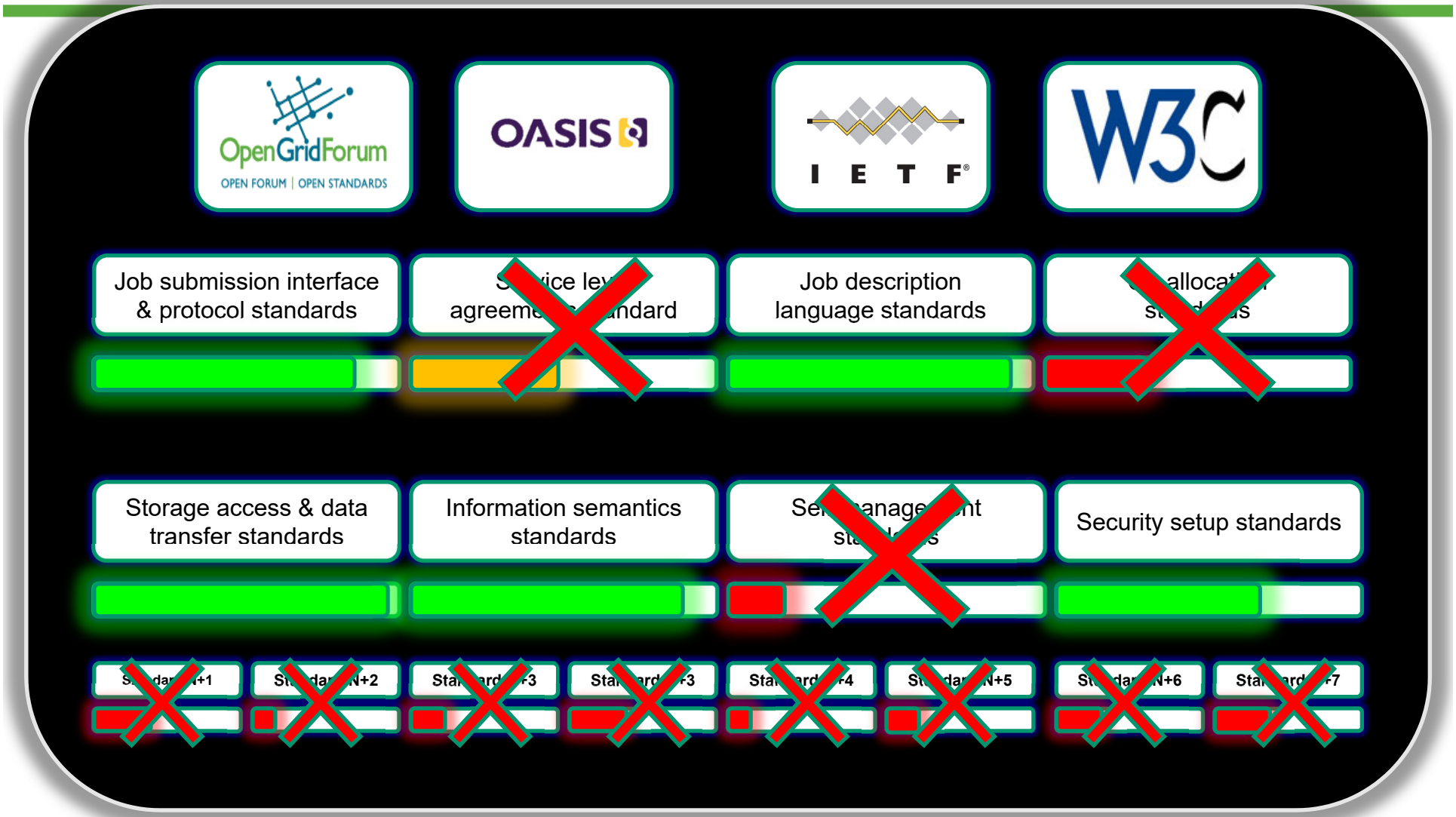
© 2008 Open Grid Forum

OGSA Standards



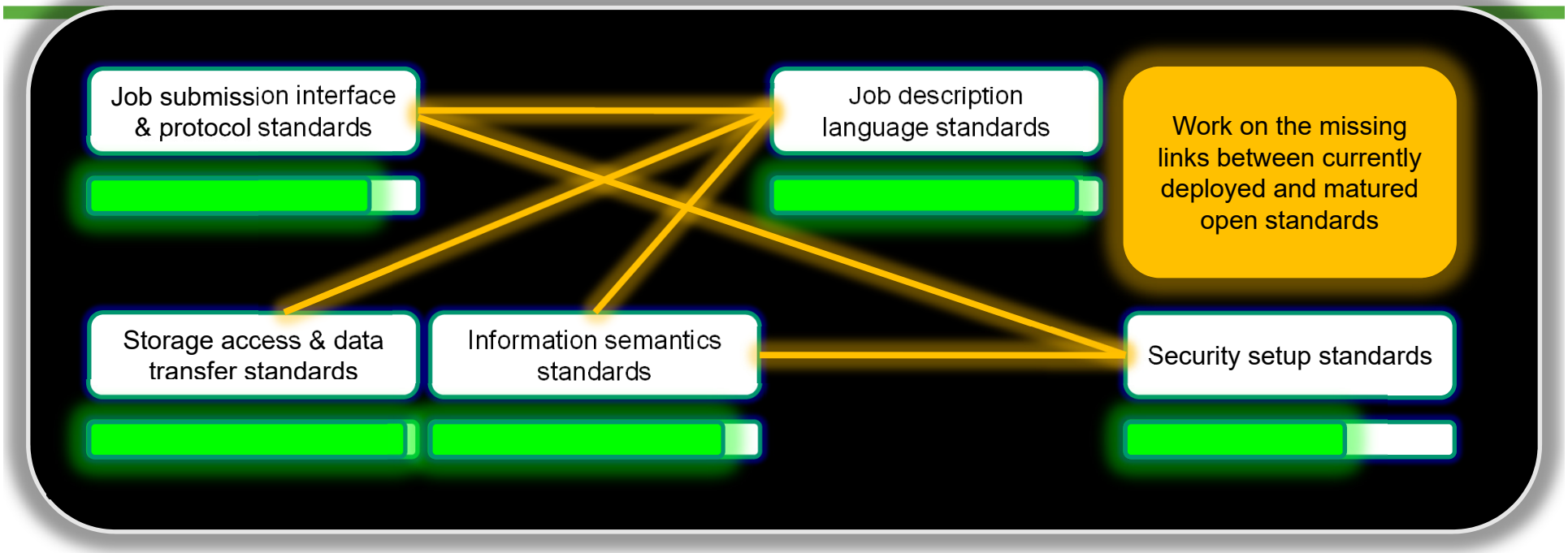
[7] Foster et al., *'The Open Grid Services Architecture'*

