TACC MICS CA

CERTIFICATE POLICY
AND
CERTIFICATE PRACTICES STATEMENT

(In RFC3647 format)
Version 1.1
12 May 2009
OID: 1.3.6.1.4.1.17940.5.3.1.1

1 INTRODUCTION

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

1. To provision 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 provisioned certificates to be accepted by relying parties of other grid, research and e-science CAs.

The TACC MICS CA relies on and leverages existing Identity Management (IdM) infrastructures to simply and securely generate short-term X.509v3 end entity certificates

to individuals authenticated by those IdMs, starting with the TACC Accounting System (TAS) managed TACC Active Directory service. In addition to managing all user accounts on TACC compute resources, TAS also serves to federate added IdMs by translating identity attributes to perpetually unique DNs.

This document describes the set of rules and procedures established by the TACC CA Policy Management Authority for the operation of the TACC MICS CA PKI service. The TACC MICS CA runs as a subordinate CA under the TACC Root CA

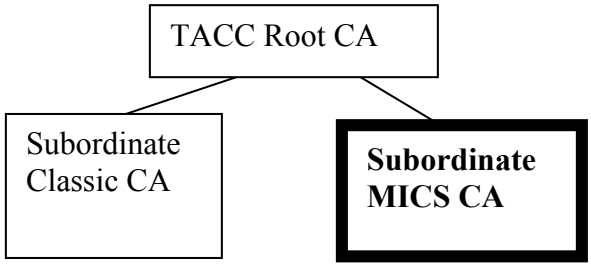
Structured according to RFC3647, this document describes policy and practices of TACC MICS CA PKI services. The Certificate Policy (CP) describes the requirements for operation of the PKI and for granting PKI credentials as well as lifetime management of those credentials. The Certificate Practices Statement (CPS) describes the actual steps that TACC takes to implement 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 MICS CA.

1.1 Overview

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

- Leverage existing IdM infrastructures.
- Simplify user credential acquisition and management.
- Generate short-term X.509v3 end entity certificates for academic science and research users relevant to TACC's campus, state, national and international research projects.

The TACC MICS CA is subordinate to the TACC Root CA and relies on the TACC Root CA to establish its authority. The TACC MICS CA itself signs only short-lived user certificates.



1.2 Document Name and Identification

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

Document title:	**TACC Member Integrated Credential Services (MICS) Grid CA Certificate Policy and Certification Practice Statement**
Document version:	**1.1**

Document date:	**12 May 2009**
OID:	1.3.6.1.4.1.17940.5.3.1.1 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) ut-austin(17940) tacc(5) micsca(3) cps(1) major version (1) minor version (1) }

Whenever there is a change in this CP/CPS, the OID version number shall change. 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 Hardware Security Module (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 MICS 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 MICS CA will issue and manage RFC5280 PKI X.509 v3 short-lived user certificates. The TACC MICS 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 MICS CA operates as a subordinate CA off of the TACC Root CA. All private keys used by the TACC MICS CA are protected in a labeled, isolated partition in the FIPS 140 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 part of each site's IdM infrastructure, specific LRAs may be established via formal agreement with the TACC CA. In all cases selection of LRAs by the TACC Security Officer occurs only after confirmation that the designated individual or IdM has the authority and the ability to identify people, hosts or services within their domain of responsibility.

1.3.3 Subscribers

The TACC MICS 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 college, university, research organization, or collaborative grid or Virtual Organization (VO) defines its specific subscribers. The TACC MICS CA issues short-term RFC5280 PKI X.509 v3 certificates

for users only upon request via a public web interface, communicating with the TACC MICS CA only via a secure (at least SSL3.0 or TLS1.0) network link. The TACC MICS CA recognizes different identity levels of assurance and may include an LoA value in certificate extensions.

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 MICS CA, for the purposes of mutual 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. Short-term Person or User certificates are not suitable for activities such as email signing and encryption, and are also not suitable for legally binding digital signatures on financial or contractual documents. Relying parties may or may not also be subscribers.

1.4 Certificate Usage

Usage of a TACC MICS CA short-lived RFC5280 X.509 v3 end entity user certificate supports application functions digitalSignature, KeyEncipherment, dataEncipherment (See 7.1.2). Applications include but are not limited to login authentication and job submission.

The certificates issued by the TACC MICS CA must not be used for financial transactions. Certificates must be used only for lawful purposes.

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

Margaret Murray, Ph.D.
Texas Advanced Computing Center (TACC)
University of Texas at Austin
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

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 RFC2119.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of Certification Information

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

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

2.3 Time or Frequency of Publication

Public information on the TACC MICS CA website is intended to be current. Documents will be posted as soon as possible or within one working day of any changes or modifications. This CP/CPS will be published whenever it is updated and after approval of the TAGPMA.

The TACC MICS 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 (CDT or CST (GMT-5 or GMT-6) timezone) it may run unattended " at risk". The TACC MICS CA does not impose any access control on its CP/CPS or PKI Disclosure Statement.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The certificate subject names used as unique certificate identifiers obey the GFD125 (http://www.ogf.org/documents/GFD.125.pdf) standard. Subject names have a fixed and a variable component. The certificate subject names start with the fixed component to which a variable component shall be appended.

