TACC ROOT CA
CERTIFICATE POLICY
AND
CERTIFICATE PRACTICES STATEMENT

(In RFC 3647 format)
January 20, 2009
OID: 1.3.6.1.4.1.17940.5.1.1.1
Version 1.2

---

1 INTRODUCTION

The Texas Advanced Computing Center (TACC) operates a Certification Authority called the TACC Root Certificate Authority (CA) to issue CA certificates for distributed and grid computing communities who run scientific applications requiring Public Key Infrastructure (PKI) services. TACC operates its PKI infrastructure for two purposes:

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

This document describes the set of rules and procedures established by the TACC CA Policy Management Authority for the operation of the TACC Root CA PKI service. The TACC Root CA signs only CA certificates.

Structured according to RFC 3647 [RFC3647], this document describes policy and practices of TACC 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 the 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 Root CA.

1.1 Overview

The TACC CA infrastructure supports grid and e-science activities provided by the **Texas Advanced Computing Center (TACC)**. This document describes the set of rules and procedures established by TACC for the operations of the TACC Root CA service. The purpose of the TACC Root CA is:

- To define and limit the community that Subordinate CAs may serve;
- To ensure that Subordinate CAs with different assurance levels and purposes can coexist;
- To enable Subordinate CAs to be maintained in adequately protected networked

systems, according to their policy and purpose.

1.2 Document Name and Identification

This document is the CP and CPS of the TACC Root CA.

Document title:	**TACC Root CA Certificate Policy and Certification Practice Statement**
Document version:	**1.2**
Document date:	**January 20, 2009**
OID:	1.3.6.1.4.1.17940.5.1.1 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) ut-austin(17940) tacc(5) rootca(1) cps(1) version 1}

1.3 PKI Participants

- Certificate Authorities: The TACC Root CA only issues CA certificates.
- Registration Authorities: There are no RAs external to the issuing authority. TACC alone (the issuing authority) is responsible for all approvals and revocations.
- Subscribers: Only Subject CAs receive certificates from the Root.
- Relying Parties: No stipulation.

1.4 Certificate Usage

The TACC Root certificate may be used for the following purposes:

- To validate the signature of a Subject CA
- More generally, to validate any certificate chain ending with this Root, provided all certificates in the chain are used for permitted purposes
- To validate the signature on a CRL issued by this Root.

No other use of the TACC Root certificate is permitted.

The TACC Root asserts that all Subordinate CAs serve the same community and they all issue in distinct namespaces.

1.5 Policy Administration

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

The person responsible for this policy and the practices of the CA is:

Margaret Murray, Ph.D.
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
Email: ca@tacc.utexas.edu.

1.6 Definitions and Acronyms

- **TACC** is the Texas Advanced Computing Center, located on the J.J. Pickle Research Campus of the University of Texas at Austin, TX.
- For the purposes of this document, a **Subject CA** is a CA whose certificate was issued by the Root whose policy and practices are described in this document.
- For the purposes of this document, a **Subordinate CA** is a Subject CA in a hierarchy whose root is described in this document.
- For the purposes of this document, **Profile** refers to the content of the signed envelope within a certificate, but excluding the public key itself and the lifetime. Thus, Profile normally comprises extensions, the issuer and subject names, but also the type of keys and algorithms, and the version of the certificate.
- **HSM** is a hardware security module.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

It is the responsibility of the TACC Root CA to publish the following information at http://www.tacc.utexas.edu/CA/:

- Its CP/CPS;
- Its certificate;
- All certificates issued by the TACC Root CA and their status;
- The signing policy of the hierarchy of which it forms the root;
- Its Certificate Revocation List (CRL)

As a member of the TAGPMA, the TACC Root CA grants the IGTF and its PMAs the right of unlimited redistribution of this information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

- Each of the Subject CAs shall have a unique name;
- Its Subject DN shall form the Subject name of each Subject CA to relate its purpose and distinguish it from others alone.
- The Issuer name shall be: /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN /CN=**TACC Root CA**
- No subject name of a Subject CA shall be reused anywhere in the hierarchy.
- Subject CA 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 as follows:

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

3.2 Initial Identity Validation

A certificate shall be issued to a Subject CA only when:

- The Subject CA has defined a CP and CPS consistent with the policy and practices described in this document;
- The Subject CA has implemented and described policy and practices sufficient to meet the restrictions that this document imposes on Subject
- The Subject CA has submitted a certificate request and is able to prove to the Root CA possession of the corresponding private key.

