

**TACC MICS CA  
CERTIFICATE POLICY  
AND  
CERTIFICATE PRACTICES STATEMENT**

(In RFC 3647 format)

D R A F T

Version 0.6

1 April 07

OID: 1.3.6.1.4.1.17940.5.3.1.1

Version 1.0

<b>1</b>	<b><i>INTRODUCTION</i></b> .....	<b>5</b>
1.1	Overview .....	5
1.2	Document Name and Identification .....	6
1.3	PKI Participants .....	6
1.4	Certificate Usage .....	7
1.5	Policy Administration .....	7
1.6	Definitions and Acronyms .....	7
<b>2</b>	<b><i>PUBLICATION AND REPOSITORY RESPONSIBILITIES</i></b> .....	<b>7</b>
2.1	Repositories.....	7
2.2	Publication of Certification Information .....	8
2.3	Time or Frequency of Publication .....	8
2.4	Access Controls on Repositories.....	8
<b>3</b>	<b><i>IDENTIFICATION AND AUTHENTICATION</i></b> .....	<b>8</b>
3.1	Naming .....	8
3.2	Initial Identity Validation.....	9
3.3	Identification and Authentication for Re-key Requests .....	10
3.4	Identification and Authentication for Revocation Request .....	10
<b>4</b>	<b><i>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS</i></b> .....	<b>10</b>
4.1	Certificate Application.....	11
4.2	Certificate Application Processing.....	11
4.2.1	Performing Identification and Authentication Functions.....	11
4.2.2	Approval or Rejection of Certificate Applications.....	11
4.2.3	Time to Process Certificate Applications.....	11
4.3	Certificate Issuance .....	11
4.3.1	CA Actions During Certificate Issuance.....	11
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate .....	11

<b>4.4</b>	<b>Certificate Acceptance .....</b>	<b>11</b>
<b>4.5</b>	<b>Key pair and certificate usage .....</b>	<b>11</b>
4.5.1	Subscriber Private Key and Certificate Usage.....	11
4.5.2	Relying Party Public Key and Certificate Usage.....	11
<b>4.6</b>	<b>Certificate Renewal .....</b>	<b>11</b>
<b>4.7</b>	<b>Certificate Re-key .....</b>	<b>11</b>
<b>4.8</b>	<b>Certificate Modification.....</b>	<b>11</b>
<b>4.9</b>	<b>Certificate Revocation and Suspension .....</b>	<b>11</b>
<b>4.10</b>	<b>Certificate Status Services.....</b>	<b>11</b>
<b>4.11</b>	<b>End of Subscription.....</b>	<b>11</b>
<b>4.12</b>	<b>Key Escrow and Recovery.....</b>	<b>12</b>
<b>5</b>	<b><i>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....</i></b>	<b>12</b>
<b>5.1</b>	<b>Physical Security Controls .....</b>	<b>12</b>
<b>5.2</b>	<b>Procedural Controls .....</b>	<b>12</b>
5.2.1	Trusted Roles .....	12
5.2.2	Number of Persons Required per Task .....	12
5.2.3	Identification and Authentication for each Role.....	13
5.2.4	Roles Requiring Separation of Duties .....	13
<b>5.3</b>	<b>Personnel Controls .....</b>	<b>13</b>
5.3.1	Qualifications, Experience, and Clearance Requirements .....	13
5.3.2	Background Check Procedures.....	13
5.3.3	Training Requirements .....	13
5.3.4	Retraining Frequency and Requirements .....	13
5.3.5	Job Rotation Frequency and Sequence.....	13
5.3.6	Sanctions for Unauthorized Actions.....	14
5.3.7	Independent Contractor Requirements.....	14
5.3.8	Documentation Supplied to Personnel .....	14
<b>5.4</b>	<b>Audit Logging Procedures.....</b>	<b>14</b>
5.4.1	Types of Events Recorded .....	14
5.4.2	Frequency of Processing Log.....	14
5.4.3	Retention Period for Audit Log .....	14
5.4.4	Protection of Audit Log.....	15
5.4.5	Audit Log Backup Procedures.....	15
5.4.6	Audit Collection System (internal vs. external) .....	15
5.4.7	Notification to Event-causing Subject.....	15
5.4.8	Vulnerability Assessments .....	15
<b>5.5</b>	<b>Records Archival .....</b>	<b>15</b>
5.5.1	Types of Records Archived.....	15
5.5.2	Retention Period for Archive .....	15
5.5.3	Protection of Archive .....	15
5.5.4	Archive Backup Procedures.....	15
5.5.5	Requirements for Time-stamping of Records.....	15
5.5.6	Archive Collection System (internal or external).....	16
5.5.7	Procedures to Obtain and Verify Archive Information .....	16
<b>5.6</b>	<b>Key Changeover.....</b>	<b>16</b>
<b>5.7</b>	<b>Compromise and Disaster Recovery.....</b>	<b>16</b>