The fixed component is common to all certificates issued by the TACC MICS CA and is used to identify the namespace that can be signed by this CA. This fixed component is: /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA

Whenever identity information is collected from a remote IdM infrastructure instead of the local TACC Accounting System (TAS), a variable component shall follow the fixed component to indicate the IdM or distributed LRA who vetted the user's identity. For example:

- /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA /O=UT-SYSTEM FEDERATION/OU=UT-ELPASO/
- /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA /O=TAMU CAS/OU=COLLEGE STATION/

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.

All TACC MICS certificates contain a common name (CN). This is a unique variable component that identifies the subject name within the CA namespace. In the event that a new user's presented CN is identical to an existing CN, the TACC Accounting System (TAS) appends the new user's unique TAS record number to that CN.

3.1.3 Anonymity of or Pseudonyms for Subscribers

Anonymity and user pseudonyms are not supported.

3.1.4 Rules for Interpreting Various Name Forms

This Distinguished Name (DN) is based on identity vetting done by the TACC LRA and identity information from the TACC Accounting System (TAS) database:

- /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA /CN=Chris User

The following DN is based on UT-System Shibboleth Federation identity assertions from the UT-ElPaso campus:

- /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA /O=UT-SYSTEM FEDERATION/OU=UT-ELPASO/CN=Nic A. Smith-Jones

The common name (CN) that uniquely identifies the subject name within the CA namespace must follow all variable component organization (O) and organizational unit (OU) pairs. Common names must be encoded as Printable Strings according to RFC1778 and RFC2252. Compound characters shall be represented by their ASCII equivalent. Strings containing up to 128 of the following characters are allowed:

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

3.1.5 Uniqueness of Names

The local TACC Accounting System (TAS) maintains a database of all existing CNs and DNs. TAS maintains CN uniqueness whether it is provided by the TACC RA or collected from a remote IdP and associates a unique record number with every CN. TAS can therefore normalize uniqueness across multiple IdM infrastructures that may have different uniqueness policy requirements. When TAS creates a new CN for any new user, it checks whether a duplicate CN already exists. As binding of a CN to an individual is permanent for the lifetime of the TACC PKI and can be used in both TACC MICS and TACC Classic certificates, TAS will enforce uniqueness by appending the new user's unique TAS record number to the CN. For example:

- /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA /CN=Chris User
- /DC=EDU/DC=UTEXAS/DC=TACC/O=UT-AUSTIN/O=TACC MICS CA /CN=Chris User 525903

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Certificate requests must be digitally signed.

3.2.2 Authentication of Organization Identity

Affiliation of a user with an organization shall be established in one of the following ways:

- Identity assertions made by an organization's IdM via previously agreed upon message exchange protocol
- Manual verification performed by an LRA via search of the organization's public directory and website or organizational email verification or department phone calls.

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 MICS 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 LRA 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 identification against presented government documents with picture that confirm the user is who s/he says s/he is. Alternately, a remote videolink identification may occur against notarized copies of government documents with picture that have been sent via Registered Mail to the LRA.
- 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.
- The date and time when the user accepted the AUP conditions.
- Whether the authentication was successful or not and why.

LRAs include authorized personnel in approved IdM infrastructures as well as designated site personnel for whom a formal TACC MICS CA RA agreement is in place. (See Appendix B.)

Identity assertions made by IdMs to the TACC MICS CA must occur over encrypted SSL/TLS channel according to clearly articulated definitions and methods. (See Appendix C.)

All TACC designated LRAs must use the interface provided by TACC to perform RA functions. Data collection functions during initial identity validation include:

1. Identity Information: Verifiable identity vetting information shall be accessible either from the IdM system or from the TACC Accounting System (TAS).
2. User Contact Info: Sufficient information shall be stored in TAS at initial registration to enable contact with the registered identity owner.

3. 2nd Element Security Info: A user-specific question and answer shall be setup during the initial registration process to enable an optional 2nd authentication element.

If the IdM infrastructure does not provide all three data components, then the missing data must be stored in TAS and will necessitate a one-time initial registration with an LRA. The purpose of data collection is to bind IdM or TAS identity validation to one unique end entity user CN. Unique CNs map to one and only one individual end entity for the life of the TACC PKI.

Information collected during initial identity validation must be treated as private data and stored securely according to UTS165 "Information Resources Use and Security Policy" (see: http://www.utsystem.edu/POLICY/policies/uts165.html).

Results of initial registration will be emailed to the user's contact email address. Thereafter, certificate processing will be automated and will not generate email notification.

3.3 Identification and Authentication for Re-key Requests

Not applicable. TACC MICS EE certificates expire but a user can always request a new short-term EE certificate upon successful re-authentication. The EE certificate subject belongs to one and only one individual for the lifetime of all TACC CAs.

3.4 Identification and Authentication for Revocation Request

If an approved IdM infrastructure no longer validates a user identity, that user can not request a TACC MICS CA certificate. Also, any designated LRA may request revocation given evidence of compromise or exposure of the associated private key.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Any user affiliated with an institution collaborating with TACC who has completed in-person identity vetting with either with a designated LRA or an approved IdM infrastructure may request a short-term X.509 user end-entity certificate after generating a key-pair.

The requesting party generates the key pair with a size of at least 1024 bits on their local system either through an interface provided by the MICS CA or using *openssl* utilities.

4.2 Certificate Application Processing

For initial registration, TACC MICS CA authenticates requests as described in Section 3.2.3. Subsequently, upon successful IdM authentication (either through the TAS

managed TACC Active Directory service or some other Identity Provider), the MICS CA makes an API callout to TAS to fill out the CSR fields. While TAS maintains a publishable form of the DN, technically the DN is generated when the certificate gets created.

