March 29, 2004 OGSA-WG teleconference minutes

1 Early discussion

(1) Note taker assignment: Fred Maciel
(2) Roll call
- Fred Maciel (Hitachi)
- Hiro Kishimoto (Fujitsu)
- Latha Srinivasan (HP)
- Andrew Grimshaw (UvA)
- Frank Siebenlist (ANL)
- Bill Horn (IBM)
- Jem Treadwell (HP)
- Ian Foster (ANL)
- Ravi Subramaniam (Intel)

(3) Approve the minutes of last teleconference: no comments, approved
(4) Agenda bashing

2 Security design team discussion

- Frank sent an e-mail to the OGSA-WG mailing list with brief descriptions of the security-related use cases that he wants to explore with the security design team over the coming months. Lobbying with people working on these technologies and have commitments to contribute work on them.
- Frank describes each use case (in numbered items below) followed by discussion on each of them:
  (1) Many sites won't allow long-term secrets on the workstations and also mandate two factor authentication. Many would like to use WS-Authentication, but it was not submitted to a standards body. SAML is less elegant but could work.
    - Andrew: intent is to standardize authentication scheme? Frank: Yes. Andrew thinks it's a mistake. Frank: need it to standardize a protocol to get interoperability, there is no protocol now. Andrew: Liberty qualifies? Frank: no, low-level.
    - Andrew: not sure what is meant by authentication. Frank: e.g., simple password authentication. Andrew: done in each Grid operation? Frank: No (explains authentication method). Andrew: so need to use a scheme that we will determine? Frank: no, there is no scheme now, have to agree on mechanisms and protocols to interoperate.

- Andrew notices that there is a mismatch of assumptions somewhere in discussion above. There are two separate problems: (a) user authenticates him/herself (lots of different ways to do it, don't need to make that a standard), (b) on a set of Web services, how do they propagate security information (the most important one). In Legion had to use multiple schemes because organizations wouldn't change their authentication schemes. Frank: use case refers to (b), could have multiple authentication schemes for (a).

(2) Simplified configuration: user configuration is too complicated. Use user configuration server, which will communicate to user all that is need. Andrew: had this in Legion, very useful.
- Ravi: username/password assigned to user or authority? Frank: username/password is a good example, from them bootstrap environment and then download all configuration data. Standardize "provisioning protocol" for that. Ravi: there could be many ways to get to that information. Frank: this can be input to use case. Ravi: standardize solution or communication for that? (Better doing the latter) Frank: requires a standardized protocol to communicate.

(3) Firewall traversal
- Frank: need it but have not seen anybody working on it. Andrew: lots of things being done on that; P2P WG had whole working group on it and generated a solutions document. Legion and Avaki do it. Exploit multi-level naming scheme and allow re-direction under the covers. Agree it's a problem and there is a need for standards.
- Andrew: requirements of business and HPC people on throughput and cost are different (business has many small transactions, in HPC will have large volumes of data). Might need different ways to solve the problem. Hiro: to which one use case applies? Frank: both.
- Hiro: what does silent mean? Frank: they don't discuss routing at all, it's not dealt with in WS-Addressing or WSRF spec. There is WS-Routing, but does not seem to fit with WSRF.
- Ravi: any difference between what might be required for Grid other than low-latency, high-speed, etc? Frank: no. Ravi: drive to other organizations doing standards? Frank: even better, drive other people.

(4) Centralized path validation: specialized processing required for each kind of certificate; differences in trust chains; differences in policies and mechanisms. Results in operational nightmare, which many sites are going through right now. Have to standardize that.

- ♦ Andrew: single place in organization or single place overall? Frank: centralizing per administrative domain.
- ♦ Ravi: proposing standardization how it is done or what needs to be there? Frank: configuration on client or server etc.; if they receive a certificate or certificate chain they will do the crypto validation and outsource all the path validation to a central server, will communicate the whole security chain and get an answer (e.g., "valid"). Ravi: looking at protocol, not at one central server? Frank: correct. There are a number of solutions already, hopefully can leverage.

(5) Interactions within a VO context: requesters can be part of more than one VO at the same time, they have to specify the VO context for interactions between the parties. Need to decorate the protocols, but how does it fit in WSRF is unclear.

- ♦ Ravi: what types of services involved? Frank: not focusing on services but on the decoration of the messages.

(6) Communication of authentication credentials: recurring discussion, would like to see in what cases it makes sense. Sees it just as a kind of optimization.

- ♦ Ravi: how different from resource and WSRF with authentication credential being a resource? Andrew: what to add to EPR so that services can authenticate one another? Frank: if you use SSL you would need that, protocol includes the exchange of authentication information.
- ♦ Ravi: what means by credentials? Authentication establishes identity; are these credentials that define identity? Frank: used wrong words, correct is "authentication information".

- Next steps: take one or two use cases and work with people to write one level deeper, and call for first teleconference to discuss them. Hopefully something to discuss next week.
  - – Andrew: when is the security design team teleconference? Frank: date not set; first listing things that are important, look for people and form design team.
  - – Discussion on the day of the conference call. Andrew: need call to organize. Some discussion on the date, Thursday April 8 seems to be the best one. Frank will talk with interested parties, fix the date, and send time and agenda items to the list.
- Andrew: these are more technical challenges than use cases. Frank: depends on how formulates. Andrew: regulations (hospitals, etc.) introduce interesting requirements. It is important to keep business (non-HPC) use cases in mind.
  - – Andrew: language in medical area different. Ravi: language or concepts? Andrew: mostly language, can be mapped to ours. Extra policies also ("am I on a machine that has a disk drive or not?").

- Ravi (side subject): time synchronization is needed in Grids, but there is no one talking on it; need some notion of it in OGSA. Frank: good point; some discussion on time stamps on protocols to synchronize deviation with other party. Andrew: well-known problem.

3 OGSA infrastructure dependencies (continuation of last week's discussion)

- Andrew: if we try to keep OGSA spec neutral, have to go through contortions on explanations and will get an awkward document. On CORBA 1.1, name depended on implementation, there was no interoperability. Only on CORBA 2.0 and IIOP these things were corrected. OGSA could have the same problem. (Two people expressed agreement).
  - Ravi: two rounds, implementation-dependent spec first and then generic spec? Fred: already proposed in last teleconference. Ravi: important thing for us is to make progress.
- Ravi: OGSA is about selecting standards, and WSRF is one of these selected standards. There are many standards we implicitly decided to adopt (WSDL, XML, etc.), already assuming a lot of things. This choice makes architecture concrete (the discussion is not about "focusing on WSRF" or not). Andrew agrees; the question is whether we assume it or not.
  - Andrew: concern is on IP issues? Ravi: concerned on our modus operandi. There could be other changes in standards (e.g., WS-Agreement changes) we have to call out these new standards. We have to change – no discussion on that – the point is how.
  - Bill: WSRF is a meta-standard, composed of many specs. Ravi: yes, might make explicit which ones apply in which aspects.
- Hiro, summarizing: there are two options, WSRF, WS-Notification as special, or simply listed as specifications. No consensus now, will continue discussion (David Snelling will send e-mail with issues, hopefully reach consensus this or next week).
  - Bill: WSRF still a moving target, might want to wait a couple of months.

4 Other discussions

- Ravi: discussion on taxonomy? Hiro: have to start this discussion. Fred: looking forward to IBM's input, could be useful (will contact related people soon). Ravi: concerned with how to communicate OGSA, how to morph Jay's figure into something more meaningful. Hiro: also thinking how to re-organize the document.

- Hiro: mailing list for the logging service mailing list? Bill: not yet. Discussions are on the WG preparation stage.