GIN Production Experience



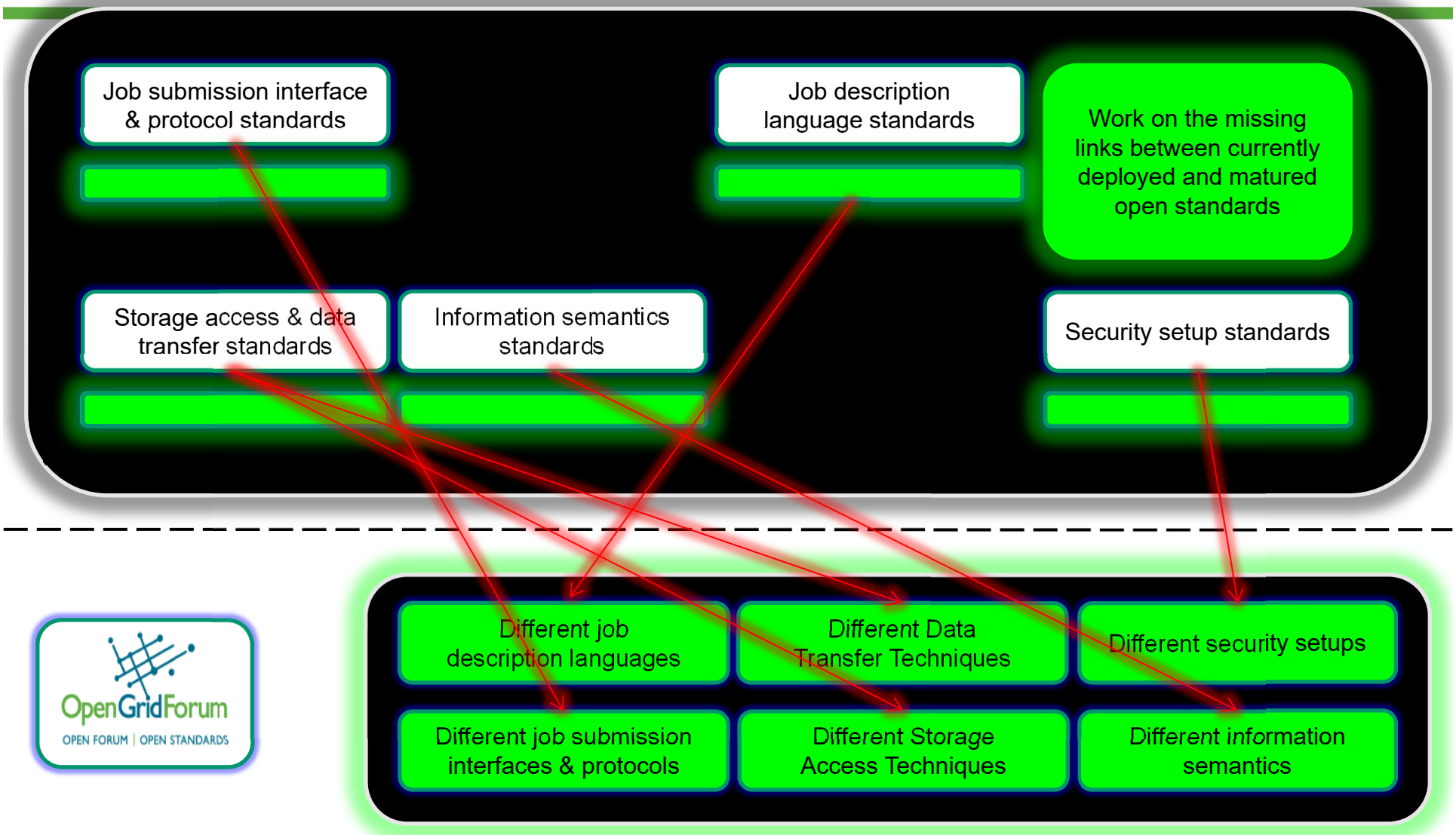
[8] Riedel et al., *'Interoperation of World-Wide Production e-Science Infrastructures '*

PGI Approach (1)



© 2008 Open Grid Forum

PGI Approach (2)



[5] Riedel et al., *'Experiences and Requirements for Interoperability between HTC- and HPC-driven e-Science Infrastructures'*

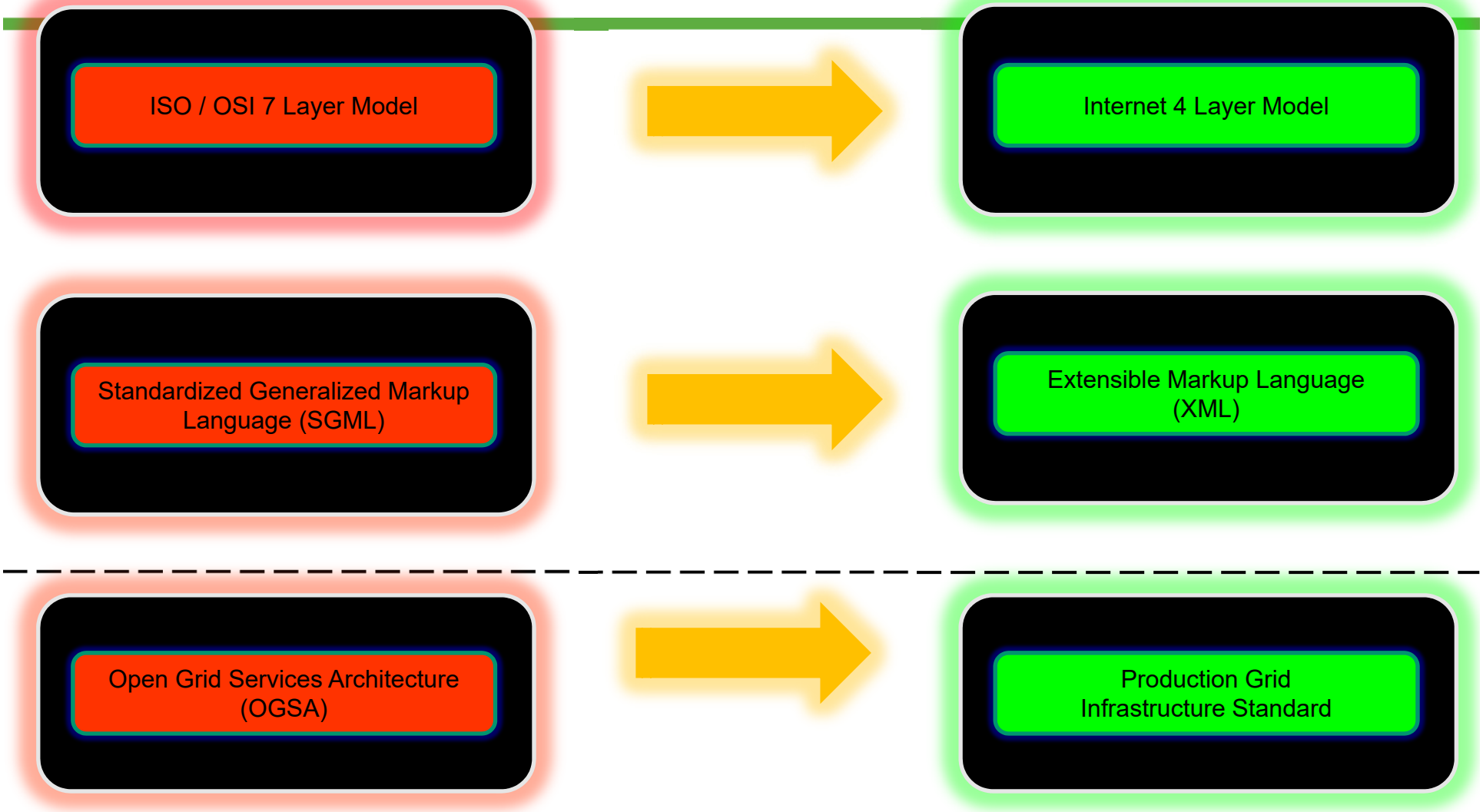
Scope

- 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'

