TACC Classic CA
Certificate Policy
and
Certificate Practices Statement

(In RFC 3647 format)

January 31, 2009

OID: 1.3.6.1.4.1.17940.5.2.1.1
Version 1.2

1 INTRODUCTION

The Texas Advanced Computing Center (TACC) operates a Certification Authority called the TACC Classic Certificate Authority (CA) in support of grid computing communities who run scientific applications requiring Public Key Infrastructure (PKI) services. TACC operates its PKI infrastructure for two purposes:

To generate X.509 certificates for academic science and research users and resources relevant to TACC's campus, state, national and international research projects.
To allow TACC generated identities to be accepted by other grid and e-science research and science organizations.

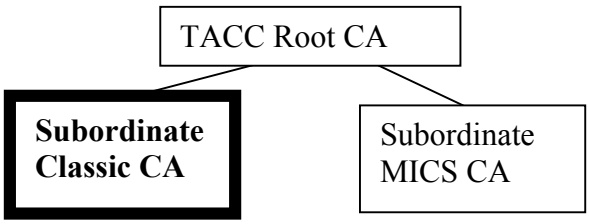
The TACC Classic CA supports long-term X.509 credential authentication for use in designated scientific grids. The TACC Classic CA runs as a subordinate CA running under the TACC Root CA and follows the IGTF Classic Authentication Profile.[1]

Structured according to RFC 3647, this document describes policy and practices of TACC Classic CA PKI services. The Certificate Policy (CP) describes the requirements for operation of the PKI and for granting PKI credentials as well as lifetime management of those credentials. The Certificate Practices Statement (CPS) describes the actual steps that TACC takes to implement this CP. These two statements taken together are designed so that a Relying Party can look at them and obtain an understanding of the trustworthiness of credentials issued by the TACC Classic CA.

1.1 Overview

The TACC Classic CA infrastructure supports grid and e-science activities provided by the **Texas Advanced Computing Center (TACC)**. The purpose of the TACC Classic CA is:

- To provide a simple, consistent and secure method for generating long-term X.509v3 certificates to hosts, services and individuals relevant to TACC's campus, state, national and international research projects.
- To support naming and policies that enable Registration Authority (RA) functions to be distributed to Local Registration Agents (LRAs) at remote organizations.



[1] Groep, David, ed. Authentication Profile for Traditional X.509 Public Key Certification Authorities with Secured Infrastructure, Version 4.2, October 2008, http://www.eugridpma.org/guidelines/IGTF-AP-classic-4-2b.pdf

1.2 Document Name and Identification

This document is the CP and CPS of the TACC Classic CA:

Document title:	**TACC Classic CA Certificate Policy and Certification Practice Statement**
Document version:	**1.2**
Document date:	**January 31, 2009**
OID:	1.3.6.1.4.1.17940.5.2.1.1 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) ut-austin(17940) tacc(5) classic-ca(2) cps(1) version 1 }

Whenever there is a major change in this CP/CPS, the OID version number shall change. Major changes shall be announced to the TAGPMA and approved before signing any certificates under the new CP/CPS. All versions of this CP/CPS under which valid certificates were issued shall be available at http://www.tacc.utexas.edu/CA.

1.3 PKI Participants

TACC will manage and operate the TACC PKI. This includes the on-line HSM-protected Root CA, the on-line HSM-protected TACC Classic CA, the on-line HSM-protected TACC MICS Grid CA, a single Registration Authority (RA) and all the Local Registration Agents (LRAs) located at TACC or at remote collaborator sites.

1.3.1 Certification Authorities

The TACC Classic CA issues certificates for researchers associated with TACC projects or wishing to access scientific computing resources primarily located in Texas and/or associated with TACC projects. The TACC Classic CA will generate and manage RFC5280 PKI X.509 v3 long-lived user, host and service certificates. The TACC Classic CA is on-line. It operates on a physically and procedurally protected server accessible only via transactions employing secure sockets layer or transport layer security protocols (SSL3.0 or better/TLS1.0 or better).

The TACC Classic CA operates as a subordinate CA off of the TACC Root CA. All private keys used by the TACC Classic CA are protected in a labeled, isolated partition in the FIPS 140-2 level 3 compliant Hardware Security Module (HSM) device.

1.3.2 Registration Authorities

There is a single Registration Authority (RA) for the TACC PKI that is managed by the TACC Security Officer. In addition to Local Registration Agents (LRAs) who are members of TACC staff, each participating grid or collaborating site may nominate specific LRAs according to site location or project position. In all cases selection of LRAs by the TACC Security Officer occurs only after confirmation that the designated individual or identity management organization has the authority and the ability to identify people, hosts or services within their domain of responsibility. The TACC Classic CA will provide a secure web interface to facilitate, organize and validate RA transactions. This interface communicates with the TACC Classic CA to:

- Approve or Reject certificate requests
- Initiate certificate revocations
- Search for certificates

Examples of Local Registration Agents (LRAs) include grid organization administrators and principal investigators or their delegated administrative representative.

1.3.3 Subscribers

The TACC Classic CA issues certificates for researchers based in Texas or researchers wishing to access scientific computing resources primarily located in Texas or resources associated with TACC projects. Each participating grid or Virtual Organization (VO) defines its specific subscribers. The TACC Classic CA issues long-term RFC5280 PKI X.509 v3 certificates for users, hosts and services only upon request via a public web interface, communicating with the TACC Classic CA only via a secure (at least SSL3.0 or TLS1.0) network link.

1.3.4 Relying Parties

Grid and scientific or research organizations or VOs control access to their computation or storage resources by validating identity certificates. Grid organizations or VOs may also establish relationships between multiple CAs (e.g. federation, bridge, subordinate). Any CA entering into an agreement with the TACC Classic CA, for the purposes of transitive trust, agrees that:

- Person or User certificates can be used only to authenticate a person as eligible for access to some defined set of scientific computation or storage resources. This authentication may require the signing of Globus proxy certificates. It is expected that participating sites will be collaborating with TACC. While Person or User certificates may be used for other activities such as email signing and encryption, these are not activities supported by TACC personnel. Issued certificates are not suitable for legally binding digital signatures on financial or contractual documents.
- Host and Service certificates can be used to identify a named resource or service and for encryption of communication via SSL/TLS. These certificates may be used to authenticate the resource or service to another Grid entity.

Relying parties may or may not also be subscribers.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

The TACC Classic CA issues long-term RFC5280 X.509 v3 certificates to natural persons, hosts and services relevant to scientific computing users and resources in grid organizations or VOs.

1.4.1 Appropriate Certificate Uses

CA certificates may only be used to issue certificates and for checking certificates that claim to be issued by the TACC Classic CA. The end-entity certificate may be used for any application that is suitable for X.509 certificates such as integrity and non-repudiation (see Section 6.1.7), in particular:

a) Authentication of users, hosts and services;
b) Authentication and encryption of communications;

Certificates may only be used or accepted for actions authorized by the certificate keys.

1.4.2 Prohibited Certificate Uses

The certificates issued by the TACC Classic CA must not be used for financial transactions. Certificates must not be used for purposes that violate US or Texas law or the law of the country in which the target entity (i.e. application or host to use) is located.

Certificates issued by the TACC Classic CA do not claim legal value, nor does the ownership of a certificate issued by the TACC Classic CA imply automatic access to any kind of computing resources.

1.5 Policy Administration

The Texas Advanced Computing Center (TACC) operates the TACC PKI infrastructure and is responsible for drafting, registering, maintaining and updating this CP/CPS.

1.5.1 Organization Administering the Document

Texas Advanced Computing Center (TACC)
University of Texas at Austin
Research Office Complex 1.101, J.J. Pickle Research Campus
10100 Burnet Road (R8700), Building 196
Austin, TX 78758-4497
Telephone: (512) 475-9411
Fax: (512) 475-9445

1.5.2 Contact Person

All inquiries about TACC Classic CA operation and usage may be directed to:

Margaret Murray, Ph.D.

Texas Advanced Computing Center

10100 Burnet Rd. (R8700)

Austin, TX 78758-4497 USA

(512) 232-7124

ca@tacc.utexas.edu.

1.5.3 Person Determining CPS Suitability for the Policy

A committee of TACC staff members representing the Advanced Computing Systems, High Performance Computing, and Distributed and Grid Computing groups reviews TACC Classic CA policy and procedures.

Questions about TACC CP/CPS may currently be directed to Margaret Murray, Ph.D. at the above address. Alternately, she may be reached via email at marg@tacc.utexas.edu or by telephone at (512) 232-7124.

1.5.4 CPS Approval Procedures

The TACC Classic CA seeks accreditation by The Americas Grid Policy Management Authority (TAGPMA).

TAGPMA accreditation requires review of the TACC Classic CA CP/CPS by at least two TAGPMA members and a face-to-face presentation of TACC Classic CA policy and procedures at a TAGPMA meeting to determine whether the CP/CPS meets the requirements of the IGTF Classic CA 4.2 profile.

