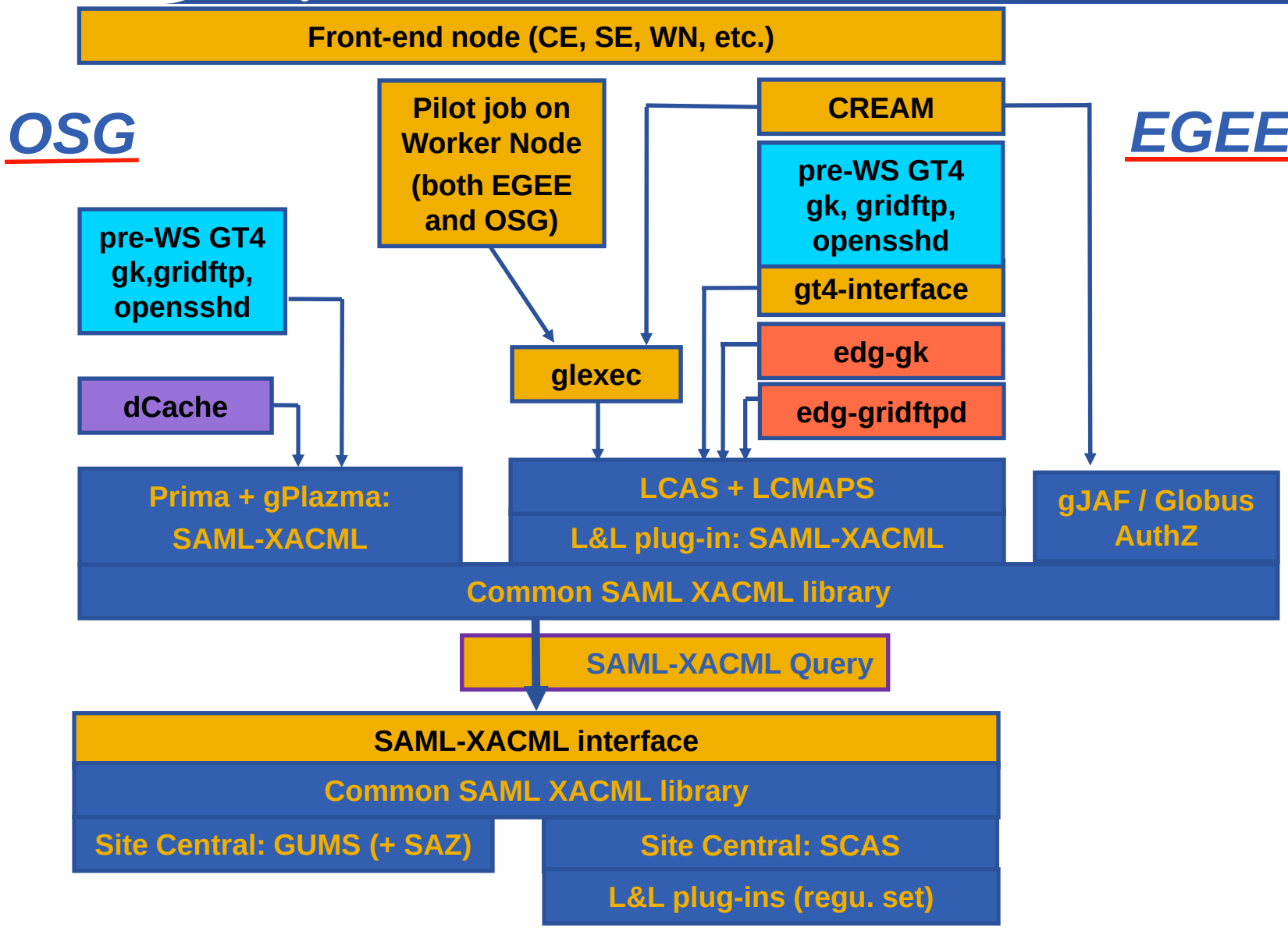
AuthZ Interop: A common XACML Profile

(Bonus material about the implementation)