Furthermore, the TACC Root CA requires, as a condition for certificate issuance, that:

- All Subject CAs make available to the TACC Root CA results of CA audits and plans to remedy deficiencies
- All Subject CA Managers and Operators agree to be signed up to a closed mailing list, maintained by the TACC Root CA;
- The Subject CA's certificate request (and hence certificate) contains no personal information.

3.3 Identification and Authentication for Re-key Requests

TACC Security Officers who manage the Subject CA shall prove possession of the private key corresponding to the certificate being renewed, and prove possession of the private key corresponding to the request being submitted.

3.4 Identification and Authentication for Revocation Request

The certificate of a Subject CA will be revoked when:

- A revocation request is received which is signed with the private key of the Subject CA; or,
- An authenticated revocation request from the CA Manager of the Subject CA is received; or,
- The TACC Root CA has otherwise determined the need for revocation, e.g., if the Subject CA does not comply with the requirements imposed on it by the TACC Root.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

For both the TACC Root CA and Subject CAs, keys shall be generated by the HSM. The private key shall be protected within that HSM and managed according to the documented practices of the CA.

The Subject CA shall have a lifetime not to exceed five years. The TACC Root CA's certificate shall have a lifetime of ten years.

4.1 Certificate Application

For an initial request, the Manager of the Subject CA shall agree to the namespace of the Subject CA with the Manager of the TACC Root CA, and shall submit a CP/CPS under which the Subject CA will operate. It is the responsibility of the Manager of the Subject CA to ensure that it operates within the constraints imposed by the Policy of the Root.

All TACC Root and Subject CAs operate within a FIPS 140 Level 3 Hardware Security Module (HSM) that protects Root and Subject CA private keys and supports PKCS #11 processing as follows:

1. The TACC Root CA Manager uses the Administrative Security Officer PIN that controls the entire HSM to:
    a. Create a dedicated slot for a requested Subject CA using the HSM whole device Administrator PIN.
    b. Initialize a token and set an initial Administrator PIN for use by the designated Subject CA Operator to control that dedicated, labeled slot.
2. The Subject CA Operator (who may or may not be the same as the TACC Root CA Manager) logs into the dedicated Subject CA slot using its Administrator PIN to:
    a. Change the Slot Administrator PIN (if the CA Operator is different from the TACC Root CA Manager).
    b. Create a User PIN to protect access and use of objects stored in this dedicated token on this dedicated slot.
    c. Create a private key object that resides only in the HSM's Subject CA token.
    d. Use OpenSSL to create a Subject CA Certificate Service Request (CSR) that uses the private key resident on the HSM.

4.2 Certificate application processing

When the TACC Root CA Manager is satisfied that Subject CA will operate within the constraints imposed by the Root, The TACC Root CA will issue and publish the certificate of the Subject CA.

4.3 Certificate issuance

The TACC Root CA Manager makes the Subject CA available on its website.

4.4 Certificate acceptance

Both the TACC Root CA Manager and the TACC Subject CA Manager shall verify the content of the Subject CA certificate against the CP/CPS of the Subject CA and test its use (e.g. against grid middleware). If problems are discovered during testing, the certificate shall be revoked by the TACC Root CA, and reissued with changes, provided that these changes are still compatible with the CP/CPSes of both the TACC Root and Subject CAs.

4.5 Key pair and certificate usage

The certificates of all Subordinate CAs and those of the EEs issued by Subordinate CAs must be used only for purposes of direct academic science and grid work, or related incidental support (i.e. infrastructure, email).

The certificates issued to Subject CAs may only be used as CA certificates, i.e., for validating certificates issued by them, and for validating CRLs.