1.6 Definitions and Acronyms

The key words " MUST" , " MUST NOT" , " REQUIRED" , " SHALL" , " SHALL NOT" , " SHOULD" , " SHOULD NOT" , " RECOMMENDED" , " MAY" , and " OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Acronym	Term	Definition
CA	Certificate Authority	The entity / system that issues X.509 identity certificates. The CA places a subject name and public key in a document and then digitally signs that document using the private key

		of the CA.
CP	Certificate Policy	A named set of rules that indicate the applicability of a certificate to a particular community and/or class of applications with common security requirements.
CPS	Certification Practice Statement	A statement of the practices that a certificate authority employs to issue certificates.
CRL	Certificate Revocation List	A periodically updated list of certificates no longer valid for use by a particular community and/or class of applications with common security requirements.
CSR	Certificate Service Request	A formal request by a subscriber for issuance of a TACC Classic CA X.509 certificate.
	Host Certificate	A certificate for host/server identification as well as encryption of encrypted SSL/TLS communications between secure hosts.
LRA	Local Registration Agent	A person authorized by their organization and the TACC Registration Authority to perform identity vetting and approve or reject certificate service requests (CSRs).
	Person / User Certificate	A certificate for identifying a natural person.
PKI	Public Key Infrastructure	The combination of people, hardware and software used to implement X.509 certificate creation, usage and management (including revocation).
RA	Registration Authority	An infrastructure for initial identity validation of persons requesting person certificates and system administrators requesting host or service certificates.
	Relying Party	Natural persons, hosts or services controlling access to their computation or storage resources by validating identity certificates.
	Service Certificate	A certificate for uniquely identifying a named service.
	Subscriber	A natural person who requests a person certificate or a system administrator who requests a host or service certificate.
VO	Virtual Organization	An organization created to represent a particular research or development effort independently of the physical sites where its scientists or engineers work.
HSM	Hardware Security Module	A FIPS 140-2 Level 3 validated device providing tamper-proof protection of TACC PKI CA keys.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The online repository of information from the TACC Classic CA is accessible at the URI http://www.tacc.utexas.edu/CA/. As a member of the TAGPMA, the TACC Classic CA grants the IGTF and its PMAs the right of unlimited redistribution of this information.

2.2 Publication of Certification Information

The TACC Classic CA publishes the following information on its public website at URL: http://www.tacc.utexas.edu/CA/:

- TACC Classic CA CP/CPS documents
- The self-signed TACC Root CA certificate that acts as the trust anchor for the TACC PKI infrastructure.
- TACC Classic CA certificate (in both PEM and DER formats)
- TACC Classic CA certificate signing policy
- A link to the current TACC Classic CA Certificate Revocation List (CRL) in both PEM and DER formats.

2.3 Time or Frequency of Publication

Public information on the TACC Classic CA website is intended to be current. Documents will be posted as soon as possible or within one working day of any approved changes or modifications.

The TACC Classic CA Certificate Revocation List (CRL) is published every hour and expires 7 days later.

This CP/CPS will be published whenever it is updated and after approval of the TAGPMA.

2.4 Access Controls on Repositories

The online repository is maintained on a best effort basis and is available substantially 24 hours per day, 7 days per week, subject to reasonable scheduled maintenance. Outside the period 08:00-17:00 Monday-Friday it may run unattended “at risk”.

The TACC Classic CA does not impose any access control on its CP/CPS, its CA certificate, issued certificates or CRLs. However, only an authenticated Repository Administrator may create, update, delete and modify files in the repository.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The certificate subject names used as unique certificate identifiers obey the X.501 standard. Subject names have a fixed and a variable component. The certificate subject names start with the fixed component to which a variable component is appended to make it unique.

The fixed component is common to all certificates issued by the TACC Classic CA and is used to identify the namespace that can be signed by the CA. The fixed component is as follows:

/DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC Classic CA

The variable component shall contain a common name (CN) that uniquely identifies the subject name within the CA namespace. This common name must be obtainable from the subject's real name as stated in section 3.1.2. For computer systems or services, the common name is the DNS fully-qualified domain name (FQDN) of the system. IP addresses are not acceptable.

Certificate requests made to the TACC Classic CA may contain names that might reasonably be assumed to be the trademark or well-known nickname of a grid or virtual organization (VO). If this is true, then the signing requestor must demonstrate his/her right to make use of this name, and must provide documentation that the organization has previously delegated to TACC the right to sign a certificate containing this name.

3.1.1 Types of Names

The common name (CN or variable part of the DN) for names on User, Host and Service certificates are defined below:

User Certificates: CN names must be obtainable from the subject's real name and uniquely map to the individual for the validity period of the entire TACC PKI. Uniqueness validation occurs in the TACC Accounting System (TAS). In case of a potential duplicate, the database adds a distinguishing record number uniquely associated with that user. In this way, subject names can uniquely map to the individual in perpetuity regardless of the certificate's validity period. Examples:

- **/DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC Classic CA/CN=John Doe.**
- **/DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC Classic CA/CN=John Doe 67513**

Host Certificates: The CN entry for a host shall be the fully qualified domain name (FQDN) that can be universally used to access that host. Example:

- **/DC=EDU /DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC Classic CA/CN=host1.tacc.utexas.edu**

Service Certificates: The CN entry for a service shall be the name of the application followed by a slash ("/") followed by the FQDN. Example:

- **/DC=EDU/DC-UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC Classic CA/CN=gridftp/tg-gridftp.lonestar.tacc.teragrid.org**

CNs must be encoded as Printable Strings according to RFC1778 and RFC2252. The maximum length of CNs is 128. Compound characters shall be represented by their ASCII equivalent. Characters allowed in the common names of personal certificates are as follows:

a) Numbers 0 – 9
b) Letters A – Z and a – z
c) Special characters ' '(space); '('; ')'(left and right parentheses); and '-' (hyphen)

In addition, the characters '.' (period) and '/' (slash) are allowed in host and service certificates. The period must be used to separate the DNS host components and the slash must be used to separate the service name from the DNS host name.

3.1.2 Need for Names to be Meaningful

Common names (CNs) must be related to (and express a reasonable association with) the authenticated subscriber's real name and organization.

3.1.3 Anonymity or Pseudonymity of Subscribers

No user certificates shall be issued to roles or functions, only to named persons who provide sufficient documentation of their identity to a designated LRA. Pseudonymous and anonymous certificates are not permitted.

In the event of a gateway or community account, user or service certificates may be issued to enable back-end roles or functions, but only if the relevant grid or VO can map community account usage back to an individual DN from an authenticated and valid long-term certificate. Mapping must occur upon request.

A designated LRA can approve requests for establishment of gateway or community service certificates only if they include valid name and contact information for a natural person who takes responsibility for certificate and account configuration, usage, and who will respond to any usage mapping requests.

3.1.4 Rules for Interpreting Various Name Forms

Refer to sections 3.1.1 and 3.1.2.

3.1.5 Uniqueness of Names

The TACC Classic CA supports only one unique name (CN) per natural user subscriber. Under this CP/CPS policy, two names are considered identical if they differ only in case, punctuation or whitespace. Thus letter case, punctuation or whitespace are insufficient to differentiate names. Instead, the TACC Accounting System (TAS) tracks and validates the uniqueness of requested names across the entire TACC PKI during initial registration.

A person's Common Name must represent the same person irrespective of differences in grid or VO specific Subject DN attributes on multiple certificates held by that person. If a subsequent certificate request comes from a different person with the same name, then a unique identifying record number must be added to the latter's CN to distinguish those persons. Furthermore, subscribers must not share private keys or certificates.

3.1.6 Recognition, Authentication, and Role of Trademarks

The TACC Classic CA does not guarantee that the subject names of issued certificates will contain the requested trademarks. The TACC Classic CA shall not issue a certificate knowing that it infringes the trademark of another. A committee of TACC staff members representing multiple TACC groups shall resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

Certificate subscribers must prove their identity to a designated TACC Classic CA Local Registration Agent (LRA) at an initial face-to-face meeting. The appointed TACC LRA approves or rejects certificate requests based on personal knowledge of the requesting party and implements those requests only via a customized web interface running on a secure SSL/TLS encrypted channel and requiring bi-directional certificate authenticated access. The web interface organizes and validates data collected at the initial registration meeting according to site, grid or VO specific policy.

Validation requirements for different site, grid and VO organizations may vary in implementation but not function. For example, in the TeraGrid, the TACC Classic CA trusts AMIE user packets periodically sent from the central TeraGrid Account database while UTGrid requires a valid "UT-EID". Each LRA is trained to recognize the level-of-assurance of different initial identity validation requirements, and to conduct initial identity vetting accordingly.

3.2.1 Method to Prove Possession of Private Key

The possession of the private key by the requestor is considered proven when the digital signature of the certificate signing request (CSR) can be verified using the public key present in that request, and the request is verified by the LRA as coming from a valid subscriber who is the subject of that request.

3.2.2 Authentication of Organization Identity

The first time an organization/unit wants to get a certificate for a natural person, a server or a service, or wants to designate an LRA, it contacts a TACC Security Officer to formalize the relationship between the TACC Classic CA and that organization/unit's

authentication process. The TACC Security Officer must ascertain that the organization or organizational unit exists and is entitled to request TACC certificates. It must also validate and train the LRA put forth by the organization/unit to sign certificate requests on behalf of that organization. Every attempt will be made to designate an LRA local to a participating organization capable of identifying valid members face-to-face. These "remote" RAs perform the same tasks as local TACC Classic LRAs but only for their site, VO or domain.

