OSG PKI Acceptance Criteria

DRAFT May 14th, 2012 DRAFT

# Introduction

The following are requirements for the OSG PKI software to be deemed acceptable to enter into service (in project management terms, exit the Deployment phase and enter into the Transition phase).

Where requirements have a specific source, they are suffixed by square brackets identifying the source (and optionally a section number in the source). Abbreviations for sources are:

* RPS: OSG-DigiCert RPS
* SW: Criteria related to sustainability of the software from the OSG Software Team
* DC: Criteria related to meeting our contractual obligations to DigiCert and staying within our budgeted certificate issuance level.
* VO: Criteria from OSG’s stakeholders and user community.
* SEC: Criteria that stem from security best practices from the OSG Security Team and the OSG PKI Project Lead.

## Definitions

* Notification: Some mechanism of active notification (e.g., GOC ticket)
* Annual: during a contract year defined by OSG’s contract with DigiCert.
* Contract year: the year defined by OSG’s contract with DigiCert.
* OSG PKI staff: OSG staff authorized to make policy decisions. Exact list TBD.
* Logged: Recorded in a manner that preserves time, date and identifying information of entities involved. Acceptable forms of log creation include creation of a persistent ticket or entry in a preserved system log (syslog) file.
* Trusted Agent (TA): Grid Admin or Registration Authority Agent authorized to approve user or host certificates respectively.

# Software Sustainability Criteria

Software has a nasty habit of living longer than expected and being maintained by people other than the original author. Given the heterogeneous nature of the OSG Consortium, we have to assume that future software maintainers may have either less software development experience or very different experience. As such, it is of paramount importance to make this software as easy to maintain as possible.

At a minimum, this software must:

1. Have a well-defined open-source software license that will allow people from across the OSG collaboration to contribute. We recommend the Apache v2.0 license since it is already well-accepted in our community (Condor, Globus, much of EMI).
2. Have a clear software versioning scheme. If we develop any protocols or APIs, they should also be versioned.
3. Have a basic test suite. For the software that we distribute via the OSG Software stack, we must be able to run the test suite independently of the developers.
4. Have end-user documentation.
5. Have internal developer documentation to guide new software maintainers.
6. Use a source code repository with a versioning scheme such that we can recover previous versions easily (i.e. tags or branches or …) If appropriate, we may use the OSG Software Team’s source code repository.
7. Have an external code review before the final release.

In addition, we should develop this software with the idea that the next software maintainer is a homicidal developer that we do not want to upset. Ideals in developing this software:

1. As much as possible, use reliable, commonly-used software dependencies. If we depend on software, we hope that we don’t have to maintain on that external software as well. So we should choose software that appears to be well-supported.
   1. Corollary: try to avoid the need to patch software dependencies. If we need to keep up a patch, that’s like adding another piece of software to our list of maintained software.
2. We should use widely known technologies. There are a lot of great technologies out there, but we are better off using widely used but “uncool” technologies instead of way-awesome bleeding-edge technologies. We want future maintainers to be able to come up to speed quickly, and a larger community will enable that.
3. More than one developer should understand the code.
4. We should have a security assessment. I realize this is expensive, but there are people at UW-Madison that may be able to assist with this.

# Certificate Issuance

## Approval

1. All certificates issuances shall be approved by a Trusted Agent [RPS 4.1.1].
2. All applicants are required to accept the OSG PKI AUP [SEC, ?].

## Auditing

1. All requests for certificates shall be logged.
2. All approvals or rejections of certificate requests by Trusted Agents shall be logged.
3. All connections to DigiCert shall be logged in such a manner that they can be traced back to originating user-initiated connection.
4. Every request to DigiCert shall be auditable back to an incoming request
   1. In other words, given an API connection to DigiCert, we can trace back to the incoming front-end user request that caused it.
5. For each issued Certificate OSG shall log:
   1. The issued certificate in its entirety.
   2. All contact information provided by the requestor (Source: RPS)
   3. The IP address of the requestor.
   4. The VO associated with the requestor.
   5. In the case of renewals, the replaced certificate
   6. The identity of the approving TA (Source: RPS)
   7. The digitally signed evidence used by the TA to vet the request (Source: RPS)
   8. The IP address of the TA approving the request.