In the event that TACC is operating in an elevated security mode, all users will be asked a 2nd element authentication question. After successful authentication, certificate applications are automatically processed.

4.3 Certificate Issuance

Upon successful user authentication, back-end processing begins with acceptance of retrieved user attributes. The TACC MICS CA server shall receive the CSR from the TACC MICS CA interface and create a certificate signed with the private key of the TACC MICS CA. The resulting signed certificate is then returned to the user. Requests for short-term X.509 user end entity certificates are processed automatically from a web application in the order received in close to real-time.

4.4 Certificate Acceptance

Retrieval of a certificate from the TACC MICS CA either by the user or on behalf of the user via portal software is considered acceptance.

4.5 Key pair and certificate usage

Subscribers must protect the private keys corresponding to their X.509 certificates and notify the MICS CA operators of any incident involving possible exposure or theft of a private key.

The TACC-issued certificate may be used for grid transactions. For example, a MICS EE certificate may be presented to authenticate login, file transfers, job submission or SSL/TLS tunnel encryption.

A relying party must check the validity of a certificate issued by the TACC MICS CA by using the TACC MICS CA public key to validate its signature and checking that the certificate has not expired.

4.6 Certificate Renewal

TACC MICS EE certificates do not normally renew. Users who often require certificates lasting longer than 1M seconds should avail themselves of the TACC Classic CA. In contrast, if a specific grid application normally runs jobs that complete within a day or two, but may occasionally expect to run longer jobs, that specific grid application may enable certificate renewal on a per case basis. In all cases, short-term end entity certificates may only be renewed if the user re-authenticates. Upon successful re-authentication, a trusted interface may request a new expiration date for a MICS EE certificate already securely stored, but no more than three times.

4.7 Certificate Re-key

Not applicable. TACC MICS EE certificates expire but a user can always request a new short-term EE certificate upon successful re-authentication. The EE certificate subject belongs to one and only one individual for the lifetime of all TACC CAs.

4.8 Certificate Modification

Not applicable.

4.9 Certificate Revocation and Suspension

A certificate issued by the TACC MICS CA must be revoked if:

- The private key is known or suspected to be lost or exposed.
- The information in the certificate is known to be inaccurate.
- The certificate is no longer needed.

Requests for certificate revocation may be made with cause by:

- The end-entity user;
- The LRA;
- The CA;
- The federated IdM.

4.10 Certificate Status Services

Not currently supported.

4.11 End of Subscription

The subscription ends with the expiry of the certificate.

4.12 Key Escrow and Recovery

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The TACC MICS CA runs on a machine that contains a FIPS 140 level 3 capable Hardware Security Module. The private key for the TACC MICS CA is stored on a dedicated partition in this tamper-proof device. The CA machine is physically located in a locked Security Rack in the keycard access controlled TACC computer room in the Commons Center on the J.J. Pickle Research Campus of the University of Texas at Austin.

Only TACC Security Officers and recognized auditors have access to the TACC MICS CA. The TACC MICS CA uses both a software and a hardware firewall to protect and monitor network access.

The FIPS 140 level 3 HSM provides a tamper-protected log of HSM events. Logs can be securely copied to an external location for inspection.

5.1 Physical Security Controls

Only TACC Security Officers may access the locked rack, the safe or any servers located inside the locked rack. Rack access is logged. The TACC on-line MICS CA server operates in an air-conditioned environment and is not rebooted or power-cycled except for essential maintenance. Online machines are located in a first floor access-controlled computer room with a raised floor and sprinkler system. The media and key archive storage GSA safe is fireproof.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

- TACC Security Officers
- Software developers of customized user and RA portal applications
- Designated LRAs. (See Appendix B.)

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The TACC MICS CA Security Officers must have Linux sysadmin experience as well as knowledge of any approved IdM infrastructures. TACC Security Officers and grid software developers must be permanent TACC staff. Grid software developers must follow security best practices and test code for potential compromise.

5.3.2 Background Check Procedures

TACC MICS 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 standing with both the TACC MICS CA and the organization they represent, including the authority to perform RA identity validation functions as stated in an official letter to the TACC Root CA. (See Appendix B.) A TACC Security Officer accepts this letter.

5.3.3 Training Requirements

TACC MICS CA and RA personnel will receive training in:

- TACC MICS CA operation
- RA portal application usage
- Approved IdM infrastructure usage and verification
- TACC Accounting System (TAS) database queries for account verification
- VOMRS and VOMS usage to support relevant Virtual Organizations (VOs)
- User portal documentation
- Physical and procedural security mechanisms.

5.3.4 Retraining Frequency and Requirements

Retraining shall be mandatory when new software or features or new approved IdM infrastructures are introduced.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Sanctions for unauthorized actions by TACC or UT 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 MICS 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 MICS CA personnel on request.

5.4 Audit Logging Procedures

No stipulation.

5.4.1 Types of Events Recorded

The TACC MICS CA logs the following CA functions:

- Certificate requests
- Certificate issuance and copies of certificates
- Certificate revocations and copies of CRLs
- All issued DNs, whether Active, Revoked or Expired;
- HSM events (tamper detection, device errors, slot operations, SO, Admin and User access);

- Login/logout/reboot of the CA server.