3.2.3 Authentication of Individual Identity

The RA shall verify that the requesting party's organization or a unit of an organization is entitled (see 1.3.3) to get a certificate from the TACC Classic CA and that s/he consents to the request and the certificate acceptable use policy (AUP).

The first time an organization/unit wants to get a certificate for a natural person, a server or a service, or wants to instantiate an LRA, it has to announce this officially to the appropriate RA and the TACC Security Officer or CA Manager. The designated LRA must ascertain that the organization or organizational unit exists and is entitled to request TACC certificates.

For individuals, identity is verified against a government issued photo ID and either their record published in an organizational directory, or a letter of introduction signed by an authorized organization authority.

For each authentication, the LRA will record and archive:

- A verified CN, organization, email, phone number and address of the requester from the official published phone directory maintained by the academic or research organization or government lab. Alternately, a letter of introduction from an official organization authority will be accepted.
- In-person or remote video verification or government documents with picture that confirm the user is who s/he says s/he is;
- The document(s) used as proof of relationship with the organization or organizational unit;
- An LRA assessed level-of-assurance (LoA) of the identity presented by an organization.
- The date, time and place of the authentication;
- Whether the authentication was successful or not and why.

For host or service certificates, requests must be signed by a TACC Classic CA or other IGTF accredited personal certificate corresponding to the system administrator or person responsible for the resource. The designated LRA will verify whether the requester has the right to request a certificate for the intended host or service, usually by checking with a site security officer. The designated LRA must also verify that requested host names are associated with public 'A' records in registered DNS namespace.

3.2.4 Non-verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

The person nominated to become a TACC LRA must have the authority to identify the users within their organization or unit as well as owners responsible for systems or services. The designated LRA must agree to field all questions related to certificate requests for their site, VO or domain.

Designated LRAs implement the provisions outlined in 3.2.3. The use of the designated LRA's user certificate to access TACC's RA web interface shall be sufficient for authenticating all future information exchanges with or requests from that organization/unit. When any organization/unit within a site, VO or domain rescinds an individual's authorization to be the designated LRA, it must inform its RA and the TACC CA Manager of this fact in the same way as the authorization was established. Upon receipt of such notice, the TACC Security Officer or CA Manager will disable that user's access to the RA web interface.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Certifications must not be renewed or re-keyed for more than 5 years without a form of auditable identity and eligibility verification. Rekey before the certificate expires can be done using a secure web interface or by sending a re-key request based on a new public key in an email signed with the old private key to the appropriate TACC LRA. If the certificate subject is a person s/he must still provide the LRA with proof of a relationship with the organization(s) mentioned in the certificate subject name (See Section 3.2.2). Although a proof of relationship is required, a re-key prior to 5 years from the initial face-to-face meeting does not require the physical presence of the subject. (If proof of relationship is performed, supporting documents can be sent to the LRA by surface mail or faxed to a physically secured fax machine). After 5 years, the LRA must re-verify identity either in-person or via remote video as stated in Section 3.2.3. After expiration of the certificate no rekey is possible. A new application for initial registration must be made instead.

3.3.2 Identification and Authentication for Re-key after Revocation

After revocation of a certificate, no re-key is possible. A new certificate must be requested and initial registration checks must be repeated.

3.4 Identification and Authentication for Revocation Request

Unless the revocation request originates from the TACC Classic CA because it has independently verified that a key compromise has occurred, the revocation request must be verified and the requesting party must be authenticated. Such a request coming from

an LRA can be made using the TACC secure web interface or in an email sent to the TACC CA Manager signed by a valid non-expired certificate. Before revoking a certificate the TACC Classic CA has to authenticate the source of the request as it did for the request for certification. Such a revocation request must be made by:

- The owner of the certificate in an email signed with the private key associated with the non-expired certificate;
- The owner, in person, with a designated LRA who must authenticate the requestor following the same procedure for a certificate request (See section 3.2.3);
- On behalf of the owner who lost his/her private key in an email signed by an authorized person of the organization/unit that consented to the certificate;
- On behalf of the organization/unit that consented to the certificate in an email signed by an authorized person;
- The designated LRA who has knowledge of a key compromise.

In case of emergency the revocation can be initiated via oral communication with the appropriate LRA or to a TACC Security Officer or CA Manager who will make a best effort attempt to authenticate the request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The TACC Classic CA issues certificates to members of grid or virtual organizations who have previously established a formal relationship with the TACC Classic CA. Examples of who may apply are as follows:

- Users of a participating grid or VO
- Project or System administrator of a host or hosts of a participating grid or VO
- Project or System administrator of a service or services provided on a host in a participating grid or VO.

4.1.2 Enrollment Process and Responsibilities

The requesting party generates the key pair with a size of at least 1024 bits on their system through the form provided by the TACC Classic CA web interface. After this form has been completed, the encrypted private key will be stored on the system where the browser runs in a file only accessible to the requestor (if the operating system allows such a restriction), and the Certificate Signing Request (CSR) will be sent to the appropriate LRA of the TACC Classic CA. If using the browser for this purpose is not appropriate (e.g. when a secure hardware device generates the key pair), the CSR in PKCS #10 format can be generated using appropriate software (e.g. OpenSSL) and uploaded to the secure web interface sent to the appropriate LRA. In this case, the subscriber must coordinate with the TACC CA Manager beforehand to get the correct DN to be included in the request.

By submitting an application, TACC Classic CA subscribers are confirming that they have read and will adhere to the procedures published in the TACC Certificate Acceptable Usage Policy. In summary they must:

1. Only use GRID resources to perform work, or transmit or store data consistent with academic research sponsored by their institution or organization and in compliance with resource usage conditions.
2. Refrain from the following unacceptable activities:
    - Using, or attempting to use, GRID resources without authorization or for purposes other than those related to your sponsored research.
    - Tampering with or obstructing the operation of the facilities
    - Reading, changing, distributing, or copying others' data or software without authorization
    - Using GRID resources to attempt to gain unauthorized access to other (non-GRID) sites
    - Activities in violation of local or federal law
3. Immediately report any known or suspected security breach or misuse of GRID resources, or any misuse of their registered TACC credentials. Request certificate revocation by notifying your RA, the TACC Classic CA and any relying parties immediately:
    - If the private key is lost, destroyed or compromised;
    - If the subscriber is no longer entitled to a certificate, or;
    - If the information in the certificate is no longer correct or is inaccurate.
4. Use GRID resources at their own risk. There is no guarantee that GRID resources will be available at any time or that they will suit any purpose. Services are provided on a best-effort basis, subject to planned and emergency maintenance outages.
5. Ensure the confidentiality of any intellectual property or other confidential data used on GRID resources. GRID sites provide technology to preserve the confidentiality of data, but it is their responsibility to use that technology appropriately.
6. Appropriately acquire and use all software used on GRID systems according to the specified licensing. Possession or use of illegally copied software or unauthorized distribution of copyrighted software or materials is prohibited and subject to penalties.
7. Recognize that access to GRID resources is explicitly governed by the existing policies of the institution through which you gain such access, as well as the existing usage policies of the resources accessed through grid methods.
8. Take every precaution to prevent any loss, disclosure or unauthorized access or use of certificate key materials:
    - Generate a key pair using a trustworthy method;
    - Select a strong passphrase with a minimum of 12 characters; and
    - Protect the passphrase from others, in the case of user certificates.
9. Authorize the processing and conservation of the personal data required for the request verification process (as required under applicable data protection regulations such as UT-System Information Resources Use and Security Policy

(UTS 165).

These restrictions are part of the TACC Certificate AUP (See Appendix A) available on the TACC Classic CA web site.

4.2 Certificate Application Processing

Users may request certificates through a secure web interface responsible for queuing these requests for consideration by the RA. Designated LRAs must arrange for a face-to-face initial registration meeting where the LRA will approve or reject pending certificate requests. TACC LRAs interface with the TACC Accounting System (TAS) and the TACC Classic CA.

4.2.1 Performing Identification and Authentication Functions

Any TACC LRA must possess a valid TACC Classic user certificate and use a secure web interface to validate pending certificate submission requests. The LRA will record and archive identity checks as specified in Section 3.2.3.

4.2.2 Approval or Rejection of Certificate Applications

The LRA reviews collected subscriber information and if satisfied, checks “Approve” or “Reject” in the secure web interface. RAs may also choose to make additional inquiries or contacts in order to make a decision.

4.2.3 Time to Process Certificate Applications

The turn-around time from request to issuance depends mostly on the authentication process, and should not be more than 10 working days. If the authentication information proves to be inaccurate or if a requesting party fails to meet the authentication requirements within 9 days after the RA receives the request, it shall be rejected. If the requesting party insists on getting a certificate after a rejection event, a new request must be initiated.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The CSR shall be transferred electronically to the on-line signing computer running only the services necessary for the CA operations. On this system, the certificate will be created and signed with the private key of TACC Classic CA. The signed certificate shall then be transferred electronically to the TACC online web server. The subject DN is also recorded in the TACC Accounting System (TAS) for auditing purposes.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The TACC Classic CA web interface will notify the subscriber of certificate issuance by email sent on behalf of the RA.