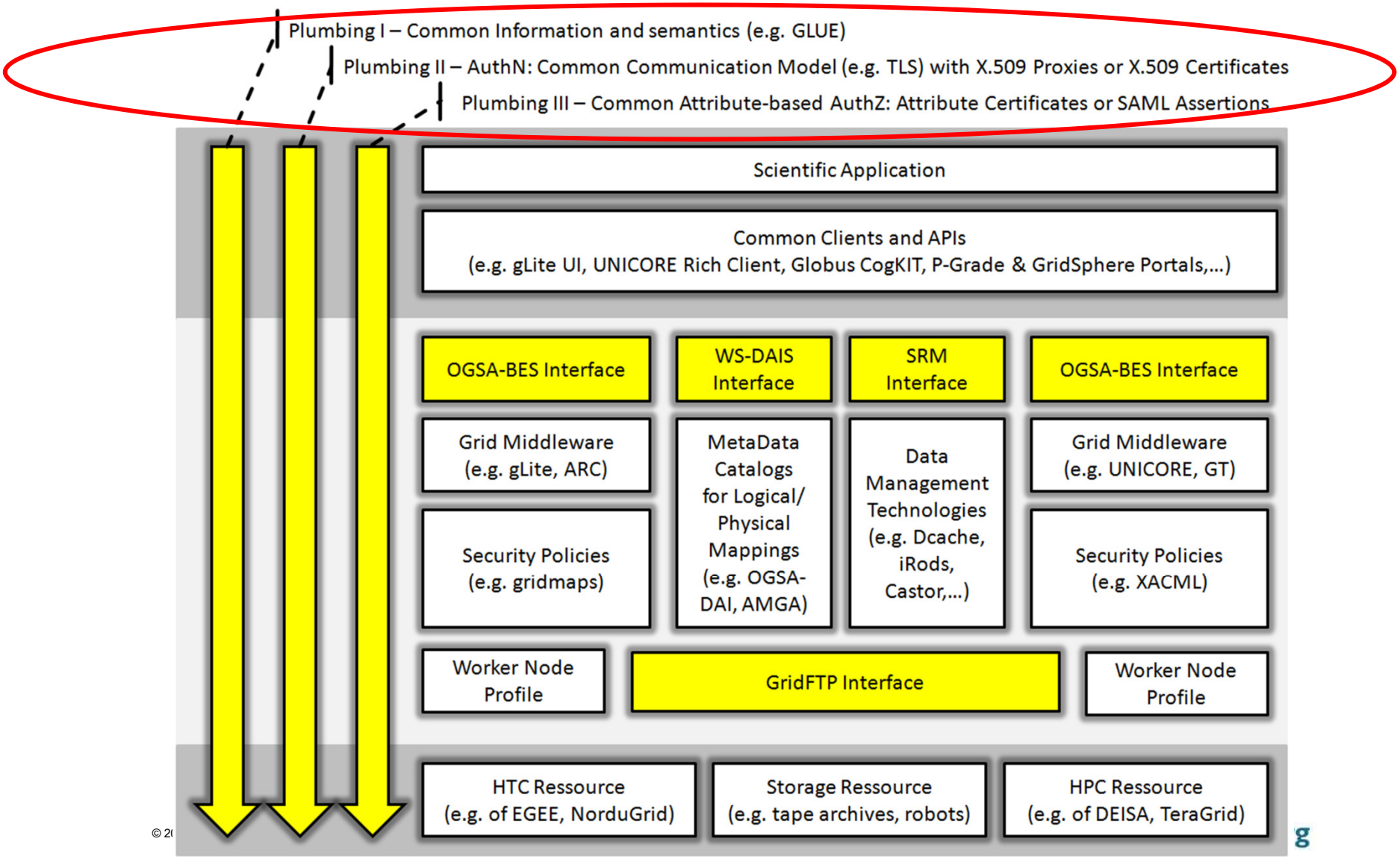
© 2008 Open Grid Forum

Compare History of Computer Science



© 2008 Open Grid Forum

PGI Ecosystem Overview

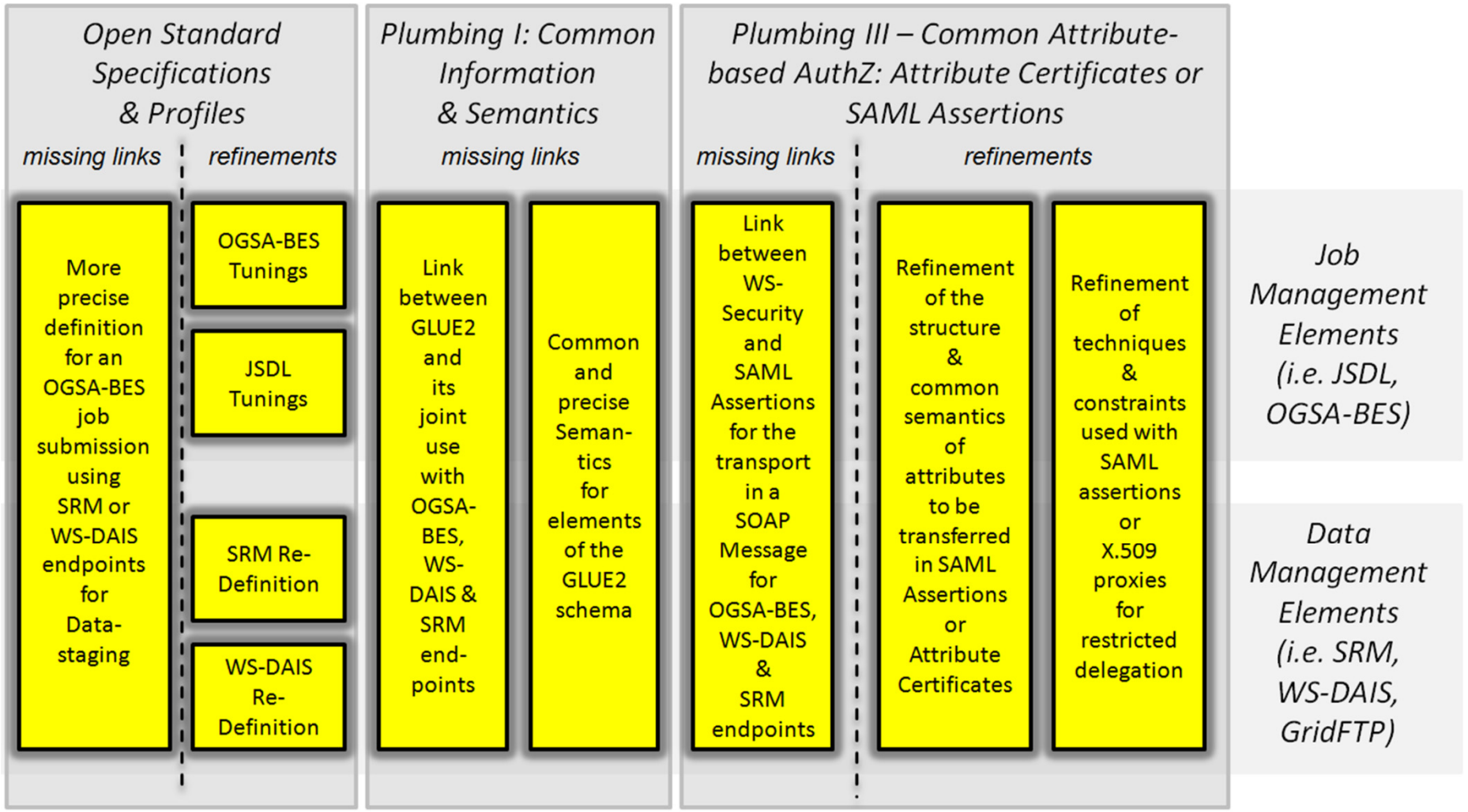


Plumbings Idea

- Plumbings can be used to put different ‚elements' through
  - E.g. warm water (realizing normal OpenSSL-TLS connections) vs. Cold water (realizing GSI connections)
- Many plumbings can be installed in parallel – while not crossing the other 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