The user and RA web interface runs on a different server and records the following RA events:

- Identity check (indicating all supporting documentation, including AUPs, agreements, approval or rejection)
- Certificate submission requests (CSR)
- RA authority designation and all supporting documentation including ID, AUPs, agreements
- User and RA portal application release date, version number and verification checksum

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

Digitally signed audit logs will be stored for a minimum of three years after expiry or revocation.

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 must be periodically burned to read-only media suitable for either internal or external review. The audit collection system is internal to TACC CA.

5.4.7 Notification to Event-causing Subject

Operators of the TACC MICS CA can contact any event-causing subject using the ***email***, ***phone*** and ***address*** values associated with the user end-entity. In the event that a user can not be contacted within 24 hours by email or phone, the TACC MICS CA reserves the right to suspend that user's ability to create an X.509 user certificates and will send notification to that effect to the designated address. In the event that no contact can be made within 7 days, the TACC MICS CA will suspend certificate creation and will also notify identity authorities at the user's home Identity Provider.

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 Security Officers or internal or external auditors.

5.5.4 Archive Backup Procedures

Records shall be backed up routinely according to best practices for Class I data to meet UTS165 "Information Resources Use and Security Policy" requirements. (See (http://www.utsystem.edu/policy/ov/uts165.html).

5.5.5 Requirements for Time-stamping of Records

All event records shall bear a time-stamp.

5.5.6 Archive Collection System (internal or external)

Internal.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

In the case of a changeover of the TACC MICS 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 any 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 1Million seconds long.

5.7 Compromise and Disaster Recovery

The TACC MICS CA follows disaster recovery plans and procedures as available from the UT-Austin campus.

5.7.1 Incident and Compromise Handling Procedures

If the MICS CA is or may be compromised, TACC Security Officers will inform all

known participating relying parties, revoke the TACC MICS CA certificate and stop issuing user end-entity certificates. Upon remediation, the TACC MICS CA will be re-keyed and a new CA certificate will be issued.

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

The TACC MICS 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 MICS CA is corrupted the following steps shall be performed:

- All TACC MICS CA server 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 state of the software and data last known to be uncorrupted. Any credentials logged as issued subsequent to the last known uncorrupted backup must be checked and regenerated.
- If not all encrypted copies of the TACC MICS CA private key are destroyed or lost, and are not compromised, CA operation shall be reestablished as soon as possible without need for rekeying.

5.7.3 Entity Private Key Compromise Procedures

The TACC MICS CA relies on users and approved IdM infrastructures to manage user IdP password compromise. However, the TACC MICS CA Security Officer may choose to operate in elevated security mode where in addition to supplying a valid network identity and password, all users must answer a 2nd element question that was setup during initial registration.

In case the private key of an end entity is compromised, that certificate must be revoked. If the private key of an LRA is compromised, any certificates approved by that LRA from the initial date of the compromise must be revoked. All relying parties known to accept the compromised key shall 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. After revocation, the user will have to request a new certificate.

5.7.4 Business Continuity Capabilities after a Disaster

The TACC MICS 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 MICS CA operation.

5.8 CA or RA termination

Before the TACC MICS CA terminates its services, it will

- Inform all known relying parties.
- Make information of its termination widely available.
- Stop issuing certificates.
- Destroy its private keys and all copies.

An advance notice of no less than 60 days will be given in the case of normal (scheduled)

termination. 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.

In the event that a designated LRA leaves or is terminated from that position, a new LRA may be designated by the sponsoring organization. If an alternate LRA is found and formally designated, then no additional changes are required. If no LRA can be identified within 30 days, then all certificates previously issued by the previous LRA will be revoked and users will need to re-authenticate elsewhere.

6 TECHNICAL SECURITY CONTROLS

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

In the PKCS #11 model, a *slot* represents a device interface and a *token* represents the actual cryptographic device. The TACC MICS CA Manager generates a key pair for the TACC MICS CA as a labeled cryptographic token on a dedicated slot protected by the tamper-proof HSM.

The TACC MICS 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. In effect, users must generate their own private keys.

6.1.3 Public key Delivery to Certificate Issuer

Subscriber's public key is delivered to the TACC MICS CA as part of a CSR via a bi-directionally authenticated SSL/TLS connection.

6.1.4 CA Public Key Delivery to Relying Parties

The TACC MICS CA certificate (containing its public key) can be downloaded from its 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 are not accepted. The TACC MICS CA key is of length 2048 bits (RSA modulus).

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 MICS CA is defined by this CP/CPS document.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The keys may be used according to the type of certificate. The MICS CA's private key is the only key that can be used for signing certificates. Short-term user end entity certificates may be used for:

- Authentication
- Data and key encryption
- Proxy creation and signing

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The TACC MICS 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 MICS 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 MICS 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 MICS 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 Level 3.

6.3 Other aspects of Key Pair Management

6.3.1 Public Key Archival

The TACC MICS CA archives all issued short-term X.509v3 user end entity certificates on removable media that is stored offline in a secure GSA safe.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Subscriber's end entity certificates have a validity period set by the participating grid or VO, but less than 1 million seconds (approximately 11 days).

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The TACC MICS CA private key is protected by strong passphrases of at least 15 characters. The TACC Acceptable Use Policy (See Appendix A.) instructs users on the importance of protecting their certificate key materials.

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 MICS 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 MICS CA server.

6.5.1 Specific Computer Security Technical Requirements

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

6.8 Time-stamping

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

7 CERTIFICATE PROFILE

This section articulates details of certificates issued by the TACC MICS CA. The TACC MICS CA does not currently provide OCSP support.