4.4 Certificate Acceptance

Notification email will contain a link to a certificate acceptance web page.

4.4.1 Conduct Constituting Certificate Acceptance

Interaction with the certificate acceptance web page validates certificate usability.

4.4.2 Publication of the Certificate by the CA

New certificates will be published on the TACC CA website within one hour of generation.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Certificates issued by the TACC Classic CA and their associated private keys must only be used according to the permissions and prohibitions stated in section 1.4. They must only be used according to the key usage fields of the certificate. When a certificate is revoked or has expired the associated private key should no longer be used.

4.5.2 Relying Party Public Key and Certificate Usage

A relying party should, upon being presented with a certificate issued by the TACC Classic CA check its:

a. Validity by:
    - Checking that it trusts the CA that issued the certificate,
    - Checking that the certificate hasn't expired
    - Consulting the TACC Classic CA CRL in effect at the time of use of the certificate or querying the certificate's validity using the OCSP facility, after its planned installation.
b. Appropriate usage as outlined by the CP pointed to by the certificate and the usage keys included in the certificate

4.6 Certificate Renewal

Certificates may not be renewed. Instead, a new certificate may be requested.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Others

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

For security reasons, the certificate re-key is the preferred method for issuing a new certificate to a subscriber whose certificate is about to expire or who require a change in the certificate's parameters.

The TACC Classic CA does not perform a re-key of a certificate after its revocation. A new certificate must be requested and the procedure for obtaining a new certificate must be followed.

4.7.2 Who May Request Certification of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificates must not be modified. The old certificate must be revoked and a new key-pair must be generated and a request for the modified certificate contents submitted with the new public key. The revocation may be conditioned on the issuance and acceptance of the new certificate. Thus, the old certificate will only be revoked after the new one is accepted.

4.8.2 Who May Request Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Others

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate will be revoked when the information it contains or the implied assertions it carries are known or suspected to be incorrect or compromised. This includes situations where:

- The TACC Classic CA is informed that the subscriber has ceased to be a member of or associated with a TACC related program or activity,
- The end user loses his/her private key or suspects it to be compromised,
- It is not needed any more,
- The information in the subscriber' s certificate is wrong or inaccurate, or suspected to be wrong or inaccurate
- The private key of the TACC Classic CA has been compromised or lost. (In this case, all certificates signed with it shall be revoked.)

4.9.2 Who Can Request Revocation

In addition to the subscriber, who must request revocation if any of the circumstances

outlined in Section 4.9.1 arise, a certificate revocation can be requested by:

- The owner of the certified host or service system
- TACC security officers or any designated LRA who has proof of a compromise
- The organization that wants to revoke its consent to its inclusion in the certificate
- The LRA who authenticated the holder of the certificate in the event of a mistake or change of data
- Any person presenting proof that the subscriber's private key has been compromised or that the subscriber's data have changed.

4.9.3 Procedure for Revocation Request

Unless the TACC Classic CA acts on its own a revocation request must be made:

- By the owner of the certificate, properly authenticated, using the online revocation facilities. In case of emergency, the owner of the certificate must contact either the designated LRA or a TACC security officer as soon as possible and ask the appropriate LRA to request revocation.

Before revoking a certificate the TACC Classic CA shall authenticate the source of the request according procedures as used for the initial registration.

4.9.4 Revocation Request Grace Period

No grace period is defined for a revocation request. The TACC Classic CA will process authenticated revocation requests promptly and will publish the revocation to the CRL as soon as possible or within one business day.

4.9.5 Time within which CA must Process the Revocation Request

No grace period is defined for a revocation request. The TACC Classic CA will revoke the certificate as soon as possible and publish the revocation on its CRL immediately or within one hour.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties should check certificates against the TACC Classic CA CRL before using them.

4.9.7 CRL Issuance Frequency

The TACC Classic CA issues a new CRL every hour that remains valid for seven days.

4.9.8 Maximum Latency for CRLs

Each CRL issued by the TACC Classic CA will be posted to the repository immediately upon issuance and prior to the value in the nextUpdate field of the preceding CRL.

4.9.9 On-line Revocation/status Checking Availability

The latest CRL is always available from the TACC Classic CA web site. The TACC Classic CA shall publish the CRL in effect in its repository (see 2.1). No other on-line checking is available now, but an OCSP facility is possible in the future.

4.9.10 On-line Revocation Checking Requirements

Relying parties must check the CRL before they use and trust a certificate. No access control shall limit the possibility to check the CRL.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

The TACC Classic CA does not suspend certificates.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The TACC Classic CA shall store in its public repository and make them available via its web site the contents described in Section 2.2

4.10.2 Service Availability

The TACC Classic CA shall run this service continuously, except for unavoidable maintenance and outages. Due to the nature of the Internet this service cannot be guaranteed.

4.10.3 Optional Features

The TACC Classic CA may offer an OSCP service at a later date.

4.11 End of Subscription

The subscription ends with the expiry of the certificate. A subscription may end earlier if the subscriber requests a revocation of its certificate or if the subscriber ceases their association with an approved TACC project or organization.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No key escrow or recovery services are provided. The key owner must take all reasonable steps to prevent loss of his/her private key.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

See Section 4.12.1.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section discusses specific TACC procedures related to its facility and TACC Classic CA operation.

5.1 Physical Controls

5.1.1 Site Location and Construction

The TACC on-line Classic CA system resides in a locked rack in an access-controlled TACC computer room. A FIPS 140 compliant HSM exports CA private key backups to Smart Cards. Smart Card media is then stored in a sealed (tamper-evident) envelope in the fireproof safe residing in the same locked rack.

5.1.2 Physical Access

Only TACC Security Officers or CA Managers may access the locked rack, the safe or any servers located inside the locked rack.

5.1.3 Power and Air Conditioning

The TACC on-line Classic CA server operates in an air-conditioned environment and is not rebooted or power-cycled except for essential maintenance.

5.1.4 Water Exposures

Online machines are located in a first floor computer room with a raised floor and sprinkler system.

5.1.5 Fire Prevention and Protection

The media and key archive storage safe is fireproof. The computer room contains fire warning and protection systems that meet University of Texas standards.

5.1.6 Media Storage

All media used for:

- Backup storage of TACC Classic CA private keys encrypted on Smart Cards;
- Backup copies of CA related information kept on CD or DVD;

are stored in sealed labeled envelopes in the locked fireproof safe located inside the locked rack to which only authorized personnel have access. Access to this safe will be logged.

5.1.7 Waste Disposal

Waste containing data to be protected (cryptographically relevant data like private keys or passphrases, or personal data) shall be disposed of in a way to guarantee that the information may not be re-used.

5.1.8 Off-site Backup

A copy of essential CA keys and passphrases will be stored in sealed envelopes with a check-out/check-in logbook in a 2nd separate safe place.

5.2 Procedural Controls

5.2.1 Trusted Roles

Personnel performing the following roles for the TACC Classic CA must be trusted:

- TACC Security Officers are responsible for overseeing administration of all TACC security and identity vetting functions.
- TACC CA Manager(s) are responsible for secure operation and maintenance of the CA system.
- Designated LRAs record and archive results of the identity validations they perform.
- Software developers of the web interface follow best practices and make their code available for validation or verification.
- Software developers of TACC Accounting System (TAS) ensure that relevant functions comply with this CP/CPS

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for each Role

All roles must be performed by full-time staff subject to organizational governance.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The TACC Classic CA Managers must have Linux sysadmin experience as well as experience using and managing grid certificates.

Designated LRAs must have experience using and managing grid certificates and familiarity with using the RA web interface.

Software developers must follow security best practices and test code for potential compromise.

5.3.2 Background Check Procedures

TACC Classic CA personnel will be full-time University of Texas – Austin employees who meet state and university requirements for employment. No specific background check is required.

Designated LRAs must have official documented standing with both the TACC Classic CA and the organization hosting the LRA and must have authority to perform RA identification functions as stated in an official letter to the TACC Root CA. A TACC Security Officer accepts this letter. A "Request for TACC LRA Designation" letter template (See Appendix B) is available from the TACC CA website.

5.3.3 Training Requirements

TACC Classic CA personnel will receive training in:

- Security hardware operation of the hardware security module (HSM).
- Web interface usage
- Organization, Grid or VO specific identity requirements
- Security software maintenance and usage
- Physical and procedural security mechanisms.

5.3.4 Retraining Frequency and Requirements

Retraining shall be mandatory when new software or features, as well as new organizational procedures are introduced.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

In the event of unauthorized actions, abuse of authority or unauthorized use of entity systems by the CA or RA personnel, the TACC Security Officers may revoke the privileges concerned.

Sanctions for unauthorized actions by TACC Classic CA personnel follow University of Texas personnel policy and procedures.

5.3.7 Independent Contractor Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

All TACC Classic CA personnel shall be provided with all documentation required to successfully perform their assigned tasks.

Training documentation containing sanitized examples will be provided to TACC Classic CA and LRA personnel on request.