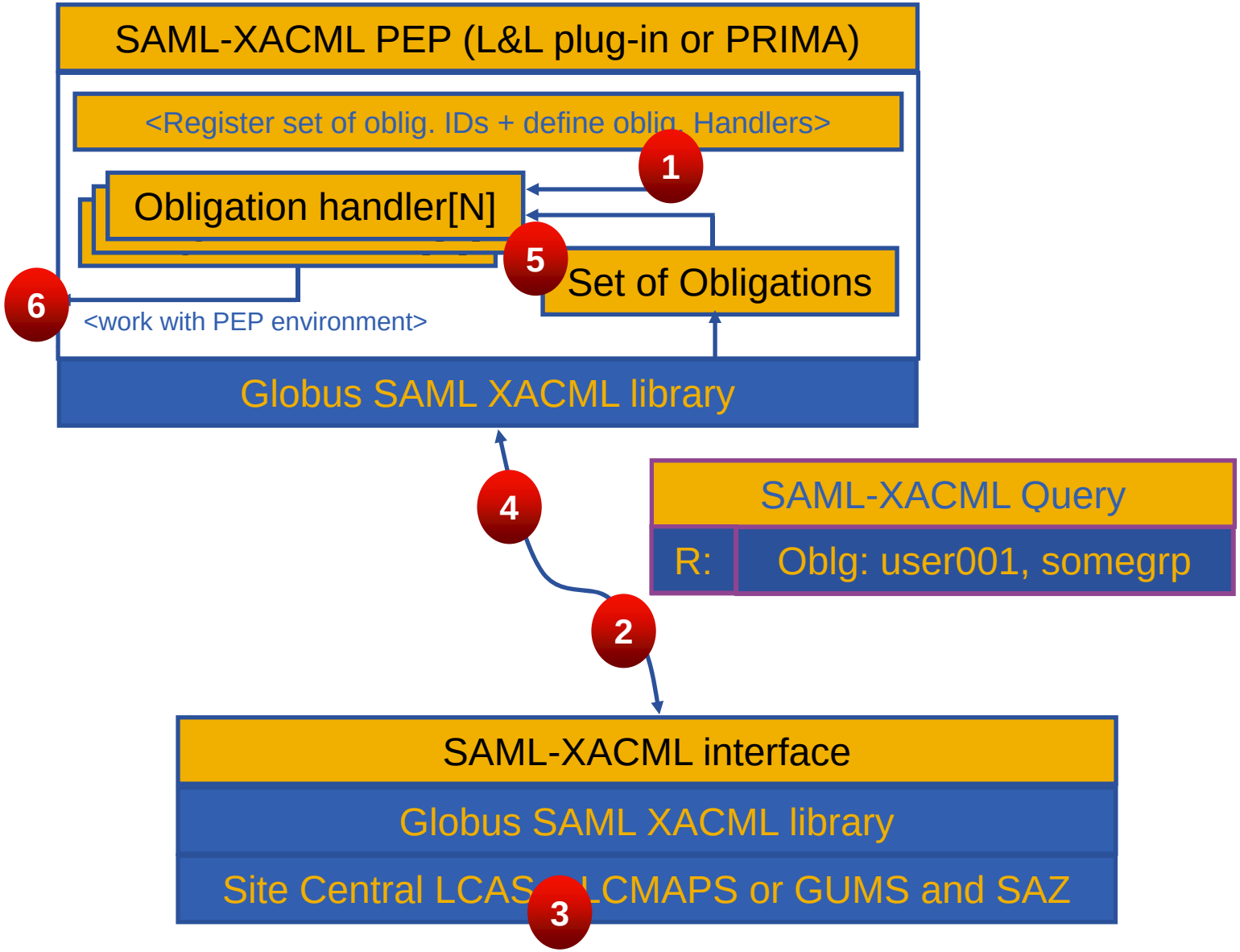
Oscar Koeroo

The architecture

Scope: on *one* site



How it should work (conceptual)



