

TeraGrid Certificate Management and Authorization Policy

Status: POLICY

This document outlines TeraGrid policy that was developed in July 2004 and has been in practice since that time. It contains minor revisions to reflect updated TeraGrid management structure.

Revisions in this document (February 7, 2006) include format changes, new subsections (status, abstract, security considerations, acknowledgements), and modification of references to “TeraGrid Executive Committee” to reflect the current management structure. Specifically, references to the “TeraGrid Executive Committee” were changed to “TeraGrid Security Officer” in all cases but one (§5), where the reference was changed to “TeraGrid Director.” Revisions made (March 1, 2006) include a URL to the current repository for TeraGrid CAs.

Abstract

TeraGrid security rests substantially on the integrity of credentials that are associated with end users. These credentials are issued and managed by certificate authorities (CAs), which involve a set of technical services operated by an institution. This document outlines TeraGrid policy with respect to certificate authorities and responsibilities of various parties including CA managers, TeraGrid partners, and end users.

Table of Contents

1. Assumptions.....	2
2. Certificate Authority Actions.....	2
2.1 Approved Certificate Authorities for TeraGrid.....	2
2.2 Certificate Authority Addition.....	2
2.3 Certificate Authority Removal	3
2.4 Certificate Authority Reinstatement.....	3
3. Responsibilities.....	4
3.1 TeraGrid-Approved Certificate Authority Responsibilities	4
3.2 KX509 Service-Provider Responsibilities.....	4
3.3 TeraGrid Resource-Provider (Site) Responsibilities	5
3.4 TeraGrid Principal Investigator Responsibilities.....	6
3.5 TeraGrid User Responsibilities	6
4. Appendix A: Certificate Authority Compliance Checklist	7
5. TeraGrid Certificate Management and Authorization Policy Publication and Maintenance.....	8
6. Security Considerations	8
7. Acknowledgements	8
8. Editor Information	8
9. References.....	8

1. Assumptions

All users of TeraGrid resources must be associated with at least one active TeraGrid award or grant, as described in [3].

Access to TeraGrid resources by users will be limited to only those TeraGrid resources approved for their project as specified in the TeraGrid award or grant for their project.

All digital certificates used for authentication by TeraGrid sites must conform to the X.509 standard and include fields required for proper Grid Security Infrastructure (GSI)-based authentication (see <http://www.globus.org/security/>).

Principal Investigators (PIs) whose projects have been approved by the TeraGrid Resource Allocations Committee are assumed to be trusted and authoritative regarding designation of users who may charge usage against the PI's project allocations.

Every TeraGrid site has a designated Site Security Officer (or staff equivalent) who is responsible for dealing with security incidents associated in any way with TeraGrid certificates (e.g. compromise of pass-phrases, violations of acceptable use, other conditions endangering the security of and trust in certificates and GSI-authenticated access)

2. Certificate Authority Actions

2.1 Approved Certificate Authorities for TeraGrid

The TeraGrid will not operate a Certificate Authority (CA) of its own. Instead, a limited number of existing Certificate Authorities will be designated as approved sources of TeraGrid user, host, and service certificates. Currently approved TeraGrid-accepted CAs can be found here:

<<https://repo.teragrid.org/head/security/teragrid-certs.tar.gz>>

Certificates issued by the former Globus CA will not be accepted for TeraGrid use.

All changes to the list of approved CAs for TeraGrid must be vetted and confirmed by the TeraGrid Security Working Group.

2.2 Certificate Authority Addition

TeraGrid users and participating sites may request that an additional CA be accepted for TeraGrid purposes. Approval of an additional CA is contingent upon demonstrated need (in support of an approved TeraGrid project), and compliance of the CA with all requirements set forth in this TeraGrid Certificate Management and Authorization Policy.

The TeraGrid Security Working Group will thoroughly review all requests for acceptance of an additional CA and advise the TeraGrid Security Officer in the form of a statement of recommended action (either accept or decline) regarding the additional CA.

TeraGrid sites retain the prerogative to decline acceptance of a CA if doing so violates their site-specific regulations or policies.

A checklist to evaluate CA compliance with TeraGrid CA acceptance and implementation requirements is provided in Appendix A.

2.3 Certificate Authority Removal

Certificate Authorities may be removed from the list of approved CAs for TeraGrid for reasons including:

- Failure of the CA to sustain TeraGrid CA requirements (e.g., changes in certificate issuing policies, accessibility and currency of revocation lists, etc.)
- Expiration of the period during which the CA is needed to support an approved TeraGrid project
- Changes in TeraGrid policy which cause a CA to no longer be compliant with current TeraGrid requirements
- Exercised prerogative of TeraGrid sites to decline acceptance of a CA if doing so violates site-specific regulations or policies

2.4 Certificate Authority Reinstatement

“No grandfather clauses.” CAs which previously were approved for TeraGrid use may be reinstated as approved CAs for TeraGrid if their operating policies and procedures satisfy the current TeraGrid policies and requirements for accepted CAs, and the need to include the CA is warranted by the needs of an approved TeraGrid project.