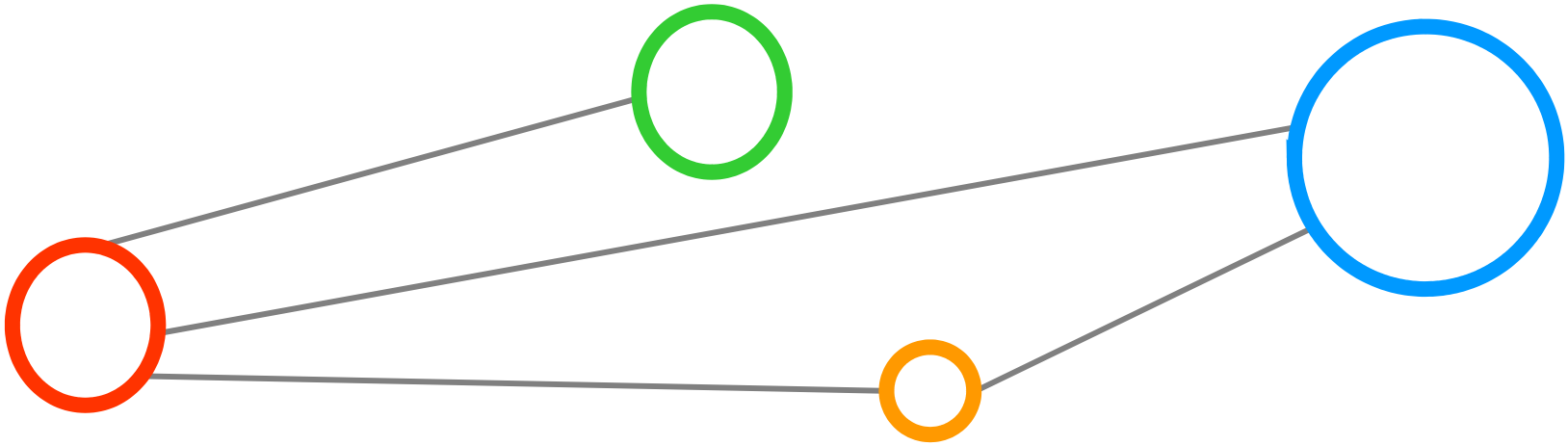
© 2008 Open Grid Forum

Missing Links & Refinements



© 2008 Open Grid Forum

3 Plumbings for Authentication



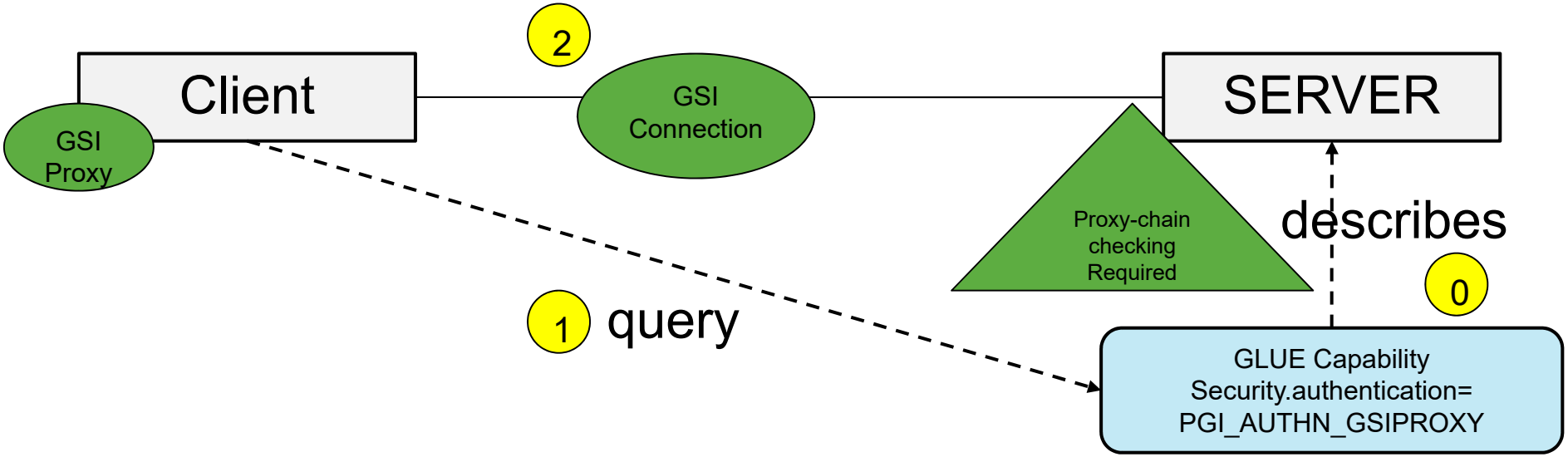
© 2008 Open Grid Forum

TLS with GSI Proxies

- GSI-based TLS is not compatible with OpenSSL TLS
  - Fixed with Globus Version 4 (*probably should be mentioned like this: It is possible to make GSI-based TLS be compatible with OpenSSL TLS, since even in GT4 (or later version), you still need to setup an environment variable to switch on compatible TLS*)
  - (a full end-entity X.509 certificate can‘t be used with this and fails) (*a full end-entity X.509 certificate actually can be used for GSI-based TLS, at least if the private key is not protected by passphrase, according to practice*) - but GSI libraries are required?!
- However, many production systems require still the GSI-based TLS
  - Proxies needed since the data staging might be delegated
  - For instance, current implementations of the SRM interface (same Web Service Level as Basic Execution Services)
  - Numerous GridFTP implementations