The paper work

Namespace

- **URI choice: URN vs. URL ⇒ URL won**
  - URL-style doesn't require centralized registration
  - Can be established by registering the (relevant) domain name to ensure uniqueness
- **Our registered Namespace (owned by David Groep):**
  - http://authz-interop.org/
- **Root namespace prefix for all our message elements:**
  - http://authz-interop.org/xacml/2.0

Request Attributes:

Namespace prefix construction:

Subject: <root-ns-prefix>/subject

Action: <root-ns-prefix>/action

Resource: <root-ns-prefix>/resource

Environment: <root-ns-prefix>/environment

Overview of Subject attributes (0)

- **Subject-id ⇒ Subject-X509-id**
  - String: OpenSSL oneline notation of the DN
- **Subject-issuer ⇒ Subject-X509-Issuer**
  - String: OpenSSL oneline notation of the Issuer DN
- **(new) Subject-Condor-Canonical-Name-id**
  - String: “user@host[.domain]”
- **Certificate-Serial-Number**
  - Integer: 42
- **CA-serial-number**
  - Integer: 1
- **CA-policy-OID**
  - String: “1.2.840.113612.5.2.4” (Robot Certificate)
- **Cert-Chain (experimental)**
  - base64Binary: “*MIICbjCCAVagA……..*”
- **Subject-VO**
  - String: “gin.ggf.org”

Overview of Subject attributes (1)

- **VOMS-signing-subject**
  - String: OpenSSL oneline notation
- **VOMS-signing-issuer**
  - String: OpenSSL oneline notation
- **VOMS-dns-port**
  - String: “kuiken.nikhef.nl:15050”
- **VOMS-FQAN**
  - String: “/gin.ggf.org/APAC/VO-Admin”
- **VOMS-Primary-FQAN**
  - String: “/gin.ggf.org/APAC/VO-Admin”

Overview of Action attributes

- **Run-type: expressed as the ‘action-id’ (enum. type)**
  - Queue
    - Requesting execution to a (remote) queue.
  - Execute-Now
    - Requesting direct execution (remotely)
  - Access (file)
    - Request for (generic) file access