7.1 Certificate Profile

All certificates issued by the TACC MICS CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 5280. The TACC MICS CA certificate 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=UTAUSTIN /CN=TACC Root CA
- The subject name shall be: /DC=EDU/DC=UTEXAS/DC=TACC/O=UTAUSTIN /CN=**TACC MICS 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 MICS CA issues only X.509 version 3 user end entity certificates.

7.1.2 Certificate Extensions

For the TACC MICS CA certificate:

- **basicConstraints** (critical): CA: true
- **keyUsage** (critical): Certificate Sign, CRL Sign
- X.509v3 Subject Key Identifier
- X.509v3 Authority Key Identifier

For natural person end entity certificates:

- **basicConstraints** (critical): CA: false
- subjectAlternativeName: email address
- Subject Key Identifier: a unique identifier of the subject key (a SHA-1 hash of the user's public key)
- Authority Key Identifier: keyid (the unique identifier – a SHA-1 hash of the TACC MICS CA certificate's public key)
- **keyUsage** (critical): digitalSignature, KeyEncipherment, dataEncipherment
- Extended Key Usage: clientAuth
- CRL Distribution Points: http://www.tacc.utexas.edu/CA/TACC_MICS_CRL.der
- Certificate Policy Identifiers:
    - The OID of this TACC MICS CA CP/CPS;

- The OID of the IGTF MICS Authentication Profile 1.3.6.1.4.1.17940.5.3.1.1.1;
- The OID indicating the type of identity vetting.

7.1.3 Algorithm Object Identifiers

The TACC MICS CA will use SHA1 for secure hashing.

• hash function: id-sha 1 1.3.14.3.2.26
• encryption: rsaEncryption 1.2.840.113549.1.1.1

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 MICS CA. The DN shall be structured as defined in the GFD125 (http://www.ogf.org/documents/GFD.125.pdf) standard.

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

1.3.6.1.4.1.17940.5.3.1.1

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

- o hash function: id-sha 1 1.3.14.3.2.26
- o encryption: rsaEncryption 1.2.840.113549.1.1.
- o signature: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.2.1 Version Number(s)

The TACC MICS 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 MICS 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 3 days 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 each one is valid for 7 days.

The CRL extensions shall include the CRL number.

7.3 OCSP Profile

Not yet supported.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The TACC MICS 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 MICS 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 MICS 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. It is recommended that assessors have a basic understanding of approved IdM infrastructures.

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 MICS CA personnel and infrastructure.

8.4 Topics Covered by Assessment

The audit will verify that the services provided by CA and LRA staff comply with the latest approved version of the CP/CPS. It is recommended that any approved IdM system make their periodic audits and reviews available to the TACC MICS CA to help identify procedural improvements.

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.

Audit failure by an RA is grounds for suspending TACC MICS CA authentication service for that campus until remediation is in place.

8.6 Communication of Results

The 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 MICS 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 MICS 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 MICS 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 MICS CA keeps personal information (work telephone number, work address) only to be able to contact subscribers and LRAs. Personal information such as 2nd element questions and answers are treated as confidential and protected according to Class I data guidelines. Personal information is treated as confidential and only stored within the secured TACC Accounting System (TAS).

Under no circumstances will the TACC MICS 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
The TACC MICS 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 UNAMgrid, AUSTRALIAGRID, CERN, CNRS, the German Grid, UK e-Science CA run by CCLRC, 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 MICS CA's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of these sources.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties
The TACC MICS CA guarantees to issue certificates only to subscribers identified by requests received from associated IdM infrastructures or designated LRAs for participating grids and VOs via secure routes. The TACC MICS 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 MICS 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 MICS CA only guarantees to verify subscriber's identities according to procedures described in this document.

The TACC MICS 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 MICS 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 MICS 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)
- Never disclose or share private keys associated with any certificate with end-entities other than the one to which the certificate was issued.
- 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 MICS 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 MICS 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 MICS 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 MICS CA cannot be held responsible for any misuse of its certificate by:

- A subscriber
- Any other 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 MICS 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 MICS 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 third-party identity management system acting in conformance with this CP/CPS.

9.9 Indemnities

The TACC MICS 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 MICS CA and all appropriate RAs 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 which violates the provisions of this CP/CPS document.

9.10 Term and Termination

Term of the TACC MICS CA is 5 years and may be renewable.

9.10.1 Term

Start date: 2008

End date: 2013

This policy becomes effective upon 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 MICS CA and any approved IdM infrastructure must be bi-directionally authenticated over a secure (SSL/TLS) channel.

All agreements between the TACC MICS 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 MICS CA Web pages at least 2 weeks before it becomes effective.

The TACC MICS 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

The OID shall change with every new version of the document. A major version number and a minor version number will be the last two components of the OID. Changes to the major version number of this CP/CPS require TAGPMA approval and a corresponding change to the OID. Changes to the minor version number and OID occur only when a new CP/CPS gets published to the TACC CA web site.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

The TACC MICS CA and its operation are subject to U.S. law and laws of the State of Texas and must comply with policies of the University of Texas.