A Subordinate CA may impose further constraints on the use of certificates on, and only on, their EEs. Conversely, no Subordinate CA shall relax constraints imposed on its policy or operations by the CP/CPS of a CA of which it is itself Subordinate.

It is the responsibility of the EE to use certificates for permitted purposes only. It is the responsibility of RPs to validate the certificate to their satisfaction at the time of reliance.

4.6 Certificate Renewal

No Subject CA certificate shall be renewed except for the reissuance associated with the non-acceptance of an issued certificate.

4.7 Certificate Re-Key

It is the responsibility of the CA Manager of each Subject CA to ensure that a timely rekeying of the Subject CA certificate is requested. The Manager shall further take into account time required for the Root to perform any necessary validations of the Subject CA, operational requirements (Root operator availability and schedule), and the time permitted to the Manager to validate acceptance of the certificate, and certificate redistribution to repositories and RPs.

It is the Manager's responsibility to ensure that this process is complete within a time interval not less than the maximal lifetime of certificates directly issued by the Subject CA before the date of expiry of the Subject CA certificate. The lifetime of the rekeyed Subject CA certificate shall not exceed that of the Root. It is the responsibility of the CA Manager of the Root CA to ensure that a timely rollover of the Root certificate is in place. To this end, the Root shall require that no Subject CA has a lifetime longer than five years.

The process for acceptance of a rekeyed Subject CA certificate is the same as for the acceptance of an initial request – see section 4.4.

4.8 Certificate modification

A TACC Security Officer may request certificate modification. Provided it is consistent with the policy and practices of the Root, the Root shall:

- Reissue the certificate with the requested modifications, provided a timely request is made due to non-acceptance of an issued certificate;
- Issue and re-publish the certificate with the requested modifications based on a

new certificate request, as for rekey.

Only in exceptional circumstances will the Root otherwise reissue the certificate with the same keys. A TACC Security Officer shall describe:

- The need for the modification of the existing certificate;
- Justify the urgency requiring a modified certificate containing the same keys;
- The means by which the modified certificate shall be published and redistributed;
- Compatibility: that the modification will not impair the usability of the certificate with existing middleware and infrastructure, except to the extent that such impairment is the intention of the modification.

These exceptional circumstances include, but are not limited to:

- Vulnerabilities of cryptographic algorithms used in the certificate are discovered, and a compatible security update is available;
- Exceptional circumstances (force majeure) beyond the control of the TACC Security Office has prevented a timely rekeying request, thus requiring a temporary, limited extension of the lifetime of the certificate.

4.9 Certificate Revocation and Suspension

A Subject key CA shall be revoked if:

- It is seen to consistently and willfully violate its own CP/CPS, or that the CA Manager of the Subject CA does not take steps to address such
- It is seen to violate requirements imposed on it by the policy and practices of the Root; or
- It can be shown that the private key has been compromised.

4.10 Certificate Status Services

The Root CA shall issue a CRL. Certificates and certificate status of Subject CAs are available on the Root CA's web site. See also section 7.2.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

The TACC Root CA and Subject CA keys shall be encrypted using a separate, PIN-protected wrapping key and then backed up to a Smart Card using HSM management utilities. HSM recovery of keys to their labeled slots and tokens conversely requires PIN entry in response to HSM management utilities.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

5.1 Physical Security Controls

The machine on which the Root signs its certificates and CRLs is implemented on a machine dedicated to CA processing in the locked Security rack in the access-controlled TACC computer room.

5.2 Procedural Controls

Only TACC CA Managers may access the locked rack, the safe or any servers located inside the locked rack. One TACC or CA Manager may physically access materials and machines within the locked rack, but s/he must have another TACC CA Manager or Advanced Computing Systems (ACS) staff check and log task status.

5.3 Personnel Controls

Training: The Root CA is OpenSSL based, and TACC CA Managers must have sufficient experience with OpenSSL to be able to issue certificates and CRLs. TACC CA Managers must be permanent University of Texas at Austin staff.

5.4 Audit logging Procedures

All OpenSSL operations and basic system logs for the signing machine will be saved in files that are periodically signed and written to CDROM. Logs can be copied and emailed upon request.