5.4 Audit Logging Procedures

Audit logging is treated as confidential information and will be archived in the TACC Accounting System (TAS).

5.4.1 Types of Events Recorded

The TACC Classic CA logs the following CA functions:

- Issued signed certificates or Certificate submission requests (CSR) processing problem
- Revoked Certificates
- CRL creation
- Web interface software release date, version number and verification checksum
- CA system reboot / login / logout

The TACC Classic CA also logs the following RA functions:

- Identity check (indicating all supporting documentation, including AUPs, agreements, approval or rejection)
- RA designation and all supporting documentation including ID, AUPs, agreements)

5.4.2 Frequency of Processing Log

The TACC Accounting System (TAS) will provide logging reports to the TACC Classic CA Security Officers on a monthly basis or upon individual request.

5.4.3 Retention Period for Audit Log

Audit logs will be stored for a minimum of three years.

5.4.4 Protection of Audit Log

CA and RA events in the audit logs are treated as confidential information. Audit logs are viewable only by TACC Security Officer personnel or internal or external auditors. When processed, the archives are copied to a read only off-line medium and stored in a safe place. The protection shall be state-of-the-art best effort. Logs will be signed by the TACC Security Officer's key.

5.4.5 Audit Log Backup Procedures

The TACC Accounting System (TAS) and CA system excluding the HSM are routinely backed up according to best practices for data backup onto the TACC hierarchical storage manager archive system.

5.4.6 Audit Collection System (internal vs. external)

CA and RA events may be burned to CDROMs suitable for either internal or external review. The audit collection system is internal to TACC CA.

5.4.7 Notification to Event-causing Subject

Notification to event-causing subject occurs first by sending email to the email contact recorded in the TACC Accounting System (TAS) from the certificate submission request process.

5.4.8 Vulnerability Assessments

Part of the annual audit will include an assessment of known vulnerabilities and countermeasures.

5.5 Records Archival

5.5.1 Types of Records Archived

See 5.4.1.

5.5.2 Retention Period for Archive

The minimum retention time is 3 years.

5.5.3 Protection of Archive

Archives are accessible only by TACC accounting and security personnel or internal or external auditors.

5.5.4 Archive Backup Procedures

Records shall be backed up routinely according to best practices for data backup onto the TACC hierarchical storage manager archive system.

5.5.5 Requirements for Time-stamping of Records

All event records shall bear a time-stamp based on system synchronization with ntp.

5.5.6 Archive Collection System (internal or external)

The archive collection system is internal to the TACC PKI. Information considered confidential is not made available to be public. Information considered non-confidential may be made available to the public only if the information is kept on-line.

5.5.7 Procedures to Obtain and Verify Archive Information

Not defined**.**

5.6 Key Changeover

As end-entity key generation is carried out by the subscriber (e.g., using a web browser), no provision is made by the TACC Classic CA for a key changeover. In the case of a changeover of the TACC Classic CA's key pair, an overlap of the old and new keys will exist. While the new key will be used for signing certificates, the older but still valid

certificate must be available to verify old digital signatures – and the private key to sign CRLs – until all the certificates signed using the associated private key have also expired. The overlap of the old and new key must therefore be at least as long as the validity of an end entity certificate (see Section 4.3.2).

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If the private key of an end entity is lost or compromised due to corruption, the end entity must inform their RA immediately in order to request the revocation of their certificate. All relying parties known to accept the key should be informed by the owner of the key.

The private key of the TACC Classic CA is protected by a FIPS 140 validated hardware security module (HSM). If that device gets tampered, then the TACC CA Manager must recover keys from secured backup media.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The TACC Classic CA will take best effort precautions to enable recovery.

In order to be able to resume operation as fast as possible after the compute basis of the TACC Classic CA is corrupted the following steps shall be performed:

- All TACC Classic CA software shall be backed-up onto removable media after a new release of any of its components is installed and stored in a locked, fireproof safe.
- In case of corruption of any part of the running system, replacement hardware shall be loaded with the latest backup of the software and data last known to be uncorrupted. Any certificates logged as issued subsequent to the last known uncorrupted backup must be re-issued.
- If not all encrypted copies of the TACC Classic CA private key are destroyed or lost, and are not compromised, CA operation shall be re-established as soon as possible without need to revoke all issued certificates.
- If public certificates stored in the repository are lost or corrupted, they will be revoked.

5.7.3 Entity Private Key Compromise Procedures

In case the private key of an end entity or an RA is compromised, any corresponding certificates must be revoked. All relying parties known to accept that key should be informed by the owner of the key.

If an end entity's certificate private key is compromised the certificate will be revoked following the procedure in Section 4.9. If an end entity's public key needs to be revoked, the same procedure should be followed. After revocation, the user will have to request a new certificate

5.7.4 Business Continuity Capabilities after a Disaster

The TACC Classic CA is located within the infrastructure of the University of Texas at Austin. Any disaster recovery facilities made available by this infrastructure to TACC will be applied to continue TACC Classic CA operation.

5.8 CA or RA Termination

Before the TACC Classic CA terminates its services, it will

- Notify designated TACC LRAs.
- Notify subscribers and relying parties, including all participating grids and VOs.
- Make information of its termination widely available.
- Stop issuing certificates.
- Revoke all certificates.
- Issue a final CRL
- Notify relevant security contacts.

An advance notice of no less than 60 days will be given in the case of normal (scheduled) termination. Upon termination, all copies of its private key will be destroyed. The TACC Security Officers at the time of termination shall be responsible for the subsequent archival of all records as required in section 5.5.2.

6 TECHNICAL SECURITY CONTROLS

This section discusses technical aspects specific to the operation of the TACC Classic CA.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The TACC Classic CA will use OpenSSL toolkit with the PKCS11 ‘dynamic’ engine to generate and protect its private key pairs.

The TACC Classic CA does not generate private keys for subjects. Where possible, trusted software within a customized public web interface will facilitate key generation on behalf of requesting users on their own systems.

6.1.2 Private Key Delivery to Subscriber

Each subscriber must generate his/her own key pair using a trustworthy method. Therefore delivery of private keys is not required. The TACC Classic CA will provide a public web interface to guide certificate requests

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber’s public keys are uploaded to the secure TACC Classic CA server via a bi-directionally authenticated SSL/TLS connection through the RA web interface.

6.1.4 CA Public Key Delivery to Relying Parties

Download the TACC Classic CA certificate containing its public key from the public website at http://www.tacc.utexas.edu/CA/ . Alternately, the CA certificate can also be obtained from the IGTF's TAGPMA repository to which a copy will be securely transferred once accreditation has been approved by the TAGPMA.

6.1.5 Key Sizes

Keys of length less than 1024 bits (RSA modulus) are not accepted. The TACC Classic CA key is of length 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

There is no stipulation as to the validity and quality of the generated end entity key pair. Only the validity of the certificate issued by the TACC Classic CA is defined by this CP/CPS document.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The TACC Classic CA issues X.509 v3 certificates which are valid if they have been signed by the TACC Classic CA's private key and have not been revoked, i.e. do not appear in the currently valid CRL.

The keys may be used according to the type of certificate. Uses of an end-entity certificate may include:

- Authentication
- Non-repudiation
- Data and key encryption
- Message integrity
- Session establishment
- Proxy creation and signing

The Classic CA's private key is the only key that can be used for signing TACC Classic certificates and CRLs.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The TACC Classic CA signing private key is managed by a FIPS 140 compliant Hardware Security Module (HSM). This private key is stored in 3DES encrypted form in tamperproof HSM memory. The private key is never available in plain text form (that is, in a usable form) to the server operating system or any back up service. The private key is managed via software based on OpenSSL and the PKCS11 'dynamic' engine. Backups of the encrypted private key occur only to smart cards. Access to these keys is only available through the device API. Several copies of PCI smart cards containing backups

of the private key have been created and stored in a locked safe accessible only to TACC Security Officers or CA Managers.

6.2.1 Cryptographic Module Standards and Controls

The TACC Root CA server contains a tamper-proof FIPS 140 Level 3 validated Hardware Security Module.

TACC Security Officers have separate password (aka PIN) access to the entire HSM device and may create and delete slots and initial Slot Administrator passwords where each slot corresponds to a separate TACC CA. Security Officers may also check HSM logs; reset passwords an perform backups or maintenance on the HSM.

TACC CA Managers may use Administrator PINs to separately manage each HSM slot (i.e. TACC Root; TACC Classic; TACC MICS). CA Managers use these password/PINs to create key pairs and verify key attributes.

Each CA slot also has a separate application password used by the software applications. The Classic CA web interface employs this application password to access the previously and separately created keypairs to sign certificate service requests and CRLs.

All HSM password/PINs are case-sensitive; support symbols; are at least 15 characters long and may be up to 32 characters long. PINs are set by humans using HSM utilities, and securely stored on the HSM. Current best practices for selecting unguessable PINs must be followed.

In addition, the HSM has additional protection against brute-force PIN/password attempts: After three failed login attempts, a multiple of 5 seconds delay is added before processing the PIN/password. So, after the 4th attempt there would be a 5sec delay, after the 5th attempt, a 10sec delay, after the 6th, a 15sec delay, etc.