© 2008 Open Grid Forum

TLS with GSI Proxies



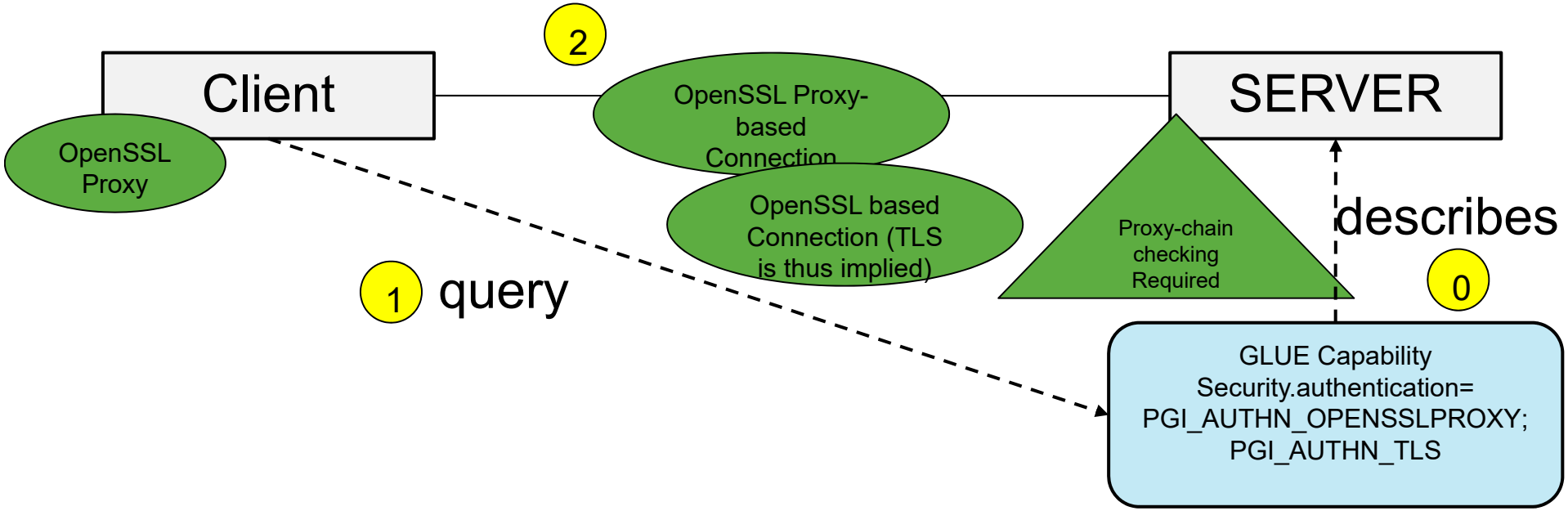
© 2008 Open Grid Forum

TLS with OpenSSL Proxies

- Service Container of NAREGI, ARC & gLite (CREAM-BES) 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
- 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

© 2008 Open Grid Forum

TLS with OpenSSL Proxies



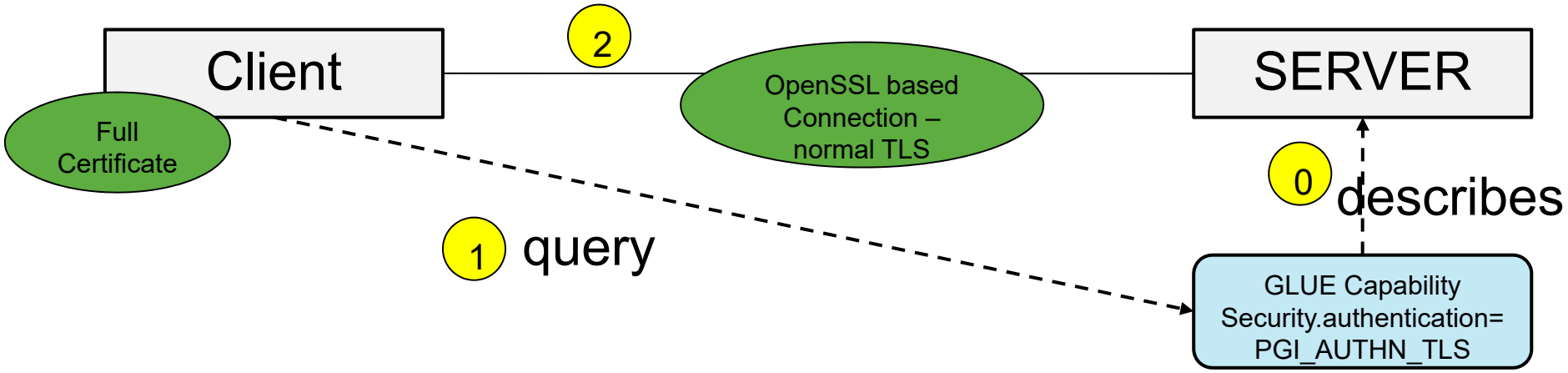
© 2008 Open Grid Forum

TLS with Full Certificates

- Service Container of UNICORE require TLS connections using full end-entity certificates
  - Service container could not work with proxies in this setup
  - proxy chain checking is not required!

© 2008 Open Grid Forum

TLS with Full Certificates



© 2008 Open Grid Forum

Message layer Authentication

- 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 AuthZ. SAML Token includes <saml:Subject> and <saml:Attribute> (see Web Services Security:SAML Token Profile V1.0)
    - The VOMS SAML Service can be enhanced to support this profile

© 2008 Open Grid Forum

```
<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>
```

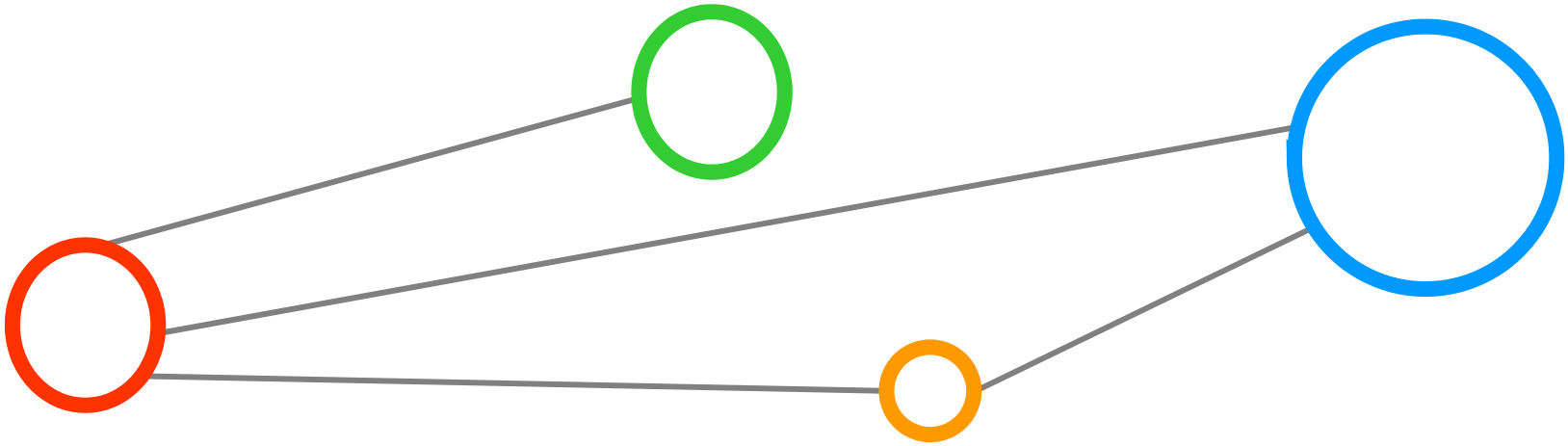
© 2008 Open Grid Forum

Message layer Authentication

- WS-Trust
  - 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.