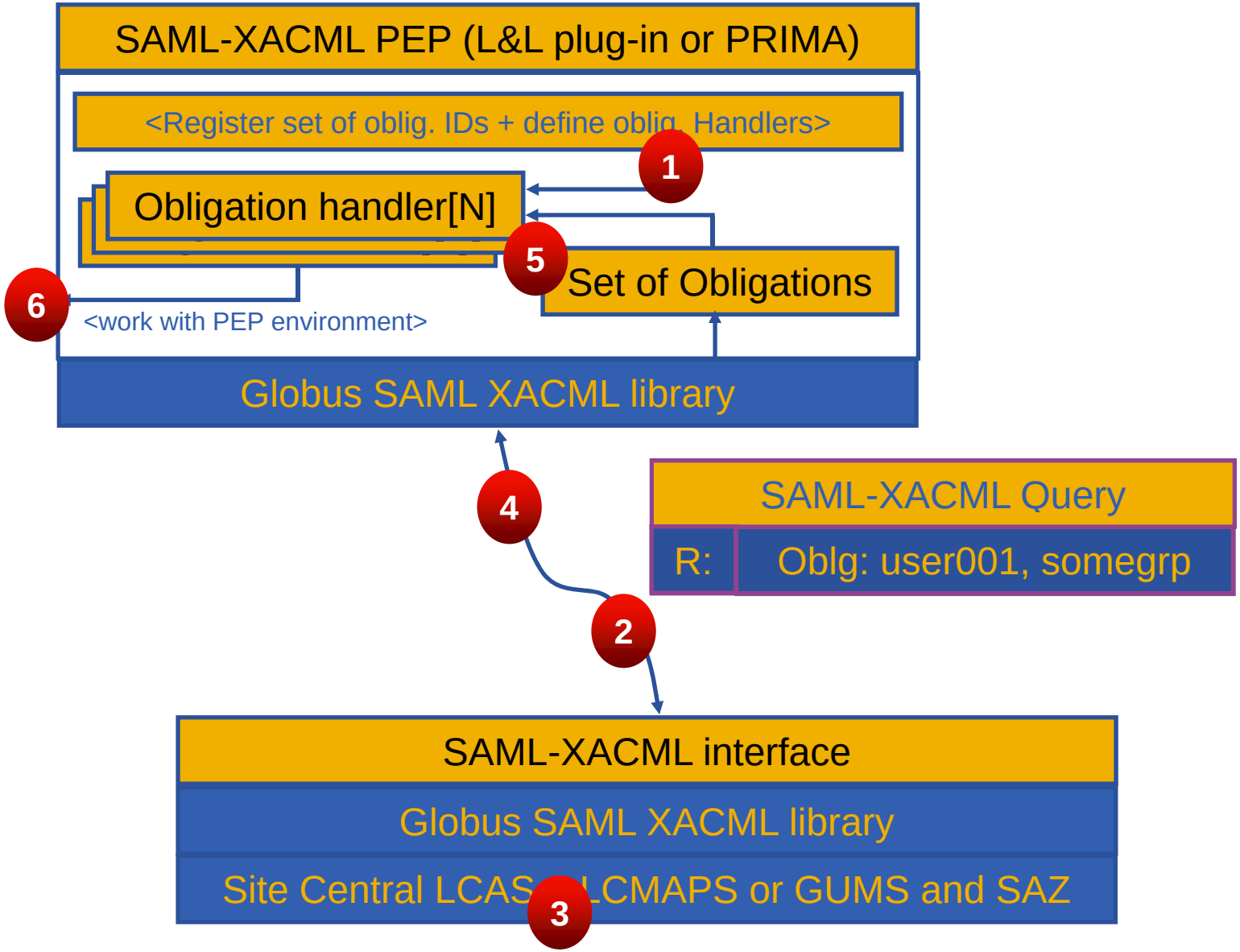
Overview of Resource attributes

- **Node-type: (enum. type)**
  - CE (Computing Element)
    - Can also be the head-node or entry point to a cluster
  - WN (Worker Node)
    - A node type that will process jobs, typically in a cluster
  - SE (Storage Element)
    - (Logical) storage facility or specific storage node
- **Host DNS Name**
  - The name of the host

More Resource bound/specific attributes are being discussed

- **Host certificate DN & Host certificate Issuer**

Before we hit the Environment…



Overview of Environment attrib's

- **Supported Obligations**
  - Announces the capabilities of the PEP to a PDP by sending the obligation IDs that it supports
  - The PDP can choose to return an appropriate set of obligations from this list
  - Allows upgradeability of the PEPs and PDPs independently by deploying new functionalities step by step

- **Invoker identity**
  - Used in *Pilot* job and in new *Condor* use cases
  - These attributes resemble the identity of the pilot job invoker
  - Contains the set of attributes known to be found in the Subject section

- **Invoker type**
  - The value of this element will describe very explicitly what kind of invoker scenario is at hand
    - Pilot job: as we know it in the WLCG / OSG environment
    - Unprivileged Condor daemon: new run mode which uses glexec as the only element that requires root privileges

Obligations

Namespace prefix construction:

Obligations: <root-ns-prefix>/obligation

Attributes: <root-ns-prefix>/attributes

Obligations (0)

- **UIDGID**
  - UID (integer): Unix User ID local to the PEP
  - GID (integer): Unix Group ID local to the PEP
  - Stakeholder: Common
  - Must be consistent with: Username
- **Username**
  - Username (string): Unix username or account name local to the PEP.
  - Stakeholder: VO Services Project
  - Must be consistent with: UIDGID
- **SecondaryGIDs**
  - Multi recurrence
    - GID (integer): Unix Group ID local to the PEP
  - Stakeholder: EGEE
  - Needs obligation(s): UIDGID

Obligations (1)