9.15 Compliance with Applicable Law

All activities relating to the request, issuance, use or acceptance of a TACC MICS 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

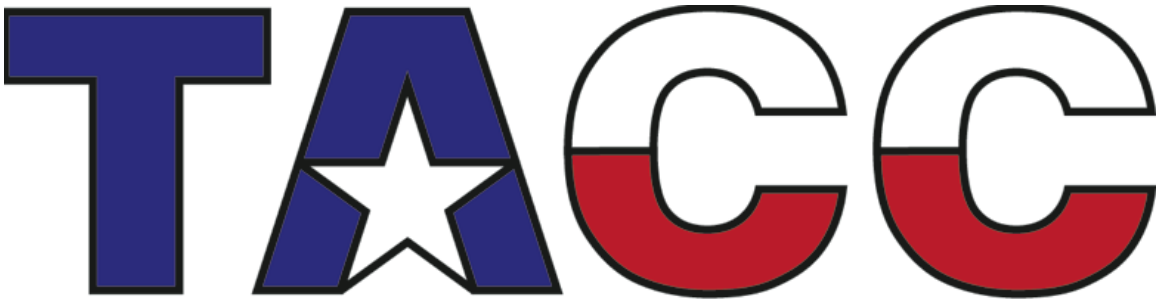
Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, that clause shall become void (and should be replaced as soon as possible by a conforming 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 MICS CA will be dealt with immediately either by the University of Texas at Austin or 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	**1.2**
Date last updated	13 May 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.
V1.2	13May09	Revised	Change User Agreement Paragraph 3 from "IGTF-approved credential" to "IGTF-accredited CA". Also minor format edits.

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 Local 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 (CA) or equivalent IGTF-accredited CA 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 MICS 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 if using a software token; 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 defined 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

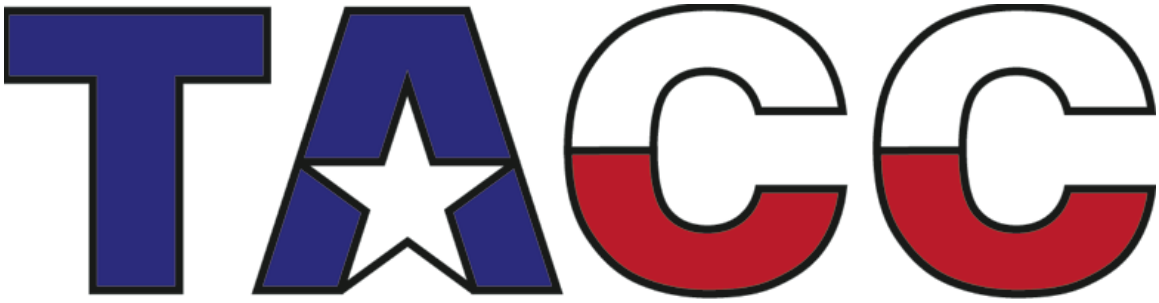
The undersigned acknowledges that s/he has read this TACC Certificate Acceptable Usage Policy Form and understands the enclosed information. The undersigned also acknowledges that s/he will abide by the stated policies and procedures to the best of his/her ability. The undersigned is also under obligation 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 verification against government documents with picture that confirm the user is who s/he says s/he is or a remote videolink identification against notarized copies of government documents with picture that have been sent via Registered Mail to the LRA.
    - 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}

APPENDIX C: UT-SYSTEM IdM FEDERATION

C.1 Overview

The University of Texas System Identity Management (IdM) Federation infrastructure consists of policies, technology and governance that enable inter-institutional collaboration based on Shibboleth middleware. Shibboleth is standards-based, open source software that enables Web Single SignOn (SSO) across or within organizational boundaries. Shibboleth identity providers (IdP) allow site application or service providers to make informed decisions about access to protected online resources based on authenticated identity assertions.

The TACC MICS CA will process any identity validated by any UT-System Federation member because all federated sites follow the same policies, use equivalent technology and are subject to the same governance.

- The procedures and policies that govern the initial, primary, identity validation are defined by the UT-System Shibboleth Federation and integrated with campus HR and identity card processes.
- The UT-System Shibboleth Federation identity data is maintained by campus HR.
- The UT-System Shibboleth Federation is connected to the MICS over a secured SSL/TLS connection. Attribute exchange is governed by a negotiated Attribute Release Policy (ARP).
- Information collected from the UT-Shibboleth Federation is checked against the default TAS database for name uniqueness prior to translation to the X.509 certificate;
- The TACC MICS CA relies on UT-System campus HR data and chooses to trust this data for no more than 1 Million seconds (~10 days) before re-verification.

C.2 General Architecture

C.2.1 Procedures & Policies that Govern Initial Identity Validation

UT-System Shibboleth users have an identity Level of Assurance (LoA) as defined by NIST Special Publication 800-63 "Electronic Authentication Guidelines" http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Identity proofing is not required at Level 1. At Level 2, identity-proofing requirements are introduced, requiring presentation of identifying materials or information. UT Shibboleth Identity information is populated by authoritative sources such as Human Resources or Student Services personnel. Although new Shibboleth users start with a default LoA at Level 1, campus hiring and registration policies require in-person identity vetting and checking of government issued documentation. When in-person identity vetting occurs, authoritative personnel may change a user's LoA to Level 2. The TACC MICS CA checks the user's LoA attribute and will only accept users identified as having an LoA of Level 2 without additional identity checking requirements.

C.2.2 IdM Management and Security

The UT-System Strategic Leadership Council http://www.utsystem.edu/slc/ promotes collaboration among all UT campuses by defining IT management principles and policies. An Identity Management Governing Board, a workgroup within the Strategic Leadership Council (SLC) sets technology standards and monitors adherence to policies.