All requests for CA reinstatement must be confirmed by the TeraGrid Security Working Group. The TeraGrid Security Working Group will thoroughly review all requests for reinstatement of the CA and advise the TeraGrid Security Officer in the form of a statement of recommended action (either accept or decline) regarding CA reinstatement.

3. Responsibilities

3.1 TeraGrid-Approved Certificate Authority Responsibilities

Public keys, X.509 signing_policy files and Certificate Revocation Lists (CRLs) for every TeraGrid-approved CA must be published and made available in a secure manner on a regular basis.

TeraGrid-approved CAs must publish and make available Acceptable Use Policies (AUPs) regarding use of certificates issued by the CA for use in authentication to TeraGrid resources.

TeraGrid-approved CAs issuing new certificates for TeraGrid users must implement a procedure (a.k.a. Registration Authority, or RA) for validating the identities of users requesting certificates. Required components include some means for establishing sufficient confidence in the identity of the requestor (e.g., valid Government-issued identification), and correlation of the user certificate request with an approved and valid TeraGrid project.

All TeraGrid-approved Certificate Authorities must maintain, securely publish and make available current Certificate Revocation Lists (CRLs) that are updated at least daily. CRLs must be valid for at least 24 hours unless updated and replaced sooner. All CRLs must be digitally signed by the CA.

Current CRLs for all TeraGrid-approved CAs must be available to all TeraGrid resources at all times. The Uniform Resource Locator (URL) format location for each TeraGrid-approved CA's current CRL file must be available in a file named with the .crl_url suffix along with the corresponding .0 public key files and .signing_policy files for each CA.

All TeraGrid-approved CAs must notify TeraGrid sites of scheduled down-times (e.g. affecting current CRL availability) at least 48 hours in advance, and as soon as possible in the event of unscheduled down-times.

CRLs distributed/published by CAs should not contain expired certificates (e.g., those that although prematurely revoked, are no longer valid anyway since the current date is past their original expiry date). Nevertheless, CAs should maintain a record of revoked certificates along with a description of the reason for the revocation of each certificate.

TeraGrid-approved Certificate Authorities must revoke a TeraGrid certificate when:

- the certificate's security has been compromised (at the CA, or at any TeraGrid or external location)
- the holder of the certificate is no longer authorized to use the certificate (as directed by the TeraGrid Security Officer)
- the certificate is replaced by a new certificate (e.g. for renewal)
- requested to do so in a secure and verifiable manner by the certificate holder

3.2 KX509 Service-Provider Responsibilities

Sites that provide Kerberos-authenticated, short-term user certificates via the KCA service and associated client software (kx509, kxlist) must ensure that the Kerberos infrastructure and KCA services are secured at least as well (if not more strongly) as a TeraGrid-approved Certificate Authority.

KCA services approved for use on the TeraGrid must have a parent CA that is one of the TeraGrid-approved CAs. This means that a TeraGrid-approved CA must issue and sign the KCA service's signing certificate.

If a KCA service's certificate must be revoked, then all KCA/KX.509 services provided by that KCA must be terminated immediately and remain off-line until the service has been securely re-established and a new signing certificate for the KCA service has been issued by a TeraGrid-approved CA.

3.3 TeraGrid Resource-Provider (Site) Responsibilities

The public keys and signing policies of all TeraGrid-approved CAs must be retrieved and installed in the appropriate locations on all TeraGrid computational resources to permit validation of user-, host-, and service certificates.

TeraGrid resource-providers are responsible for validating the certificates and authorization of all users, systems and services seeking GSI-authenticated access to their TeraGrid resources prior to granting access to their TeraGrid resources.

GSI-authenticated access must be denied for expired and revoked certificates. TeraGrid resource-providers are responsible for consulting the Certificate Revocation Lists (CRLs) of applicable CAs to ensure that certificates presented to them for GSI-authenticated access have not been revoked prior to their expiry date.

Each TeraGrid resource-provider site must provide complete, illustrated documentation, based on the TeraGrid Users' Guide [4] for users whose local TeraGrid home accounts are at that site, regarding:

- Application process for acquiring and renewing TeraGrid user certificates
- Installation procedures for placing certificate-related files in appropriate, secured locations within their TeraGrid home account, including installation of previously-acquired, TeraGrid-approved certificates.
- Acceptable Use policies and procedures for TeraGrid user certificates
- Procedures for user-initiated certificate retirement/revocation
- Emergency procedures and contact information of each TeraGrid site's Site Security Officer (SSO) for security-related problems associated with TeraGrid users' accounts and certificates.