© 2008 Open Grid Forum

2 Plumings for AuthZ



© 2008 Open Grid Forum

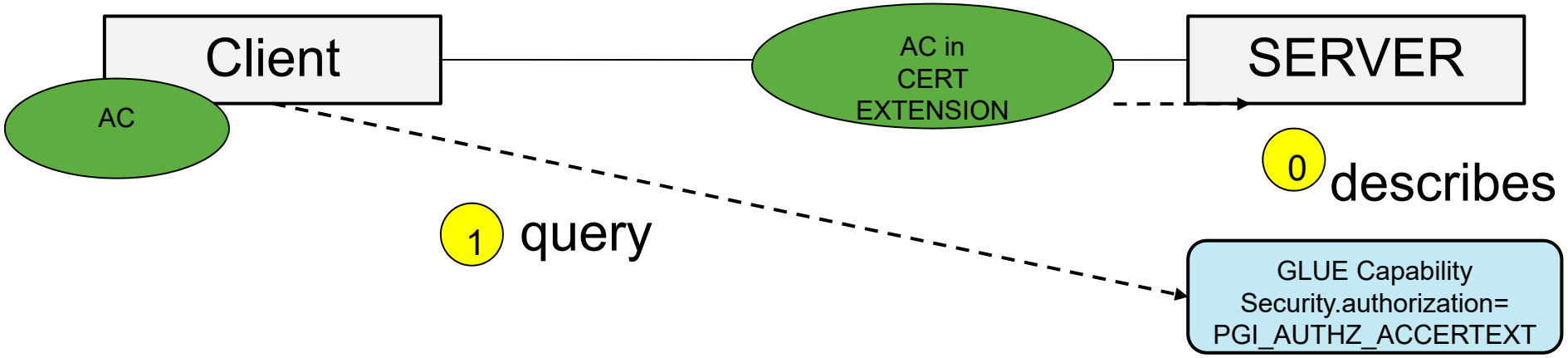
AC Certificates in Extensions

- Supporting legacy VOMS exposing ACs

- AC can be combined transported with any option used for AUTHENTICATION (*? should not the AC be transported through Proxy certificate's extension, and proxy is the only option for authentication in this case?*)

© 2008 Open Grid Forum

AC Certificates in Extension



© 2008 Open Grid Forum

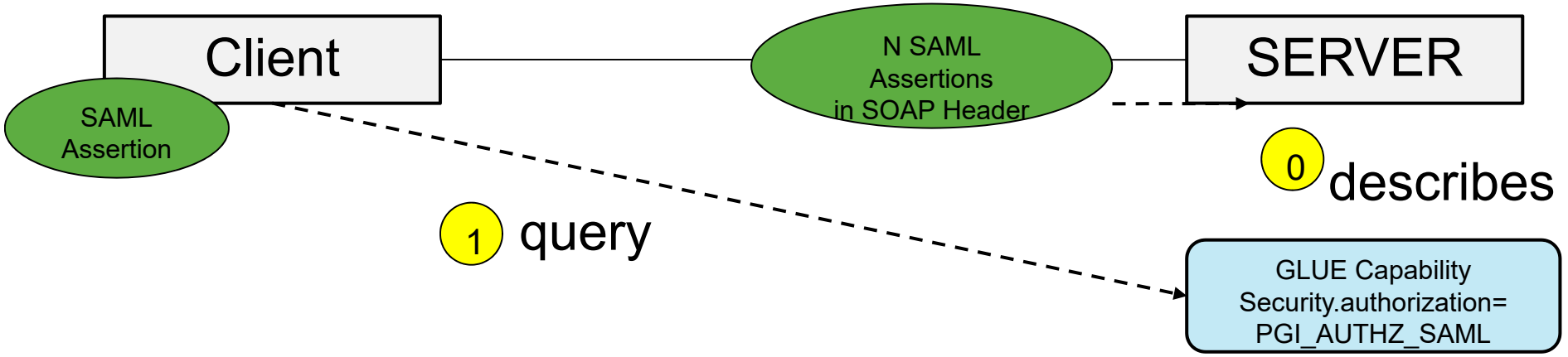
SAML Assertions in SOAP Header

- Supporting SAML-based VOMS exposing SAML assertions

- SAML assertions can be combined transported with any option used for AUTHENTICATION (*?What are the options? SAML token (SAML attributes are inside SAML token) for SOAP message layer authentication; and Proxy certificate (SAML attributes are as proxy extension) for transport layer authentication?*)

© 2008 Open Grid Forum

SAML Assertion in SOAP Header



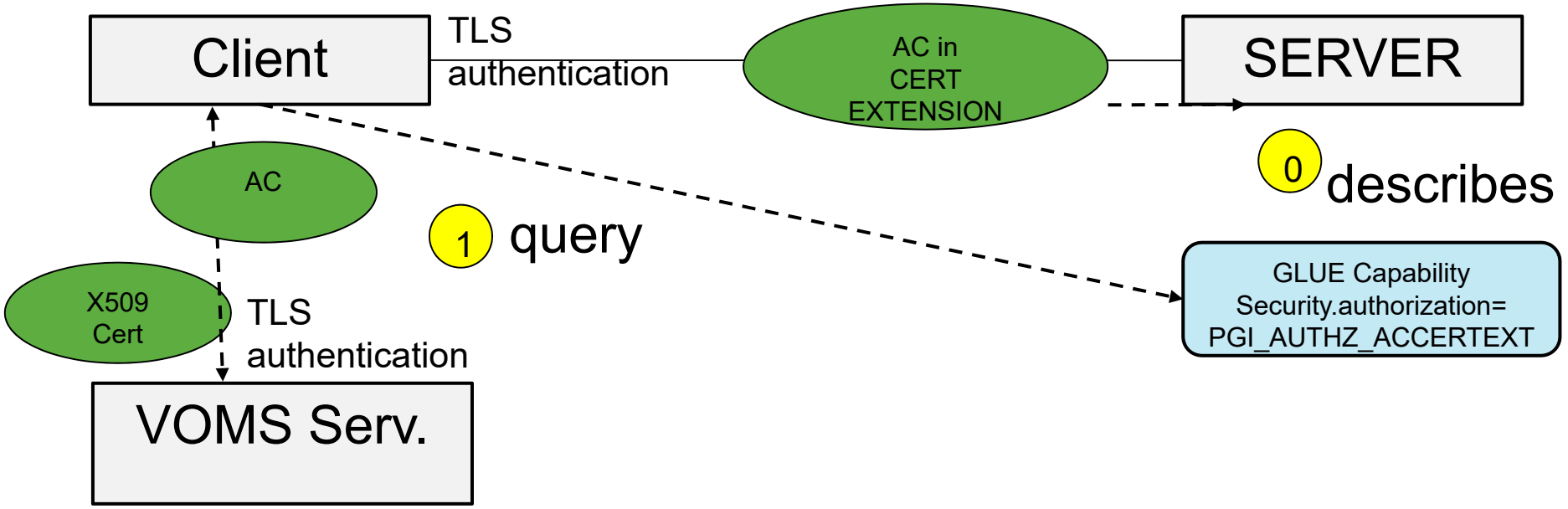
© 2008 Open Grid Forum

Two profiles for attribute based AuthZ

- a. Attribute Certificate (AC) --- VOMS mechanism
  - Proxy certificate for transport layer authentication
  - AC carried by proxy certificate
  - Third-party authority needed for AC issuing
- b. SAML assertion
  - SAML Token for message (SOAP) layer authentication
  - SAML attribute assertion carried by SAML Token
  - Third-party authority needed for SAML assertion issuing
  - Different from 'a', 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

