

# IGTF Globus Signing Policy for HLCA

## Background

HLCA are, for lack of a better term, Higher Level CAs, CAs which are *Trusted* (in the sense of the IGTF HLCA profile [ref]) on the grid, but do not themselves issue EE certificates for use on the Grid (in particular, they are not *Accredited*, again in the sense of the HLCA profile). CA certificates for such CAs are included in the IGTF distribution, also with .info and .signing\_policy files.

This document describes a problem with the current practices for writing signing policy files for HLCA, and proposed amendments.

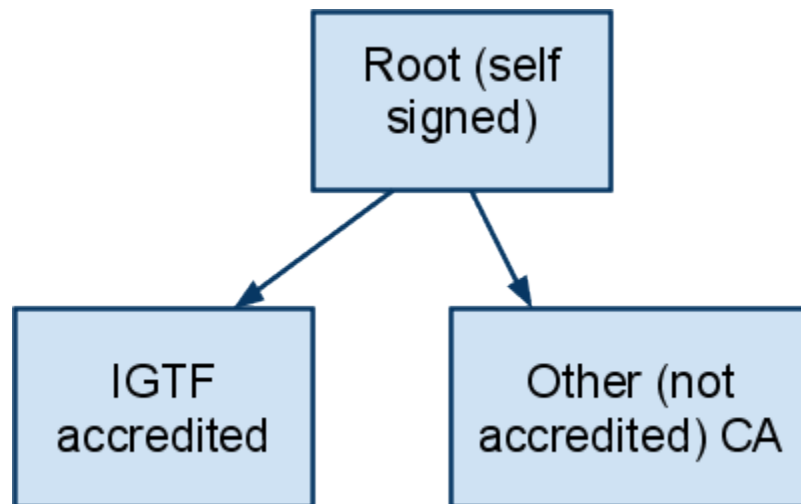
Distribution: International Grid Trust Federation

Author: Jens Jensen, for TAGPMA

## Description

Signing policy files are Globus implementations of RPDNC [ref]. Current practice for HLCA limits the subjects that the HLCAs are allowed to sign to only the Accredited (or Trusted) subject CA(s), i.e. strictly to the chain of CA certificates which are required to build a valid chain from a self-signed root to the Grid EE certificate.

The problem is the signing policy file for the HLCA conventionally names only the CAs in the IGTF distribution, which causes problems for Grids that wish to also trust certificates not in the IGTF distribution but signed by the HLCA in the IGTF distribution.



This simple picture shows a self signed root in the IGTF distribution, and one accredited CA signed by it. We assume another CA is signed by the root but is not part of the IGTF distribution (and is not accreditable - e.g. because it has a lower level of assurance). A grid wishing to trust both subject CAs must now change the signing policy file for the root, if the root names only the accredited subordinate.

This causes problems with deployments because many Grids conventionally deploy files via RPMs, and a changed file now has to be changed locally - which in turn causes problems at the next IGTF release when the updated RPM will refuse to overwrite a locally modified file, and the IGTF release will fail to install properly.

## Proposal

We propose to permit Trusted CAs (i.e. HLCAs in the IGTF distribution which do not themselves issue EE certificates) to have more permissive signing policy files in the IGTF distribution.

HLCAs should still be restricted so their namespaces do not overlap - and do not overlap with those of their subordinates.

In the example above, there are two possibilities: either the signing policy file names both CAs explicitly, or it implicitly designates a namespace for its subject CAs using wildcards (for this we're assuming that both subject CAs have a common namespace root).

## Security Considerations

For Grid resources, the IGTF will not be trusting other CAs "through the back door" as it were, since all Trusted or Accredited CA certificates have to be installed anyway, they cannot be supplied by the client.

For non-Grid resources, e.g. web servers, it is possible that a client with a certificate from an intermediate CA (e.g. the non-IGTF one in the picture above) sends the unaccredited intermediate along with the client certificate, and the server successfully builds a chain from the root. However, non-Grid resources do not check signing policy files, and the point is entirely moot. Whether we restrict the signing policy files or not is irrelevant.

Likewise, whether subject CAs on Grid resources are named explicitly or not in the signing policy file does not make a huge difference to the IGTF itself.

It would, however, seem prudent to restrict the signing policy files to be name distinct namespaces across all the IGTF, similarly to the IGTF practice for EE certificates for reasons which are described in [RPDNC].

## References

[HLCA] <https://forge.gridforum.org/sf/go/doc15144?nav=1>  
[RPDNC] <https://forge.gridforum.org/sf/go/doc4857?nav=1>