- **AFSToken**
  - AFSToken (string) in base64: AFS Token passed as a string
  - Stakeholder: EGEE
  - Needs obligation(s): UIDGID

Obligations (2)

- **RootAndHomePaths**
  - RootPath (string): this parameter defines a sub-tree of the whole file system available at the PEP. The PEP should mount this sub-tree as the “root” mount point (‘/’) of the execution environment. This is an absolute path.
  - HomePath (string): this parameter defines the path to home areas of the user accessing the PEP. This is a path relative to RootPath.
  - Stakeholder: VO Services Project
  - Needs obligation(s): UIDGID or Username
- **StorageAccessPriority**
  - Priority (integer): an integer number that defines the priority to access storage resources.
  - Stakeholder: VO Services Project
  - Needs obligation(s): UIDGID or Username

Open issues & way forward

- **Adding the host credentials (when available)**
- **Adding the current Unix UID and Unix GID(s) from the originating resource process**
- **Using the XACML Category element**
  - Sorry I don't have all the details about this
  - Pushes the Invoker identity into one element

- **Document will reach version 1.0 within two weeks**
  - Means feature freeze in the list of understood attributes, formatting and structuring
  - The implementations will base their functionality on this version

- **Risk: Uncertain if we might be incompatible with true XACML-policy engines**

?

The implementation

It works! (server side)

```
oscars-computer:~/dvl/saml2-xacml2 okoeroo$ bin/xacml-server -i
Server ready... listening on port 8080.
Pausing...
Accepted connection from remote host: localhost
- Warning: Data Oscar Koeroo and host localhost do not match!
-------------------------------------------------------------
http://authz-interop.org/xacml/2.0/subject/subject-x509-id: /C=NL/CN=Oscar Koeroo
http://authz-interop.org/xacml/2.0/subject/subject-x509-issuer: /C=NL/CN=DutchGrid CA
http://authz-interop.org/xacml/2.0/subject/certificate-serial-number: 123
http://authz-interop.org/xacml/2.0/subject/ca-serial-number: [0] 1
http://authz-interop.org/xacml/2.0/subject/ca-policy-oid: [0] /gin.ggf.org
http://authz-interop.org/xacml/2.0/subject/voms-fqan: [0] /gin.ggf.org
http://authz-interop.org/xacml/2.0/subject/voms-fqan: [1] /gin.ggf.org/pragma
-------------------------------------------------------------
```

It works! (client side)

```
oscars-computer:~/dvl/saml2-xacml2 okoeroo$ test/runtest.sh
- Warning: Data asen.nikhef.nl and host localhost do not match!
UIDGID: Got obligation http://authz-interop.org/xacml/2.0/obligation/UIDGID
 http://authz-interop.org/xacml/2.0/attribute/posix-uid
[http://www.w3.org/2001/XMLSchema#integer] = 501
 http://authz-interop.org/xacml/2.0/attribute/posix-gid
[http://www.w3.org/2001/XMLSchema#integer] = 500
Server said: urn:oasis:names:tc:SAML:2.0:status:Success:0
oscars-computer:~/dvl/saml2-xacml2 okoeroo$
```

The C implementation

- **Globus has provided the SAML2-XACML2 implementation around the gSOAP library**
  - Able to override data transport layer with basic I/O hooks
    - Used to implement an SSL/TLS layer (SOAP over HTTPS)
  - Helper functions
    - Registration of the supported obligations with obligation handlers
    - Adding the registered obligations into the request message declared as supported obligations

Performance

- **Localhost tests mostly**
  - Hardware limited to this laptop
- **The bottleneck turns out to be the CPU for the SSL negotiation phase, still reaching:**
  - Nominal: 7 Hz
  - Burst: 15 Hz
  - Interval to burst: 12 seconds

Work

- **Lot of time spend on the document, not in the code**
- **Feedback loop is slow**
  - Mostly due to timezone differences
- **Prototype finished and meets basic requirements**
- **Integration with the LCMAPS framework is almost finished**
- **Prototype has been send to Jay Packard to work on the Java side for GUMS**

?