OSG-DigiCert Interactions

DRAFT

July 24th, 2012

# Introduction

This document describes interactions between OSG and DigiCert for the purpose of operating the OSG PKI.

# Points of Contact

## Open Science Grid

The OSG Grid Operations Center (GOC) should be the initial point of contact for DigiCert to contact OSG for any issues:

The GOC is expected to route matters internal to the OSG as described in Section 5.

## DigiCert

the Open Science Grid OSG’s account number is 055259 (during the pilot, 052062 was used).

Contact information at the time of this writing is:

Support Toll Free: 1-800-896-7973 (US & Canada)

Support Direct: 1-801-877-2100

Fax Toll Free: 1-866-842-0223 (US & Canada)

Email: support@digicert.com

Hours of support:

* M-Thu 24hours
* Fri 12am - 7pm/Mountain Time
* Sat 7am – 3pm/Mountain Time

# Technical Interfaces

## Test and Production PKIs

A PKI was created in the OSG Pilot phase for evaluation, this PKI is known as the “DigiCert-Grid Test CA.” This CA will continue to be available to OSG for testing and DigiCert plans on adding a feature to it that allows OSG to select the version of the API in effect, allowing for the testing of new features before moving them into production. The OIM ITB instance ([https://oim-itb.grid.iu.edu](https://oim-itb.grid.iu.edu/)) will be configured to use the Test CA with the intent being it is available for testing and training.

The production PKI that will be used by OSG for production is the “DigiCert-Grid CA.”

Production

## DigiCert PKI Interfaces

DigiCert provides a web interface, known as the Managed PKI or MPKI interface, and a network protocol, or “REST”, interface that are used by the OSG PKI.

### Managed PKI Interface

Since the OSG primarily uses the REST interface, the expectation is that OSG staff will use the MPKI interface for administrative purposes. Reasons for accessing the MPKI interface include:

* Issuance/revocation of certificates if OIM is unavailable.
* Debugging: seeing what the state at DigiCert is to verify it is coherent with OIM’s state.
* Obtaining replacement API keys for OIM.

The URL for accessing MPKI is: https://www.digicert.com/enterprise/

The following staff will have MPKI access as the designated level of access. It is expected that identified staff may designate one or more staff as needed to back them up in the event they are unavailable. The OSG Security Officer and OSG RA will be responsible for approving and managing staff access to MPKI.

* Administrator role: Full, account-wide administrative access
  + The OSG security officer and OSG RA have Administrator access for emergencies, obtaining API keys, and managing staff who have access to MPKI.
  + During the OSG PKI Transition phase, Von Welch and Jim Basney maintain Administrator access for debugging. At the end of the Transition phase, they will relinquish this access.
* Unit Administrator: Full administrative access to one or more business units
  + OSG does not currently use Units, so this role is ignored.
* Finance: View reports, certificates, and account finance information. Request certificates, view own certificates
  + OIM developers have Finance access for debugging.
  + Indiana University Point of Contact for DigiCert (currently Von Welch) has Finance access for oversight.
* Limited: Request certificates, view own certificates
  + No one currently designated.

### REST Interface

The OSG PKI front-end to request certificates in uses the REST interface real-time. Authorization to the REST interface is via API key. The latest documentation on the DigiCert REST interface is at:

https://twiki.grid.iu.edu/twiki/pub/Security/DigiCertPilotProject/StandardAPI.doc

# OSG PKI Policies

The policies for the OSG PKI are impacted by our relationship with DigiCert in that our policies are to ensure that DigiCert complies with their CP/CPS policies and IGTF accreditation. The OSG PKI policies are be found at:

https://twiki.grid.iu.edu/bin/view/Operations/OSGPKIAgreements

# Internal OSG Handling of Issues

Under the terms of OSG’s contract with DigiCert, events can arise that require a response from OSG within a fixed period of time. For example:

* Amendments to the Registration Practice Statement require a response from OSG within five days (2.7).
* A registration authority in material breach needs to be cured within 10 days of receiving notice of the breach (6.2.i)
* Requests for audits (3.9)

DigiCert is expected to contact the GOC as described in Section 2. The GOC will then route the request internal to OSG by opening a ticket and assigning as follows:

* Queries regarding specific certificate issuances or RA behavior and audit requests should be routed to the OSG Security officer (currently Mine Altunay) with cc to the OSG Operations Lead (Rob Quick) and IU Point of Contact (Von Welch).
* Contractual issues should be routed to Indiana University, who acts on the Open Science Grid’s behalf for the purposes the OSG PKI. Contractual issues should be routed to Von Welch ([vwelch@indiana.edu](mailto:vwelch@indiana.edu)) with cc to the Indiana University PI (current Bill Barnett) and Dara Eckart ([deckart@indiana.edu](mailto:deckart@indiana.edu)).
* Other issues should be routed to IU Point of Contact (Von Welch), with cc to the OSG Security officer and the OSG Operations Lead, who will determine appropriate routing and modifications to the routing plan.

The recipient of the request will then coordinate OSG’s response, including:

* Contacting parties necessary for responding to DigiCert’s request and orchestrate obtaining the needed information.
* Contacting appropriate OSG management to arrange for availability of OSG staff necessary for response.
* Keeping the OSG Executive Team informed of the request and its resolution.

If the primary recipient of the GOC’s routing is unavailable, those cc’ed are expected to handle the request. In the event no designated recipients are available the GOC shall consult with the OSG Executive Team.