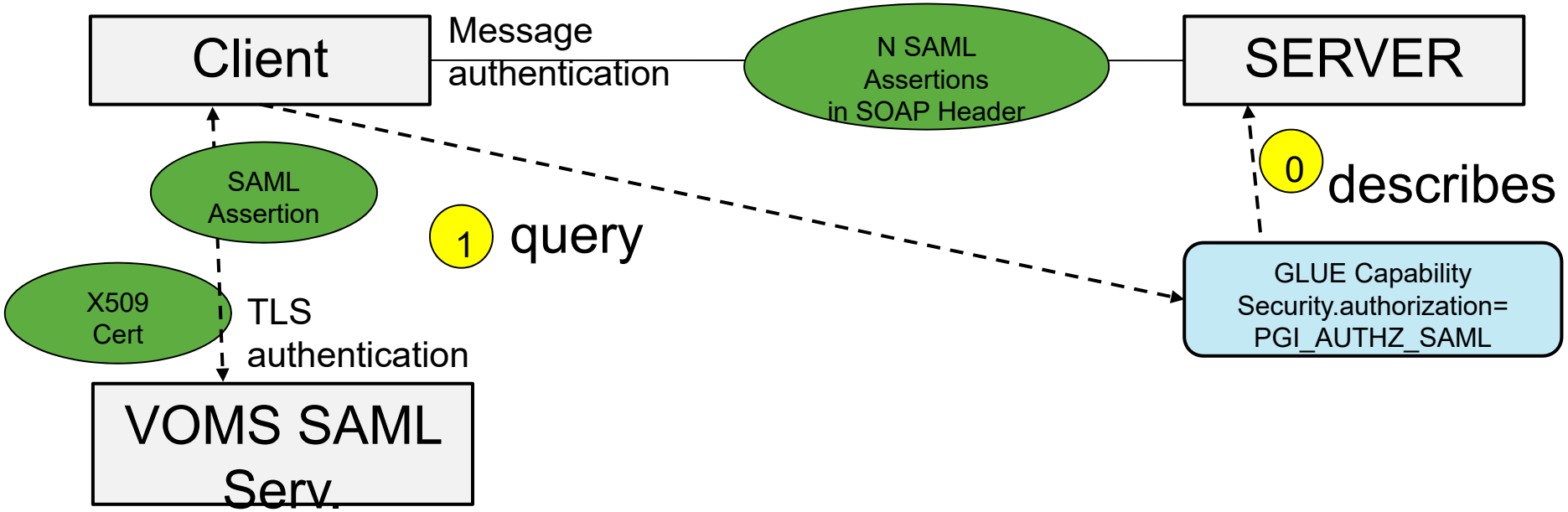
© 2008 Open Grid Forum

AC Certificates in Extension



© 2008 Open Grid Forum

SAML Assertion in SOAP Header



© 2008 Open Grid Forum

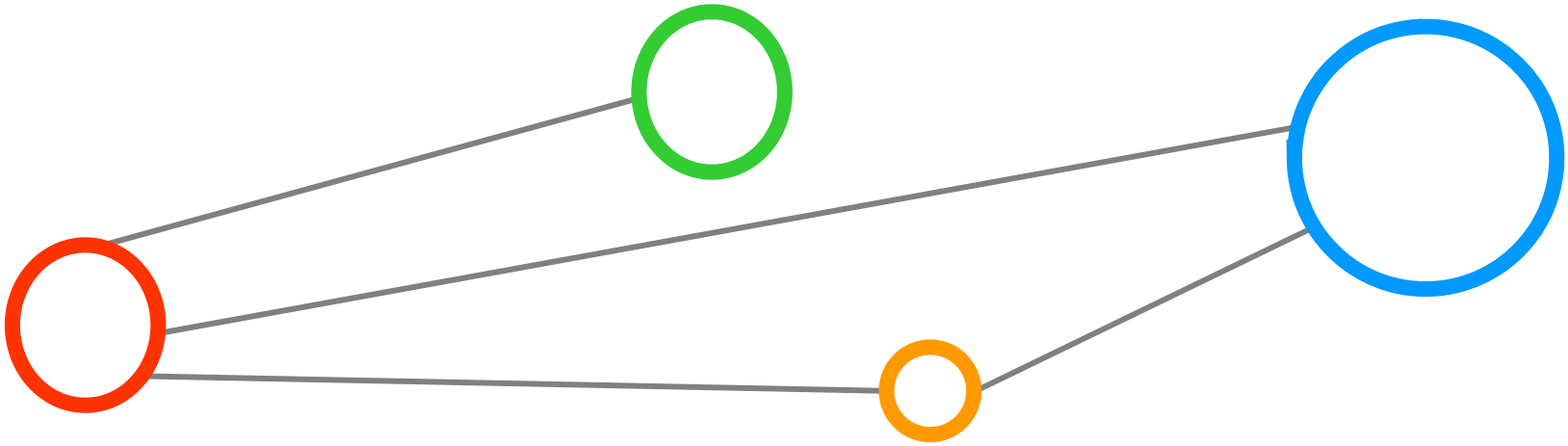
Combination of Both

- PGI mandates to use at least one of the AUTHZ plumbings should be used
- But in principle we can apply both together