No instance of the private CA key (plain or encrypted) shall reside on the permanent disk storage of any computer that is online except inside a tamper-proof FIPS 140 compliant Hardware Security Module (HSM).

An extra instance of private keys encrypted (wrapped) with a randomly generated passphrase of at least 15 characters shall be stored on removable Smart Card media in the secured and fire-proof safe.

The application passphrase is stored on read-only USB key on the CA server and is accessible only by root. Passphrases are also written down and stored on a different removable media or written down, and the paper shall be placed in a tamper-evident sealed envelope in the secured and fire-proof safe.

6.2.2 Private Key (m out of n) Multi-person Control

Not implemented.

6.2.3 Private Key Escrow

Not implemented.

6.2.4 Private Key Backup

All backup copies of the CA private key are kept at least as secure as the one used for signing (i.e. encrypted, and on media locked in a safe and in a separate secured place). The passphrase for activating the wrapping key on the private key backup is also stored in labeled sealed envelopes in both a locked safe and a separate secured place.

6.2.5 Private Key Archival

The CA private key may be exported from the FIPS 140 compliant HSM in encrypted form with an integrity preserving checksum to a Smart Card.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Only transfer methods supported by the FIPS 140 compliant HSM are supported.

6.2.7 Private Key Storage on Cryptographic Module

The TACC Classic CA private key is stored on tamper-proof FIPS 140 compliant HSM.

Access to the CA private key is activated by an application passphrase stored on a USB key on the CA server that can only be read by root. The CA private key passphrase is also kept in labeled sealed envelopes in both a locked safe and a separate secured place for use in an emergency.

One backup copy of the CA keypair is made to SmartCard using HSM utilities that also wrap this backup with a separate key and PIN. A second backup copy of the CA SmartCard is also stored in a separate safe place.

6.2.8 Method of Activating Private Key

The TACC Classic CA private key becomes active by using OpenSSL commands where the required application password/PIN is stored on a USB key on the protected CA server and accessed via stdin.

6.2.9 Method of Deactivating Private Key

Removing the USB key from the protected CA server deactivates the TACC Classic CA private key.

6.2.10 Method of Destroying Private Key

Initializing the CA slot on the FIPS 140 compliant HSM destroys all private keys on that slot. Tampering the HSM destroys all private keys on all slots.

6.2.11 Cryptographic Module Rating

TACC's HSM is validated at FIPS 140-2 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The TACC Classic CA archives all issued certificates on removable media that is stored offline in a secure fireproof safe.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Subscriber's certificates have a validity period of one year or less if the affiliation of the requesting party to the group participating in a TACC related project is less than one year.

The TACC Classic CA certificate has a validity period of 5 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The TACC Classic CA private key is protected by strong passphrases of at least 15 characters. Subscriber private keys must be protected by a pass-phrase of at least 12 characters.

6.4.2 Activation Data Protection

The Administrator and Application passphrases must be known only by the CA Manager. Any backup of these private key passphrases (machine-readable or on paper) must be stored in secured place. No other persons are privy to the activation data. Activation data for the TACC Classic CA private key is also kept in a sealed envelope in a fireproof safe with manually logged access. In an emergency, the TACC Security Officer may access this copy of the private key prior to resetting it.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

The server hosting the CA web service is a Linux based system configured (or enhanced) with all reasonable security features considered common practice by the TACC Security Officer. All sessions must be authenticated using strong passwords for login/access.

Only TACC Security Officers or CA Managers may access the on-line TACC Classic CA server.

6.5.1 Specific Computer Security Technical Requirements

The server hosting the on-line TACC Classic CA runs a Red Hat enterprise Linux system with reasonable provenance.

Only services or software related to CA or RA operation are installed on the TACC Classic CA server. The server will receive occasional patches and other adjustments if the

security risk warrants, in the judgment of TACC Security Officers.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

Development of the TACC CA web interface follows security best practices, operates under change management control and is subject to security compromise analysis. Web interface releases are published with checksums as a countermeasure to unapproved modifications.

6.7 Network Security Controls

All communication with the TACC Classic CA server occurs over encrypted SSL/TLS tunnels on known ports by authenticated users. The TACC Classic CA operates on a VLAN that is actively monitored for intrusions and protected by both a hardware firewall and a software firewall.

6.8 Time-stamping

All time stamping will be synchronized to UT-Austin network-time-protocol (ntp) servers.

7 CERTIFICATE, CRL, AND OCSP PROFILES

This section articulates details of certificates and certificate revocation lists issued by the TACC Classic CA. The TACC Classic CA does not currently provide OCSP support.

7.1 Certificate Profile

All certificates issued by the TACC Classic CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 5280. The TACC Classic CA shall have the following Profile:

- The certificate shall be version 3 (i.e., the version number shall be 2);
- The issuer shall be: /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/CN=TACC Root CA
- The subject name shall be: /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN /CN=**TACC Classic CA**
- The signature algorithm shall be **sha1WithRSAEncryption;**

- The extensions shall contain:
    - **basicConstraints:** CA=true, critical;
    - **keyUsage:** certificate signing, CRL signing, critical;
    - Subject Key Identifier: SHA-1 hash
    - Authority Key Identifier: SHA-1 hash of the TACC Root CA
    - CRL distribution points

7.1.1 Version Number(s)

The TACC Classic CA issues only X.509 version 3 certificates (i.e., the version number shall be 2).

7.1.2 Certificate Extensions

For natural person certificates:

- **basicConstraints**: critical, CA: false;
- **keyUsage**: digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment, critical
- Subject Key Identifier: SHA-1 hash
- Authority Key Identifier: SHA-1 hash of the TACC Root CA
- Subject Alternative Name: person's email address
- Extended Key Usage: clientAuth, emailProtection
- CRL Distribution Points: http://www.tacc.utexas.edu/CA/TACC_Classic_CRL.der
- Certificate Policy Identifiers: The OID of the TACC Classic CA CP/CPS and the OID of the IGTF Classic Authentication Profile.

For host/services certificates:

- **basicConstraints**: critical, CA: false
- **keyUsage**: critical, digitalSignature, KeyEncipherment, dataEncipherment
- Subject Key Identifier: SHA-1 hash
- Authority Key Identifier: SHA-1 hash of the TACC Root CA
- Subject Alternative Name: FQDN of host or server
- Extended Key Usage: serverAuth, clientAuth
- CRL Distribution Points: http://www.tacc.utexas.edu/CA/CRL/Classic_CRL.der
- Certificate Policy Identifiers: The OID of the TACC Classic CA CP/CPS and the OID of the IGTF Classic Authentication Profile.

7.1.3 Algorithm Object Identifiers

The TACC Classic CA will use SHA1.

- hash function: id-sha 1 1.3.14.3.2.26
- encryption: rsaEncryption 1.2.840.113549.1.1.1
- signature: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name Forms

Each entity has a unique and unambiguous Distinguished Name (DN) in all the

certificates issued to the same entity by the TACC Classic CA. The DN shall be structured as defined in ITU-T Standards Recommendation X.501

TACC prefers that organizations use domain component naming.

7.1.5 Name Constraints

There are no other name constraints than those that are to be derived from the stipulations in Sections 7.1.4, 3.1.2 and 3.1.1.

7.1.6 Certificate Policy Object Identifier

1.3.6.1.4.1.17940.5.2.1.1.2

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

The TACC Classic CA will issue an X.509v2 CRL that is compliant with RFC5280. Message digests of CRLs must be generated by SHA1.

- hash function: id-sha 1 1.3.14.3.2.26
- encryption: rsaEncryption 1.2.840.113549.1.1.1
- signature: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.2.1 Version Number(s)

The TACC Classic CA will create and publish X.509 version 2 CRLs that conform to the Internet PKI profile (PKIX) for X.509 Certificate Revocation Lists as defined by RFC5280.

7.2.2 CRL and CRL Entry Extensions

The TACC Classic CA shall issue complete CRLs for all revoked long-term certificates for hosts and servers or services. The reason for the revocation shall not be included in the individual CRL entries.

The CRL must include its validity date. The next CRL must be issued at least one hour prior to that expiration date, even if the list does not have changes. TACC issues a new CRL every hour but each CRL has “NextUpdate” set to seven days. In this way, CRLs are constantly refreshed but still expire after 7 days.

The CRL extensions shall include the CRL number.

7.3 OCSP Profile

Not yet supported.

7.3.1 Version Number(s)

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The TACC Classic CA shall perform a self-assessment once each year as an adjunct to required UT-Austin Information Security Office Risk Assessment (ISORA) survey in order to check operation compliance with the CP/CPS document in effect.

The TACC Classic CA shall annually assess compliance of each designated LRA with registration procedures specified in the CP/CPS document in effect.

In the event of a security compromise, it may become necessary to audit certificate activity compliance. In addition, the accreditation authority may request a compliance audit at any time. The TACC Classic CA will respond promptly to any audit request made by the TAGPMA, and will minimally conduct an annual check and training exercise of its audit capabilities.

8.2 Identity/qualifications of Assessor

Either internal or external assessors will be used. Assessors must be knowledgeable in CA operation and grid system administration.