Each TeraGrid resource-provider site must publish and make available Acceptable Use Policies (AUPs) regarding use of TeraGrid-approved certificates. Each site must implement means by which users can retrieve and acknowledge acceptance of AUPs prior to being granted access to TeraGrid resources.

Each TeraGrid resource-provider site must implement means by which TeraGrid users with affiliations to multiple TeraGrid projects can designate which project their GSI-authenticated sessions and job submissions are to be charged to.

TeraGrid resource-providers are entitled to decline GSI-authenticated connectivity to and from non-TeraGrid systems that fail to meet TeraGrid- and local security and acceptable-use requirements. TeraGrid resource-provider sites must publish and make available instructions and contact information for PIs to appeal declined connectivity.

TeraGrid users' home sites must publish and make available to every other TeraGrid site the Distinguished Name (DN) for every local TeraGrid user's certificate in a secure manner for inclusion in *grid-mapfiles* of TeraGrid resources approved for use for the user's TeraGrid project.

TeraGrid resource sites are responsible for validating the status of all TeraGrid certificates before permitting access to resources (i.e. it's not the CA's fault if you let someone in whose certificate was revoked and you didn't check it first).

Failure to validate the current status of a TeraGrid certificate due to inaccessibility of the associated CA's current CRL must result in denial of authentication using that certificate until current CRL availability is restored.

TeraGrid resource sites are responsible for validating the signatures of CRLs from CAs to establish confidence that the CRL being consulted is genuine.

3.4 TeraGrid Principal Investigator Responsibilities

The Principal Investigator (PI) for each TeraGrid award / grant must identify and provide complete contact information for every user authorized by the PI to charge use of TeraGrid resources against the project's TeraGrid award / grant allocation. All GSI-authenticated sessions and jobs submitted on TeraGrid resources will be charged against the user's PI's project.

The PI for each TeraGrid award / grant must identify and provide complete system identification and operator contact information for all non-TeraGrid systems and services that are expected to interface with TeraGrid resources during their project.

The PI for each TeraGrid award / grant must request and acquire all necessary host and service certificates from a TeraGrid-approved CA for all systems and services expected to interface with TeraGrid resources during their project.

3.5 TeraGrid User Responsibilities

For GSI-authenticated access to TeraGrid resources, every user must use an approved digital certificate issued to them by a TeraGrid-approved CA.

TeraGrid users who require access to TeraGrid resources via GSI-authentication and who do not already have an X.509 standard GSI-compatible certificate from a TeraGrid-approved CA will be directed to an appropriate TeraGrid-approved CA to acquire one. The appropriate CA will typically be that associated with the site of the user's Home TeraGrid Account, e.g., NCSA—NCSA Alliance CA, SDSC—SDSC NPACI CA, PSC—PSC CA, ANL—(TBD), Caltech—(TBD).

Users must read, accept and acknowledge notification of the TeraGrid User Responsibility Form prior to issuance of new certificates from TeraGrid-approved CAs and use of certificates from TeraGrid-approved CAs on TeraGrid resources.

Users may be required to read, accept, and acknowledge notification of additional Acceptable Use Policies for specific TeraGrid resources, as required by the individual TeraGrid resource owner/operators, prior to use of TeraGrid-approved certificates with those resources.

TeraGrid users are responsible for the security of pass-phrases used to safeguard their TeraGrid user certificates, proxy certificates, and where applicable, Kerberos credentials (e.g., for

KCA/KX.509-generated short-term certificates). TeraGrid users must notify the TeraGrid hotline or a TeraGrid Site Security Officer immediately as soon as they have reason to believe that their TeraGrid account, TeraGrid-approved certificates, or other authentication credential used on TeraGrid resources (e.g., SSH key) has been compromised.