5.5 Records Archival

Records are kept throughout the lifetime of the CA and for a period no less than three years after the termination of the CA.

5.6 Key Changeover

At re-keying, the new Root public keys shall be published on the Root CA's web site, as certificates signed by both the old and the new private key. The transitional certificate, signed with the old key, shall expire at the same time as the old Root certificate, but shall otherwise have the same content as the new Root certificate. It shall be clearly marked as a transitional certificate, and instructions shall be provided for users explaining how to verify the transition.

5.7 Compromise and Disaster Recovery

Following any compromise of the Root private key, The Root CA shall make this widely known to all peer CAs, Subject CAs and relying parties. Efforts to re-issue new Subject CA certificates will follow the method described in section 5.6.

5.8 CA or RA termination

Upon termination of the Root CA, a TACC CA Manager shall communicate this in advance to peer CAs, Subject CAs and relying parties. The advance notice should be no less than the longest lifetime of any currently valid Subject CA.

6 TECHNICAL SECURITY CONTROLS

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

6.1 Key Pair Generation and Installation

The Root CA's key pair shall be generated with sufficient entropy by the FIPS 140 Level 3 device. It shall be the responsibility of a TACC CA Manager to generate the key pair. The Root key pair shall be RSA and have a length of at least 2048 bits. Key pairs for Subject CAs are generated according to best practices. Each Subject CA key pair should have a length of at least 2048 bits.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The private key of the Root CA shall be protected on the tamper-proof FIPS 140 Level 3 device. The passphrase is typed in as needed, or is accessed by scripts via the OpenSSL standard input method.

Additionally, multiple encrypted backups of HSM private key shall be kept on Smart Cards in tamper evident envelopes. At least one envelope shall be stored in the US GSA-rated safe located inside the locked TACC Security rack. At least one envelope shall be securely stored with TACC Data Steward who is subject to annual security audit by the University of Texas at Austin.

Each copy shall be checked for integrity at least once every year.

6.3 Other Aspects of Key Pair Management

All Root CA certificates shall be kept and published throughout the lifetime of the CA, and a period no less than three years after the termination of the CA.

Subject CAs' key pairs shall have a lifetime not to exceed five years.

6.4 Activation Data

The activation data (PINs for use with the FIPS 140 Level 3 device) shall be chosen such that according to current cryptographic practice, estimates, and recommendations, recovering the key from its encrypted form is at least as hard as recovering it from the public key. Separate PINs shall be assigned to different CAs.

6.5 Computer Security Controls

Only TACC Security Officers and CA Managers may access the dedicated TACC CA server containing the FIPS 140 Level 3 device.

6.6 Life Cycle Technical Controls

Only TACC Security Officers or CA Managers may perform hardware maintenance or upgrade software on the dedicated TACC CA server.

6.7 Network Security Controls

The TACC Root 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

The CA server shall synchronize its machine clock to the TACC ntp server. In addition, the TACC Root CA Manager shall periodically check event log timestamps on the FIPS 140 Level 3 device for accuracy, adjusting that device's internal real-time clock only if needed.

7 CERTIFICATE, CRL, AND OCSP PROFILES

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

7.1 Certificate profile

All certificates issued by the TACC Root CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280 [RFC3280].

The Root CA shall have the following Profile:

- The certificate shall be version 3 (i.e., the version number shall be 2);
- The issuer and subject name shall both be the following: /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN /CN=**TACC Root CA**
- The signature algorithm shall be **sha1WithRSAEncryption;**
- The extensions shall contain:
    - **basicConstraints:** CA=true, critical;
    - **keyUsage:** certificate signing, CRL signing, critical;
    - There shall be a **subjectKeyIdentifier** and an **authorityKeyIdentifier**; both shall have the hash as a value;
    - CRL distribution points

The requirements on the Profile of the Subject CAs are as follows:

- The certificate shall be version 3 (i.e., the version number shall be 2);
- **basicConstraints** must be present and critical and must contain CA=true, (but may contain other constraints);
- **keyUsage** must be present and critical and must have certificate signing and CRL signing set, and no other value;
- There shall be a **subjectKeyIdentifier** and an **authorityKeyIdentifier** both containing the hash.
- Other extensions are allowed.