## General Format

1. All certificates shall conform to the example DigiCert certificates [3] [RPS Section 7.1].

## Certificate Distinguished Name (DN)

1. All certificates shall have a relative domain name of “DC=com, DC = DigiCert-Grid”.
2. All user certificates shall have a DN component of “OU = People”
3. All host certificate shall have a DN component of “OU = Services”
4. All DNs shall uniquely identify the subject using a unique numerical string after the legal name[RPS 3.1.5].
5. All user certificate shall bear the user’s legal name in the CN field.

## Certificate Lifetime

1. All certificates shall have a lifetime of 13 months [RPS 3.3.1].

# Audit

## Integrity of Auditing [RPS 5.4.1]

1. Logs shall be backed up and protected against loss.
2. Logs shall be protected from modification.
3. Any changes to auditing shall be logged.
4. Any attempt to delete or modify logs shall be logged.
5. The clock on the audit system will be synchronized on a regular basis.[RPS 5.5.5]

## Other errors and violations [RPS 5.4.1]

1. Any unexpected system errors will be logged.
2. Any violation of policy will be logged.

# Failed Authentication

1. Failed authentication attempts will be logged.

# Trusted Roles

Trusted roles are OSG PKI Staff and Trusted Agents.

1. Any request to assume a trusted role must be logged.
   1. For Trusted Agents, the log must include the domain or VO for which the agent would act.
2. Approval of the granting of a Trusted Role must be by OSG PKI Staff.
3. Any granting of a Trusted Role must be logged.
   1. For a Trusted agent, the log must include the domain or VO for which the agent would act.
4. Any removal of a Trusted Role must be logged.
5. Any attempt of an entity to act in a Trusted Role not granted to them shall be logged.

# Certificate Accounting and Issuance Limits

## Certificate Budgeting Issuance Checks

The following checks are to ensure OSG does not exceed its contractual limit of certificates with DigiCert.

1. OSG shall not issue a certificate that exceeds a defined limit without approval of OSG PKI staff.
   1. The defined limit is expected to be the defined by OSG contract with DigiCert.
2. OSG shall track the number of host and user certificates issued per contract year. A notification will be sent to OSG PKI staff as configurable fractions of OSG’s certificate limit as defined by OSG contract with DigiCert are reached.
   1. E.g., assuming the fraction is 1/10 and the limit of user certificate is 2500, each time N % 250 == 0 users certificates is issued, an notification will be sent.
   2. OSG shall track user and host certificate separately as different limits are defined by OSG’s contract with DigiCert.
3. Certificate requests for an entity that has a valid certificate which is not expiring “soon” shall be flagged as such and require approval from OSG PKI staff.
   1. “soon” should be configurable, I expect this to be O(month)
   2. This is to prevent accidental multiple request for the same entity.
4. Grid Admins shall be limited to requesting 50 certificates/day
   1. This is policy under the current DOE Grids PKI and helps mitigate accidents.
5. Grid Admins shall have an annual limit on certificates they can be request, set on an Admin-by-Admin basis when they are granted Grid Admin status.
   1. Increases to the limit can be done by OSG PKI staff.

## Host Certificate Issuance Checks

1. Requestors of host certificate requests shall be authenticated with a valid OSG/DigiCert certificate.
2. Requestors of host certificates shall be Grid Admins (Source: RPS)
3. Each Grid Admin shall be restricted to requesting certificate a set of domains (Source: RPS)
   1. That set of domains shall be as restricted as possible, ideally a third level domain (e.g., \*.foo.school.edu)
   2. This implies that domain-free host certificates (e.g., “localhost”) will not be issued.
   3. Hosts in certificate requests do not need to be registered in DNS or publicly reachable via the Internet.

# Private Key Generation [RPS 6.1.2]

1. All creations and deletions of private keys shall be logged in such a manner that they can be tied together.
2. All generated private keys will be encrypted with a pass phrase that has been strength tested.

# Revocation

1. Any user may request revocation of their own user certificate.
2. A Grid Admin may request revocation of any host certificate in a domain for which they are authoritative.
3. A RA Agent may request revocation for any user certificate they vetted.
4. OSG PKI staff and the OSG Security Team may revoke any certificate.
   1. A reason shall be logged for every revocation
   2. One possible reason is “Suspected or known private key compromise”.
5. Any certificate revoked for reason of private key compromise will cause OSG PKI staff and OSG Security staff to be notified.

# References

1. DigiCert Certification Practices Statement. Version 4.0.3. May 3, 2011.
2. DigiCert-Open Science Grid Registration Practices Statement. Version 1.00.
3. DigiCert Example Certificates. http://www.digicert-grid.com/

Some Appendix