- So using jointly the plumbing PGI_AUTHZ_ACCERTEXT together with PGI_AUTHZ_SAML

© 2008 Open Grid Forum

Common Attributes



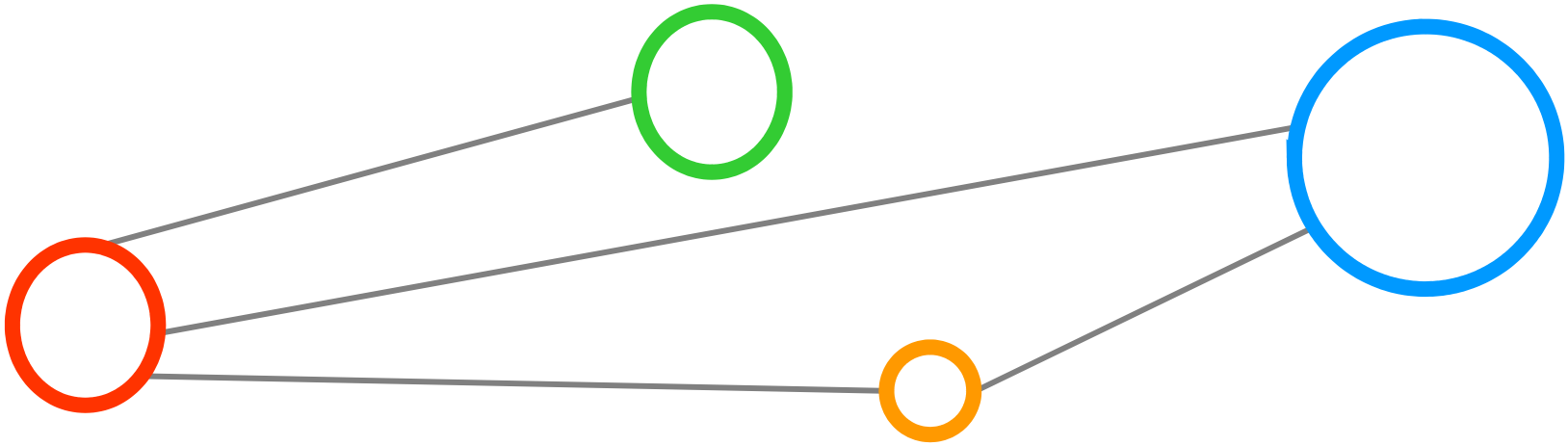
© 2008 Open Grid Forum

Common Attributes

- TBD

© 2008 Open Grid Forum

Common Constraints/Restrictions



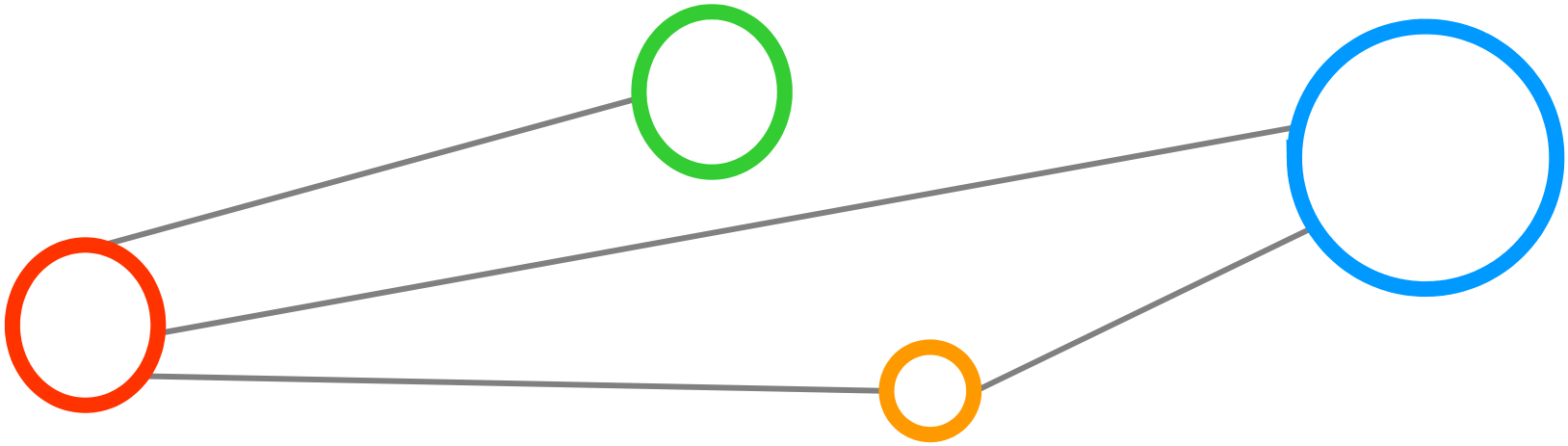
© 2008 Open Grid Forum

Common Constraints/Restrictions

- TBD

© 2008 Open Grid Forum

Out of Scope



© 2008 Open Grid Forum

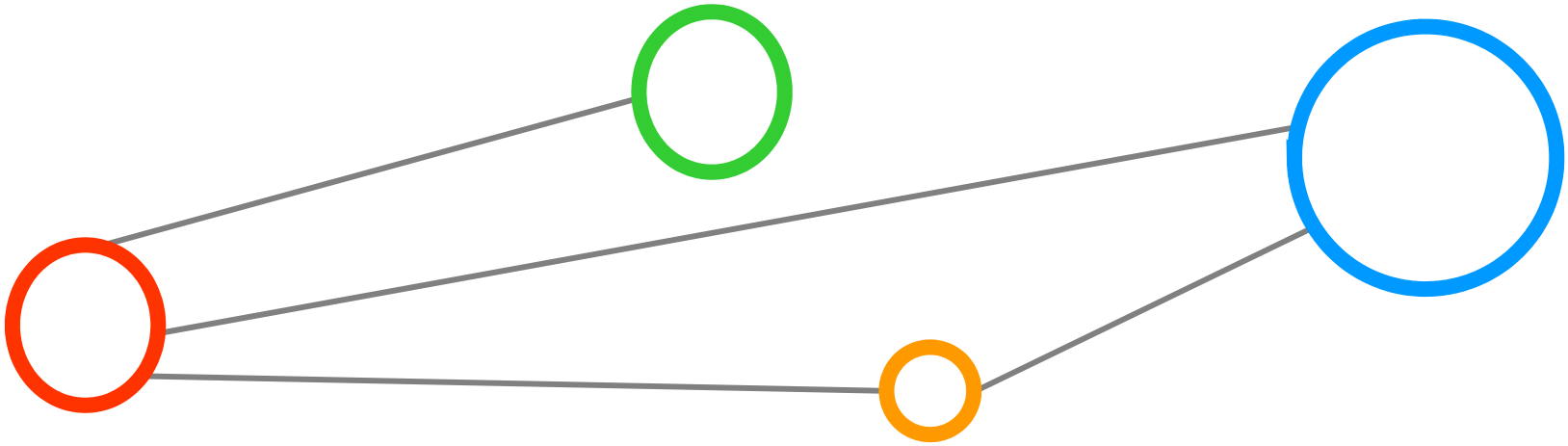
Out of Scope

- Standardization on profiles that retrieve attributes from Attribute Authorities (Aas)
  - How end-users obtain there attributes is out of scope of PGI
- Specific policy technologies and definitions
  - How specific policies, (e.g. XACML policies) are defined is out of scope of PGI

- Usage policy of production infrastructures
  - The policy of how and if end-users can use cross-Grid resources is out of scope of PGI

© 2008 Open Grid Forum

Conclusions



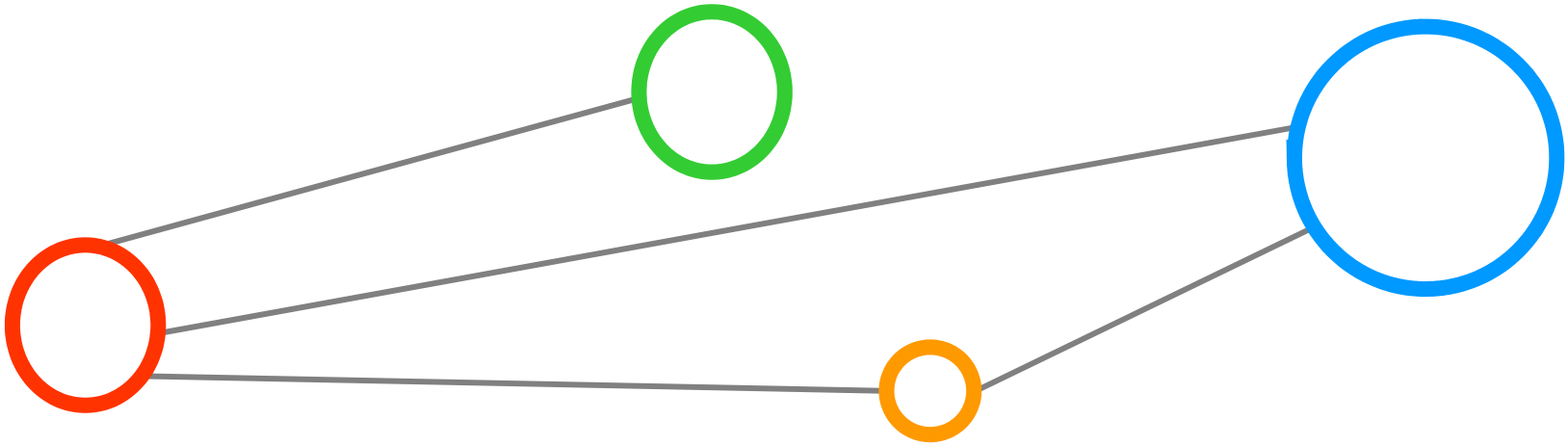
© 2008 Open Grid Forum

Conclusions

- 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)
- The main achievements in our group is agreement about certain important elements / standards
  - E.g. BES, SRM, GridFTP, GLUE, …
  - Work on missing links between them
  - Work on tunings / refinements /re-allignments of them

© 2008 Open Grid Forum

Discussions



© 2008 Open Grid Forum

Discussions

- TBD

© 2008 Open Grid Forum

Full Copyright Notice

Copyright (C) Open Grid Forum (2009). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works.

The limited permissions granted above are perpetual and will not be revoked by the OGF or its successors or assignees.