7.2 CRL Profile

The Root CA issues CRL version 2 (i.e., the version number shall be 1). The "lifetime" of the CRL is 18 months and it is issued at least once every year.

7.3 OCSP Profile

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A TACC Security Officer shall carry out a compliance audit of the Root CA once every year. The audit shall inspect the logs and check the security of the activation data and the copies of the encrypted private key.

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 Root CA charges no fees for its services.

9.2 Financial Responsibility

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

9.3 Confidentiality of Business Information

The TACC Root 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

The TACC Root CA does not process any personal data, except for the following:

- The email addresses of the TACC Security Officers and CA Managers. These are not published and are used only for announcements pertaining to the Root CA or announcements affecting all Subject CAs.

TACC Root and Subject CAs publish a generic email address to contact TACC Security Officers: ca@tacc.utexas.edu.

9.5 Intellectual Property Rights

This document is based on RFC3647 and its application to the "UK e-Science Root Certificate Policy and Certification Practices Statement" by the UK e-Science CA run by CCLRC. The TACC Root CA does not claim any IPR on certificates that it has issued. Anybody may freely copy from any version of the TACC Root CA's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of these

sources.

9.6 Representations and Warranties

When issuing a certificate to a Subject CA, the TACC Root CA will have evaluated the CP/CPS of the Subject CA and is satisfied that the Subject CA, when operating according to its CP/CPS, complies with the requirements imposed on it by this document.

9.7 Disclaimers of Warranties

TACC makes no representation and gives no warranty, condition or undertaking in relation to the TACC Root CA and its operation.

9.8 Limitations of Liability

With respect of the information published by the Root CA, including, but not limited to certificates and CRLs, the Root CA shall make best endeavors to ensure the information is timely and accurate. TACC shall be under no obligation or liability, and no warranty condition or representation of any kind is made, given or to be implied as to the sufficiency, accuracy or fitness for purpose of such information. The recipient party, whether CA, RP, EE, or anyone else, shall in any case be entirely responsible for the use to which it puts such information.

The TACC Root 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 RA acting in conformance with this CP/CPS.

9.9 Indemnities

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

Each Subject CA and relying party shall indemnify and hold harmless TACC and keep TACC indemnified against any and all damages, costs, claims or expenses, which are awarded against, or suffered by the Subject CA or relying parties or their hosting institution or company, as a result of any act or omission of the relying party or Subject CA.

9.10 Term and Termination

The initial lifetime of the TACC CA is twenty years. The TACC Root CA shall announce its termination widely to subject CAs and major relying parties and PMAs. This announcement should be made five years, or the maximal lifetime of any valid Subject CA certificate, whichever is shorter, prior to actual termination. The TACC Root CA shall issue no certificate whose lifetime will exceed the date of termination and is obligated to maintain its CRL until its termination.

9.11 Individual Notices and Communications with Participants

All agreements between the TACC Root CA and any organization must be documented and signed by the appropriate authorities. A mailing list shall be maintained for announcements pertaining to the TACC Root CA, or announcements affecting all Subject CAs.

9.12 Amendments

The TACC Root CA shall communicate amendments to Subject CAs and to the TAGPMA.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

The TACC Root 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 Root 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

No stipulation.

9.17 Other Provisions

No stipulation.

10 Change Log

Date	Version	Description
20Jan09	1.2	• Section 2: Added CA repository URL and reference to published signing policy • Section 3.1: Added fixed component of Subject CA certificates to clarify and limit namespace.

		• Section 4: Changed Root CA certificate lifetime to 10 years • Section 6.7: Added text to reflect active monitoring. • Removed off-line CA • Added on-line CA • Change signature hash back to SHA1WithRSAEncryption • Included edits appearing in latest CCLRC Root CA CP/CPS • Changed TACC mailing address.
17Sep08	1.1	• Change in Subject DN recommended by TAGPMA reviewers • Change signature hash to SHA256With RSAEncryption
26Nov06	1.0	Original version accredited by TAGPMA.