8.3 Assessor's Relationship to Assessed Entity

TACC Security Officers or members of the TACC grid community can perform internal assessments.

Personnel from TAGPMA, U.S. or Texas government departments, or academic institutions can perform external assessments.

If other trusted CAs or relying parties request an external assessment, the costs of that assessment must be paid by the requesting party, except for the costs of TACC Classic CA personnel and infrastructure.

8.4 Topics Covered by Assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 Actions Taken as a Result of Deficiency

In case of a deficiency, a TACC Security Officer will announce the steps that will be taken to remedy the deficiency. This announcement will include a timetable.

If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

8.6 Communication of Results

TACC Security Officers will make the audit result publicly available on the CA web site with as many details of any deficiency as considered necessary.

9 OTHER BUSINESS AND LEGAL MATTERS

The section headers in section 9 are taken from RFC3647 and are kept as-is for ease of reference and comparison with other CAs. They must not be interpreted or construed in any way that will affect the interpretation or construction of the contents of the sections.

Certificates and all other components of the CA must be used for lawful purposes only.

CA Managers shall sign a document to the effect that they will comply with the procedures and requirements described in this document.

9.1 Fees

The TACC Classic CA charges no fees for its services.

9.1.1 Certificate Issuance or Renewal Fees

Not applicable.

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 *Revocation or Status Information Access Fees*

Not applicable.

9.1.4 Fees for Other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

No financial responsibility is accepted for certificates issued under this policy.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 *Insurance or Warranty Coverage for End-entities*

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 *Scope of Confidential Information*

No stipulation.

9.3.2 Information Not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

The TACC Classic CA will follow best practices to protect any confidential information as well as policies as specified by the University of Texas.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

The TACC Classic CA collects a subscriber's name, work telephone numbers and e-mail address. Additional information may be collected if it is presented to the TACC Registration Agent web application. Additional information is also collected about RA personnel to substantiate their authority. The TACC Classic CA keeps personal information (work telephone number, work address) only to be able to contact subscribers and RAs. Personal information is treated as confidential and only stored within the secured TACC Accounting System (TAS).

Under no circumstances will the TACC Classic CA have access or ability to use the private keys of any subscriber to whom it issues a certificate.

9.4.3 Information Not Deemed Private

Information included in issued certificates and CRLs is not considered confidential.

9.4.4 Responsibility to Protect Private Information

TACC designated LRAs must protect private data collected as part of the face-to-face identity vetting process.

9.4.5 Notice and Consent to Use Private Information

The TACC Certificate Acceptable Usage Policy [Appendix A] describes the collection and archival of private information necessary to check subscriber identity.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Any data request must be reviewed and approved by the UT-Austin legal department prior to data release.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights (IPR)

The TACC Classic CA does not claim any IPR on certificates that it has issued.

Parts of this document are inspired or even copied (in no particular order) from the UFF Brazilian Grid CA CP/CPS, UNAMgrid, AUSTRALIAGRID, CERN, CNRS, the German Grid, UK e-Science, pkIRISGrid CA, ESnet Root CA CP/CPS, DOEGrids CP/CPS and may also be taken indirectly from documents they draw from.

Anybody may freely copy from any version of the TACC Classic CA's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of the sources.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The TACC Classic CA guarantees to issue certificates only to subscribers identified by requests received from designated LRAs for participating grids and VOs via secure routes. The TACC Classic CA will revoke a certificate only in response to an authenticated request from the subscriber, or the designated LRA who approved the subscriber's request, or if it has itself reasonable proof that circumstances for revocation are fulfilled.

The TACC Classic CA does not warrant its procedures, does not take responsibility for problems arising from its operation or the use made of the certificates it provides and gives no guarantees about the security or suitability of the service.

The TACC Classic CA only guarantees to verify subscriber's identities according to procedures described in this document.

The TACC Classic CA does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted.

9.6.2 LRA Representations and Warranties

All designated LRAs shall perform their task of identification of the requesting parties as described in 3.2.3 and 3.2.2 to the best of their knowledge. No other warranties are accepted.

An LRA can conclude, strictly at his/her own risk, a more stringent agreement with his or her subscribers, but this shall never commit the TACC Classic CA nor any of its other designated LRAs.

It is the LRA's responsibility to request revocation of a certificate if the LRA is aware that circumstances for revocation are satisfied.

9.6.3 Subscriber Representations and Warranties

By requesting a TACC Classic CA certificate a subscriber commits to use and protect the certificate and the certified keys according to the stipulations of the CP/CPS document in effect at the date of issuance of the said certificate. (S)he may however apply more stringent observances.

Subscribers must:

- Adhere to the procedures published in this document
- Use the certificate for the permitted purposes only
- Authorize the processing and conservation of personal data (as required under applicable Texas law)
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:
- Select a Strong Passphrase of 12 characters or more;
- Protect the passphrase from others;
- Notify immediately the TACC Classic CA and any relying parties if the private key is lost or compromised;
- Request revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.

In case of a breach of stipulations of the CP/CPS document that the subscriber has agreed to by requesting the TACC Classic CA certificate the certificate shall be revoked immediately. No further warranties are required from the subscriber.

9.6.4 Relying Party Representations and Warranties

A relying party should accept the subscriber's certificate for authentication purposes if:

- The relying party is familiar with the CA's CP and the CPS that generated the certificate before drawing any conclusion on trust of the subscriber's certificate;

- The reliance is reasonable and in good faith in light of all circumstances known to the relying party at the time of reliance; and
- The certificate is used for permitted purposes only; and
- The relying party checked the status of the certificate to their own satisfaction prior to reliance.

9.6.5 Representations and Warranties of other Participants

No stipulation.

9.7 Disclaimers of Warranties

The TACC Classic CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness

The TACC Classic CA cannot be held responsible for any misuse of its certificate by:

- A subscriber
- Any other party who came into possession of the corresponding private key.

The TACC Classic CA cannot be held responsible for unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

9.8 Limitations of Liability

Except if explicitly dictated otherwise by U.S. or Texas law the TACC Classic CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.

The TACC Classic CA also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the designated LRA acting in conformance with this CP/CPS.

9.9 Indemnities

The TACC Classic CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.

End entities shall indemnify and hold harmless the TACC Classic CA and all designated LRAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate that violates the provisions of this CP/CPS document.

9.10 Term and Termination

Term is 5 years and may be renewable.

9.10.1 Term

Start date: 2008

End date: 2013

This policy becomes effective on its approval by the TAGPMA.

9.10.2 Termination

This CP/CPS remains effective until it is superseded by a newer version.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications with Participants

All communications between the TACC Classic CA and a designated third-party identity management system must be bi-directionally authenticated over a secure (SSL/TLS) channel.

All agreements between the TACC Classic CA and an organization must be documented and signed by the appropriate authorities.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

9.12.2 Notification Mechanism and Period

The amended CP/CPS document shall be published on the TACC Classic CA Web pages at least 2 weeks before it becomes effective.

The TACC Classic CA will inform its subscribers and all relying parties it knows of by means of e-mail.

9.12.3 Circumstances under which OID must be Changed

Any substantial change of policy will incur a change of OID.

9.13 Dispute resolution provisions

TACC Security Officers shall resolve any disputes arising out of the CP/CPS.

9.14 Governing Law

The TACC Classic CA and its operation are subject to U.S. law and laws of the State of Texas and must comply with business practice memos of the University of Texas.

9.15 Compliance with Applicable Law

All activities relating to the request, issuance, use or acceptance of a TACC Classic CA certificate must comply with U.S. law and the laws of the State of Texas.

Activities initiated from or destined for another country than the U.S. must also comply with that country's law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP/CPS document supersedes any prior agreements, written or oral, between the parties covered by this present document.

9.16.2 Assignment

No provisions.

9.16.3 Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, that clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

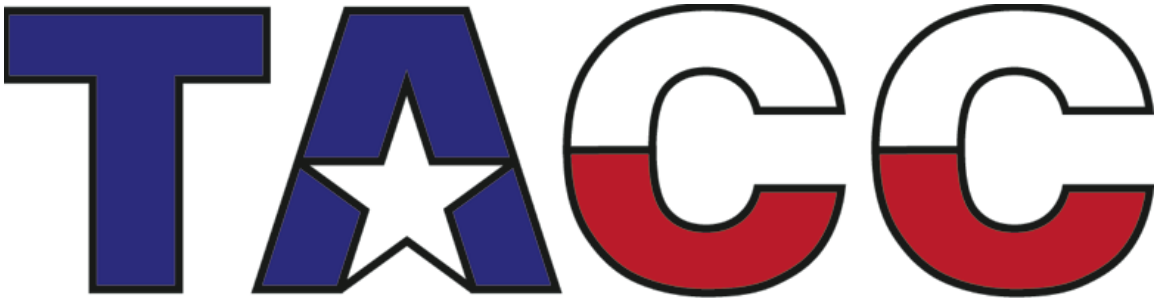
9.16.5 Force Majeure (Acts of God)

Events that are outside the control of the TACC Classic CA will be dealt with immediately by the TAGPMA.

9.17 Other provisions

No stipulation.

