OSG-DigiCert Interactions

DRAFT

May 24th, 2012

# Introduction

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

# Points of Contact

## Administrative

Indiana University acts on the Open Science Grid’s behalf for the purposes the OSG PKI. Von Welch <vwelch@indiana.edu> is the primary point of contact for DigiCert in contacting IU.

The primary point of contact at DigiCert for Indiana University is Greg Larsen <greg.larsen@digicert.com>. The general source of information regarding DigiCert PKI utilized by OSG is http://digicert-grid.com/

## DigiCert Support

DigiCert support information is provided at http://digicert-grid.com/

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

## OSG Operations Center

For urgent matters, the Open Science Grid operates a Grid Operations Center (GOC), which will also operate the OSG PKI. The GOC can be reached at:

* Phone +1 317-278-9699
* Email goc@opensciencegrid.org

# 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.”

## 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. Access to MPKI is authorized by user.

https://www.digicert.com/enterprise/

### 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.

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)

In these situations, it is expected the OSG Administrative point of contact identified in Section 2.1 of this document will be contacted. The Administrative Point of Contact 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.

# Miscellaneous

## Grid-Only CA versus Public Trusted CA

DigiCert offers two different Grid CAs, a “Grid-Only CA” that provides IGTF-accredited certificates and a “Publicly Trust CA” which meets other standards such that it is in web browser trusted stores.

OSG uses the Grid-Only CA since it operates under policies that are comparable to the ones its users are used to under the DOE Grids PKI.