Individual campus IdP servers operate within campus IT infrastructure secured to meet UTS165 "Information Resources Use and Security Policy" (http://www.utsystem.edu/policy/ov/uts165.html). Authorized UT staff are responsible for following best practices for maintaining secure production level identity authentication services.

C.2.3 IdM Connection to the TACC MICS CA

The potential TACC MICS CA User interacts with front-end authentication software via an access protected URL that requires creation of a Shibboleth session. First the user picks his/her home campus from a pull-down menu. Their request is then redirected to a specific campus IdP. That IdP authenticates the user's identity by checking his/her Shibboleth login username/password against campus maintained data. If successful, the IdP creates a Shibboleth session handle that is returned directly to the TACC MICS CA application via a Special URL. (Presence of the Shibboleth session handle asserts user identity.) The TACC MICS CA front-end authentication software now uses the session handle to issue a Shibboleth/SAML call back to the home campus Attribute Authority (AA). The TACC MICS CA front-end requests retrieval of the following attributes from the home IdP back-end datastore:

- eduPersonPrincipalName or eduPersonTargetedID – representations of the user's IdP identity
- cn – the user's common, or full name
- LOA – NIST 800-63 definition describes strength of identity verification
- Email – the user's organization email address
- Phone - the user's organization phone number
- Address at Institution – the user's organization address

If the user's LOA is only at Level 1, or if TACC is operating in an elevated security threat mode, then the TACC MICS CA front-end software will ask the user one of the 2nd element questions setup during initial registration. If the user's answer matches, then processing continues.

C.3 Identity Procedures

C.3.1 Maintenance of Unique Identity within the TACC MICS CA

The IdP identity maintained and provided by UT-System IdM Federation is expressed by ***eduPersonPrincipal*** and ***eduPersonTargetedID***. TACC's TAS database maintains a table of unique DNs keyed to the user's IdP identity, email, phone number, address and date of initial registration. DNs are guaranteed to be unique across both the TACC MICS CA and the TACC Classic CA so that every DN maps to one and only one person. Changes to an individual's email, phone number or address will trigger an RA check and serves to maintain the accuracy and integrity of the TAS data.

Unique Key	Associated Attributes	Attribute Description
CN	○ eduPersonPrincipal ○ eduPersonTargetedID ○ email ○ phone number ○ address ○ date of UT-System initial registration	○ IdP identity ○ Organization email ○ Organization phone ○ Organization address ○ Date when User met with IdM RA

C.3.2 Method Followed by the IdM to Validate Identity

The UT-System IdM Federation publishes minimum requirements and service levels of user identity at URL: https://idm.utsystem.edu/utfed/MemberOperatingPractices.pdf as follows:

1. Each UT-System Federation Member's implementation of specified minimum requirements and service levels must be audited annually by that Member's internal audit department.
2. The identity of employees, residents and post-doctoral fellows must be verified by official hiring or acceptance procedures implemented by the Member, which must include in-person identity vetting.
3. The identity of students must be verified by official admission procedures implemented by the Member, which must include in-person identity vetting.
4. Guests or other officially approved affiliates must be verified by established procedures implemented by the Member, which must include in-person identity vetting.
5. Controlled values for the multi-valued, eduPersonAffiliation attribute include "faculty, student, staff, alum, member, affiliate and employee". However, individuals that are "affiliates" can only have that sole value assigned to the eduPersonAffiliation attribute.

6. Each organization unit within a Member that is responsible for determining an individual's physical identity must submit that identity to a campus identity reconciliation process to ensure that an individual who may have been identified by multiple organizational units:
    a. Is assigned a single, permanent, unique identifier by the Member's IdM process,
    b. Has their vetted identity and assigned Member identifier permanently registered in the Member's"Person Registry"
    c. Is assigned a unique eduPersonPrincipalName (EPPN), and
    d. Has only a single "person" entry in the Member's Enterprise Directory.
7. If physical identities assigned to some individuals have not been verified according to the current Federation requirements, those identities must be re-verified prior to those individuals' being approved to use the Federation.
8. The level of assurance a relying party has in a digital credential presented for authentication personal identity depends on
    a. The degree of confidence associated with the vetting process used to establish the identity of the individual to whom the credential was supposedly issued, and
    b. The degree of confidence that the individual who used the credential is the individual to whom the credential was appropriately issued - i.e. how resistant is the credential to tampering.
    c. Credentialing of an identified individual by an IdP may be either in-person or remote.

    In-Person Credentialing:

    - For university personnel and students, the credentialing authority must require a valid current primary Government Picture ID that contains the individual's picture, and either address of record or nationality (e.g. driver's license or passport), to verify that the individual to whom the credential is being issued is the intended recipient.
    - For guests or other affiliates, the credentialing authority must require at least one government-issued, picture ID and an additional ID that may be a non-picture ID. The second ID could be a non-expired credit card, a known employer issued ID, etc.
    - An IdP must assert a **utPersonAssurance attribute of "Level One"** for any individual whose identity was unverified but to whom a username/password credential was issued.
    - An IdP may assert a **utPersonAssurance attribute of "Level Two"** for authentications by individuals whose physical identities were established by in-person vetting and were issued in person a username/password credential.
    - An IdP may assert a **utPersonAssurance attribute of "Level Three"** for authentications by individuals whose physical identities were established by in-person vetting and were issued in person a two-factor credential that is protected by a cryptographic strength mechanism. Three kinds of tokens may be

used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” tokens. These tokens protect against threats such as eavesdropping, replay, on-line guessing, verifier impersonation, and man-in-the-middle attacks.