4. Appendix A: Certificate Authority Compliance Checklist

1. Justification
 - 1.1. Title and PIs of approved TeraGrid project requiring this CA
 - 1.2. Explanation of reasons why existing, approved TeraGrid CAs are not adequate for the purposes of the TeraGrid project identified above [1.1]
2. Documented Policies
 - 2.1. CA Deployment Security and Administration
 - 2.2. Certificate Acceptable Use Policy
 - 2.3. Certificate Registration Authority (Issuance) Policy and Procedures
3. Administrative Contacts
 - 3.1. CA Policy Administrator
 - 3.1.1. Name
 - 3.1.2. Address
 - 3.1.3. Telephone
 - 3.1.4. E-mail address
 - 3.1.5. Valid PGP public key
 - 3.2. CA Deployment Systems Administrator
 - 3.2.1. Name
 - 3.2.2. Address
 - 3.2.3. Telephone
 - 3.2.4. E-mail address
 - 3.2.5. Valid PGP public key
 - 3.3. Site Security Officer / Emergency Contact
 - 3.3.1. Name
 - 3.3.2. Address
 - 3.3.3. Telephone
 - 3.3.4. E-mail address
 - 3.3.5. Valid PGP public key
4. CA acceptance installation files for /etc/grid-security/certificates
 - 4.1. CA public key, digitally signed by the CA root.
 - 4.2. CA policy file
 - 4.3. CA .crl_url file (location of CA certificate revocation list)
5. CA Certificate Revocation List (CRL) retrieval and validation Test
 - 5.1. Dated/timed transcript demonstrating successful retrieval and signature validation of the CA's current CRL.
6. Certificate Authentication Test
 - 6.1. Dated/timed transcript demonstrating successful GSI authentication using a valid, representative user certificate issued by the CA.
7. Certificate Revocation Test
 - 7.1. Dated/timed transcript demonstrating failed GSI authentication using a revoked, representative user certificate issued by the CA.
8. Certificate Expiry Test
 - 8.1. Dated/timed transcript demonstrating failed GSI authentication using an expired, representative user certificate issued by the CA.

5. TeraGrid Certificate Management and Authorization Policy Publication and Maintenance

The TeraGrid Certificate Management and Authorization Policy is established and enforced by authority of the TeraGrid Director. The most recently dated edition of this Policy will be published and made available at: <http://www.teragrid.org/>

Changes to this policy must be approved in advance by the TeraGrid Director.

6. Security Considerations

As this document outlines requirements for certificate authorities, the security implications are significant. Breach in security of a certificate authority is among the most serious types of security incidents in that such an incident would enable an individual to gain access to TeraGrid resources using the credentials of a legitimate user.

7. Acknowledgements

This work was supported by the National Science Foundation grant numbers ACI-0122296, "Distributed Terascale Facility: Build and Extend the DTF," and ACI-0307136, "TCS and ETF Operations."

8. Editor Information

Derek Simmel <dsimmel@psc.edu>
Pittsburgh Supercomputing Center
300 South Craig Street
Pittsburgh, PA 15213
(412) 268-1035
(412) 268-5832 (Fax)

9. References

- [1] **The TeraGrid: A Primer** (September 2002).
<http://wg.teragrid.org/Documents/TeraGrid-Primer-Sept-02.pdf>
- [2] TeraGrid Proposal (vendor NDA information removed). **The TeraGrid: Cyberinfrastructure for 21st Century Science and Engineering**.
<http://wg.teragrid.org/Documents/PublicDT1.pdf>
- [3] Phil Andrews (NPAC/SDSC), Dick Crutcher (Alliance/NCSA), John Towns (Alliance/NCSA), Nancy Wilkins-Diehr (NPAC/SDSC), Ralph Roskies (PSC). **PACI and TeraGrid Resource Allocations White Paper v1.0**.
http://wg.teragrid.org/User_Services/PACI_Allocations_White_Paper-v1.0.pdf
- [4] **Strawman TeraGrid User's Guide**, version 1.4 (June 18, 2002).
<http://wg.teragrid.org/Applications/tgug4.html>

- [5] **Certificate Policy and Authentication Architecture** (notes of June 11, 2002).
<http://wg.teragrid.org/Grid/draft-docs/CA-authentication-arch.htm>
- [6] (TeraGrid Authentication notes of July 30, 2002)
<http://wg.teragrid.org/Grid/draft-docs/TG-Authentication.htm>
- [7] Foster, I., Kesselman, C., Tsudik, G., & Tuecke, S. (1998). **A Security Architecture for Computational Grids**. In *Proc. 5th ACM Conference on Computer and Communications Security Conference*, pp. 83-92.
<ftp://ftp.globus.org/pub/globus/papers/security.pdf>
- [8] Housley, R., & Polk, T. (2001). **Planning for PKI**. New York, NY: John Wiley & Sons, Inc. ISBN 0-471-39702-4.
- [9] Myers M., Ankney, R., Malpani, A., Galperin, S., Adams, C. (June, 1999). RFC 2560: **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP**. Internet Engineering Task Force.
<http://www.ietf.org/rfc/rfc2560.txt>
- [10] Thompson, M. R., Olson, D., Cowles, R., Mullen, S., Helm, M. (October 2002). GWD-I: **CA-Based Trust Model for Grid Authentication and Identity Delegation**. Global Grid Forum Grid Certificate Policy Working Group.
http://www.ggf.org/meetings/ggf6/ggf6_wg_papers/IBM/TrustModel-v6c.pdf
- [11] Viega, J., Messier, M., & Chandra, P. (2002). **Network Security with OpenSSL**. Sebastopol, CA: O'Reilly & Associates. ISBN 0-596-00270-X.