Appendix A: TACC Certificate Acceptable Usage Policy



Texas Advanced Computing Center (TACC) PKI

Document Name	**TACC Certificate Acceptable Usage Policy Form**
Current Version	**1.1**
Date last updated	25 January 2009

Abstract:
This document describes the acceptable use policies, user agreements and responsibilities governing GRID access by users having TACC issued X.509 certificate identity credentials.

Change History

V1.0	12Jan09	Initial	Created based on TIGRE User Agreement and Responsibility Form
V1.1	25Jan09	Revised	Add key protections. Fix formatting.

Introduction

Each user (hereafter, "you") requesting services on TACC or IGTF academic grid resources, hereinafter referred to as the GRID, must abide by a common set of basic rules. This document lists those basic rules.

User Agreement

GRID computing facilities, which include its hardware, software, network connections and data, comprise a vital but limited resource for the academic community. For this reason, GRID sites have an obligation to protect those facilities and ensure they are used properly. Responsible conduct on your part helps ensure that the maximum amount of CPU time is available to you and other researchers. Failure to use these resources properly may result in various penalties, including civil and criminal action.

Your signature on this form implies that you have read and understand all responsibilities stated here. If you have any questions about this document, please contact a designated TACC Registration Authority (RA) to discuss the issues. When satisfied, sign and return this form to enable or continue use of your access to resources through your TACC CA certificate.

To run applications across GRID facilities, you must register your X.509 user certificate from a TACC Certificate Authority or equivalent IGTF-approved grid credential,with the GRID central services or middleware. You must also become familiar with the terms for protection and use of the private key associated with your user certificate. By registering with a TACC CA, or by executing a similar agreement with a cooperating party, you shall be deemed to accept the following conditions of use:

Acceptable Use Policy

1. Only use GRID resources to perform work, or transmit or store data consistent with academic research sponsored by your institution or organization and in compliance with resource usage conditions.
2. Refrain from the following unacceptable activities:
    - Using, or attempting to use, GRID resources without authorization or for purposes other than those related to your sponsored research.
    - Tampering with or obstructing the operation of the facilities
    - Reading, changing, distributing, or copying others' data or software without authorization
    - Using GRID resources to attempt to gain unauthorized access to other (non-GRID) sites
    - Activities in violation of local or federal law
3. Immediately report any known or suspected security breach or misuse of GRID resources, or any misuse of your registered TACC credentials to contacts listed below. Request certificate revocation by notifying your RA, the TACC Classic CA and any relying parties immediately:
    - If the private key is lost, destroyed or compromised;

- If the subscriber is no longer entitled to a certificate, or;
- If the information in the certificate is no longer correct or is inaccurate.

4. Use GRID resources at your own risk. There is no guarantee that GRID resources will be available at any time or that they will suit any purpose. Services are provided on a best-effort basis, subject to planned and emergency maintenance outages.
5. Ensure the confidentiality of any intellectual property or other confidential data used on GRID resources. GRID sites provide technology to preserve the confidentiality of data, but it is your responsibility to use that technology appropriately.
6. Appropriately acquire and use all software used on GRID systems according to the specified licensing. Possession or use of illegally copied software or unauthorized distribution of copyrighted software or materials is prohibited and subject to penalties.
7. Recognize that access to GRID resources is explicitly governed by the existing policies of the institution through which you gain such access, as well as the existing usage policies of the resources accessed through grid methods.
8. Take every precaution to prevent any loss, disclosure or unauthorized access or use of certificate key materials:
   - Generate a key pair using a trustworthy method;
   - Select a strong passphrase with a minimum of 12 characters; and
   - Protect the passphrase from others, in the case of user certificates.
9. Authorize the processing and conservation of the personal data required for the request verification process (as required under applicable data protection regulations such as UT-System Information Resources Use and Security Policy (UTS 165).

Disclaimers and Notifications

- Logged information: Information provided by you for registration purposes, shall be used only for administrative, operational, accounting, monitoring and security purposes. This information may be disclosed to other organizations anywhere in the world for these purposes. Although administrative best practices serve to maintain personal information confidentiality, no guarantees are given.
- Support/Diagnostic Access: Authorized TACC CA site personnel may review files for the purposes of aiding an individual or providing diagnostic investigation for GRID systems.
- Monitoring: User activity may be monitored as allowed under policy and law for the protection of data and resources. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site or law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such at the discretion of authorized site personnel.
- Access Notification: Access to user data and communications will not normally be performed without explicit authorization and/or advance notice unless exigent circumstances exist. Post-incident notification will be provided in such cases.

Penalties

Failure to abide by this agreement may result in one or more of a variety of penalties imposed, as described below:

- Account Suspension/Revocation: Accounts may be temporarily suspended or permanently revoked if compromised or abused. Your account on any GRID resource may be suspended without advance notice if there is suspicion of account compromise, system compromise, or malicious or illegal activity.
- Loss of Allocation: You may lose your current allocation and possibly the ability to obtain future allocations.
- Administrative Action: Abusive activity may be reported to your home institution for administrative review and action.
- Civil Penalties: Civil remedies may be pursued to recoup costs incurred from unauthorized use of resources or incident response due to compromise or malicious activity.
- Criminal Penalties: Activities in violation of federal, state, or local law may be reported to the appropriate authorities for investigation and prosecution.

Security and administrative contacts

Report all suspicious activity to abuse@tacc.utexas.edu. All questions regarding certificate support issues and TACC CA administrative practices can be directed to ca@tacc.utexas.edu.

Acceptance statement

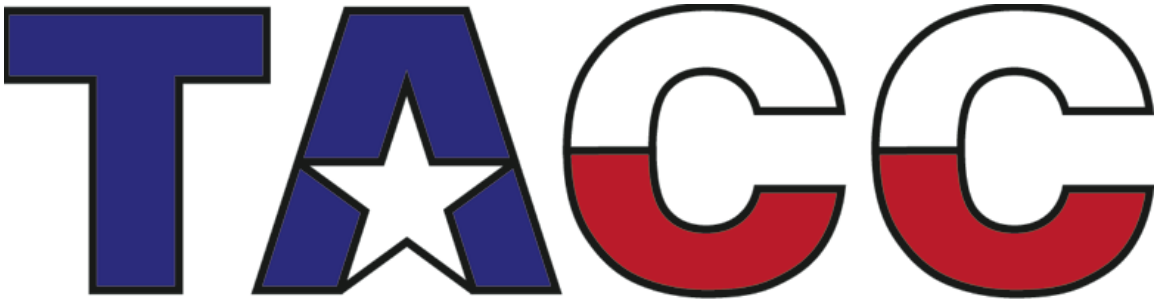
The undersigned acknowledges that s/he has read this TACC Certificate Acceptable Usage Policy Form and understands the enclosed information. The undersigned also acknowledges that s/he will abide by the stated policies and procedures to the best of his/her ability. The undersigned is also under obligation to abide by any future changes to the TACC Certificate Acceptable Usage Policy or surrender access to the GRID. All users will be notified when changes are made to this Form. The undersigned also understands that access to GRID will be terminated upon any change to user affiliation or status that removes eligibility for GRID use.

The current TACC Certificate Acceptable Usage Policy can also be found on the TACC web site in both HTML and PDF formats at the link below:

http://www.tacc.utexas.edu/CA/TACC_certificate_AUP.pdf

Name:_____
Daytime Phone#:_____
Institution:_____
E-Mail:_____
Academic status:_____
Signature:_____
Date Signed:_____

Appendix B: TACC Request for Local Registration Agent (LRA) Designation



Texas Advanced Computing Center (TACC) PKI

Document Name	**Request for TACC Local Registration Agent (LRA) Designation**
Current Version	**1.1**
Date last updated	25 January 2009

Abstract:
This document provides a template for an organization to request establishment of a remote Local Registration Agent (LRA) for a TACC Certificate Authority (CA).

Change History

V1.0	12Jan09	Initial	Created.
V1.1	25Jan09	Revised	Clarify LRA from RA.

{Organization Letterhead}

TACC Root CA Security Officer
Texas Advanced Computing Center
10100 Burnet Rd. (R8700)
Austin, TX 78758-4497 USA
{Date}

Dear Reader,
This letter authorizes and documents a request for:
{Name, Position in organization} {mailing address} {email} {phone} {fax}
to represent {Name of organization} as a designated Local Registration Agent (LRA) for the TACC CA. {Name} is authorized to perform the following RA functions for members of our organization starting on {Date}:

1. Record and archive:
    - A verified CN, organization, email, phone number and address of the requester from the official published phone directory maintained by the academic or research organization or government lab. Alternately, a letter of introduction from an official organization authority will be accepted.
    - In-person or remote video verification or government documents with picture that confirm the user is who s/he says s/he is;
    - The document(s) used as proof of relationship with the organization or organizational unit;
    - An LRA assessed level-of-assurance (LoA) of the identity presented by an organization.
    - The date, time and place of the authentication;
    - Whether the authentication was successful or not and why.
2. Facilitate submission of a TACC Certificate Submission Request (CSR)
3. Request TACC certificate revocation if:
    - A user's private key is lost, compromised, or corrupted
    - A user having a TACC certificate is no longer affiliated with our organization

Sincerely,

{Name, Position in organization}