- An IdP may assert a **utPersonAssurance attribute of “Level Four”** for authentications by individuals whose physical identities were established by in-person vetting and were issued in person a two-factor credential consisting of a “hard” token that cryptographically protects a key bound to the authentication process.

Remote Credentialing

- An IdP may remotely issue a username/password credential to an individual whose physical identity was previously vetted by an in-person appearance to that IdP’s registration agent upon comparing information securely supplied by the intended recipient to validated data in a trusted database. The IdP must assert an **utPersonAssurance attribute of “Level Two”** for such an individual.

9. To provide interoperability with Service Providers, Identity Providers must implement specific attributes as required in the Federation document entitled *Common Identity Attributes*.
10. The security domain of scoped attributes such as EPPN should be the same as that of the IdP for all Federation members.
11. Authentication, attribute and other application services provided by an IdP must be secured as specified in the physical, network and host security policies implemented by that IdP as specified by UTS165 “Information Resources Use and Security Policy”(http://www.utsystem.edu/policy/ov/uts165.html).
12. Transmission of shared secrets such as a password during the credentialing or authentication processes must be protected by SSL 128 bit or greater encryption.
13. An ***Identity Provider service***, e.g. a Shibboleth IdP, may use one of several authentication services. Examples include:
    a. ***Authentication services utilizing network transmitted passwords as an authentication credential.*** **(**It is critical that both IT personnel and users recognize that a network transmitted password is a user’s digital credential and should be known only to the credential user).
        - **Network transmitted passwords can only support Level One or Level Two assurance assertions.**
            - The network transmitted password authentication should be as secure and simple to manage as possible preferably having only a single password change module and interface that handles all aspects of password changes.
                1. Anytime a password is changed, the password change module should
                    a. Log the institutional permanent identifier of the person whose password was changed,
                    b. Log date and time of password change,

c. Log the institutional permanent identifier of the individual who changed the password, and
d. Send the password "owner" an e-mail stating when his/her password was changed and by whom.

2. Any additional mechanisms for changing passwords must be identified and documented.
3. Passwords and the controls used to limit on-line guessing attacks:
    a. Shall ensure that an attack targeted against a selected user's Password shall have a probability of success of less than 2^{-14} (i.e. one chance in 16,384) over the life of the password.
    b. Additionally, a password shall have at least 10 bits of min-entropy (a measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system) to protect against untargeted attack. *(Refer to NIST SP 800-63 Appendix A and the Credential Assessment Framework (CAF) Suite's Entropy Spreadsheet to calculate resistance to online guessing)*
    c. An example acceptable password would
        i. have a minimum length of 8 characters,
        ii. contain a mix of upper and lower case alpha characters,
        iii. have at least 2 non-alpha characters (i.e. numerals and/or special characters), and
        iv. have a password life of 90 days.
4. If possible, passwords should only be set/or reset by the identified person for whom the password is the assigned credential.
5. A password history must be maintained to prevent reuse of the current password as the new password.
6. Ideally, a network transmitted password management system should allow users also having an institutionally issued two-factor "soft" credential, "hard" credential or one-time password credential to set or change their network transmitted password.
7. If other designated individuals are permitted to change a user's password,
    a. The number of designated individuals must be kept at an absolute minimum.
    b. A list of trained designees currently approved to set or change passwords must be maintained.
    c. Any other individuals having system level

privileges that would permit changing passwords or credential binding to user authentication must be maintained.

- ***Authentication services utilizing two-factor credentials.***
  - Two-factor "soft" cryptographic credentials or one-time password credentials can be used to support Level 1, 2 and 3 assurance assertions.
  - Two-factor "hard" cryptographic credentials can be used to support Level 1, 2, 3 and 4 assurance assertions**.**
  - Cryptographic credentials must be issued by each institution's publicly rooted VeriSign certificate authority as specified by the U. T. System Master Service Agreement with VeriSign and the associated VeriSign Certificate Policy (CP) agreement and Certificate Practice Statement (CPS).

14. Processes and procedures must exist for immediately revoking or inactivating a digital credential when the Member becomes aware that a credential has been compromised.
15. Processes and procedures must exist to automatically revoke or inactivate a digital credential within 24 hours after an individual is no longer officially affiliated with the Member as indicated by any institutional source of authority (SOA) database.

C.3.7 Level of Assurance of Initial Identity Validation

Identities validated by UT-System Federation Identity Providers will have an LOA value of either 1 or 2. When LOA=2, then an in-person identity validation occurred at one of the UT-System federated institutions and the TACC MICS CA accepts this identity.

When LOA=1, the TACC MICS CA front-end checks the TACC Accounting System (TAS) to determine whether the user has been validated in-person with a designated site RA. If true, then front-end software automatically asks a 2nd element authentication question and will only proceed if the user provides the answer collected at initial registration.

C.3.8 Provisioning and Use of Second Authentication Element

The 2nd authentication element used by the TACC MICS CA is not published and is treated as private data protected according to UTS165 "Information Resources Use and Security Policy".

The 2nd authentication element is used under the following conditions:

- The user's LOA from the UT-System IdM Federation is not Level = 2 (indicating that in-person identity validation has not occurred.
- When TACC is operating at an elevated security threat level.

The 2nd authentication element is a user-specific questions and answer that is setup during the initial registration process.

The 2nd authentication element addresses the case where a user's IdM network username and password has been compromised.