

HPC Profile Kerberos Support

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.

Motivation



- Some organizations have standardized on Kerberos as the “single sign on” mechanism for their computing resources
 - DoD, DoE, orgs using Windows AD SSO, sites using AFS
 - Not all have deployed X.509 -> Kerberos solutions (i.e. want native Kerberos)
- Compute jobs use Kerberos tokens to access services during runtime
 - file transfer services, MPI task startup using rsh/ssh
- Need a way to authenticate to a BES using Kerberos
- Need a way to provide credentials to running jobs

User Authentication

- WS-Security Kerberos Token Profile + WS-I Kerberos Token Profile describe how to use WS-Security headers to pass Kerberos authentication information
 - can be adopted “as is” for the authentication step
 - acquiring credentials is “out of band” (i.e. use the usual mechanisms)
- Simple! (from a spec point of view) :-)

Server Authentication



- Even though it's possible, it's not so common in practice to do Kerberos mutual authentication
 - often there is some payload encrypted with session key that "proves" one is interacting with the "right" service
- Mandate the use of SSL + server authentication using X.509
 - like the current HPC Basic Profile

Delegation

- MUST provide Kerberos credentials to the running job
 - it's not sufficient just to do authentication
 - need credentials for the job to access other services (e.g. file services)
- WSS doesn't say anything about forwarding Kerberos tokens
 - we're on our own here

Three Delegation Use Cases



- Kerberos token provided to the running jobs
- Kerberos token used for JSDL file transfers
- Kerberos token used to authenticate to another BES when brokering/meta-scheduler
 - maybe not? maybe the broker uses it's own credentials
 - even if so, Kerberos token is needed in the environment of the job, wherever it ends up running

Next steps

- Write a use case document
- Define one or two profiles
 - maybe separate authentication from delegation
- Specify the mechanism for passing a TGT in the Activity definition
 - maybe need to describe TGT attributes (e.g. address-less tickets)
- Interest? Volunteers?

Full Copyright Notice



Copyright (C) Open Grid Forum (2008). 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.