5.7.1	Incident and Compromise Handling Procedures .....	16
5.7.2	Computing Resources, Software, and/or Data are Corrupted .....	16
5.7.3	Entity Private Key Compromise Procedures .....	16
5.7.4	Business Continuity Capabilities after a Disaster.....	17
<b>5.8</b>	<b>CA or RA termination .....</b>	<b>17</b>
<b>6</b>	<b><i>TECHNICAL SECURITY CONTROLS</i>.....</b>	<b>17</b>
<b>6.1</b>	<b>Key Pair Generation and Installation .....</b>	<b>17</b>
6.1.1	Key Pair Generation .....	17
6.1.2	Private Key Delivery to Subscriber .....	17
6.1.3	Public key Delivery to Certificate Issuer .....	17
6.1.4	CA Public Key Delivery to Relying Parties .....	17
6.1.5	Key Sizes.....	18
6.1.6	Public Key Parameters Generation and Quality Checking .....	18
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field).....	18
<b>6.2</b>	<b>Private Key Protection and Cryptographic Module Engineering Controls.....</b>	<b>18</b>
6.2.1	Cryptographic Module Standards and Controls .....	18
6.2.2	Private Key (m out of n) Multi-person Control .....	19
6.2.3	Private Key Escrow .....	19
6.2.4	Private Key Backup .....	19
6.2.5	Private Key Archival.....	19
6.2.6	Private Key Transfer into or from a Cryptographic Module .....	19
6.2.7	Private Key Storage on Cryptographic Module.....	19
6.2.8	Method of Activating Private Key.....	19
6.2.9	Method of Deactivating Private Key.....	19
6.2.10	Method of Destroying Private Key .....	19
6.2.11	Cryptographic Module Rating .....	20
<b>6.3</b>	<b>Other aspects of Key Pair Management .....</b>	<b>20</b>
6.3.1	Public Key Archival .....	20
6.3.2	Certificate Operational Periods and Key Pair Usage Periods .....	20
<b>6.4</b>	<b>Activation Data .....</b>	<b>20</b>
6.4.1	Activation Data Generation and Installation.....	20
6.4.2	Activation Data Protection.....	20
6.4.3	Other Aspects of Activation Data.....	20
<b>6.5</b>	<b>Computer Security Controls.....</b>	<b>20</b>
6.5.1	Specific Computer Security Technical Requirements.....	20
6.5.2	Computer Security Rating.....	20
<b>6.6</b>	<b>Life Cycle Technical Controls .....</b>	<b>21</b>
6.6.1	System Development Controls .....	21
6.6.2	Security Management Controls .....	21
6.6.3	Life Cycle Security Controls .....	21
<b>6.7</b>	<b>Network Security Controls.....</b>	<b>21</b>
<b>6.8</b>	<b>Time-stamping .....</b>	<b>21</b>
<b>7</b>	<b><i>CERTIFICATE PROFILE</i> .....</b>	<b>21</b>
<b>7.1</b>	<b>Certificate Profile.....</b>	<b>21</b>
7.1.1	Version Number(s) .....	21
7.1.2	Certificate Extensions.....	21
7.1.3	Algorithm Object Identifiers.....	22
<b>7.2</b>	<b>CRL Profile.....</b>	<b>22</b>

7.3	OCSP Profile .....	22
<b>8</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>22</b>
8.1	Frequency or Circumstances of Assessment .....	22
8.2	Identity/qualifications of Assessor .....	22
8.3	Assessor’s Relationship to Assessed Entity.....	23
8.4	Topics Covered by Assessment.....	23
8.5	Actions Taken as a Result of Deficiency .....	23
8.6	Communication of Results .....	23
<b>9</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>23</b>
9.1	Fees.....	23
9.2	Financial Responsibility.....	23
9.3	Confidentiality of Business Information .....	23
9.4	Privacy of Personal Information .....	23
9.5	Intellectual Property Rights .....	24
9.6	Representations and Warranties.....	24
9.7	Disclaimers of Warranties.....	24
9.8	Limitations of Liability .....	25
9.9	Indemnities .....	25
9.10	Term and Termination .....	25
9.10.1	Term.....	25
9.10.2	Termination.....	25
9.10.3	Effect of Termination and Survival .....	25
9.11	Individual Notices and Communications with Participants .....	25
9.12	Amendments.....	26
9.12.1	Procedure for Amendment .....	26
9.12.2	Notification Mechanism and Period.....	26
9.12.3	Circumstances under which OID must be Changed .....	26
9.13	Dispute Resolution Provisions .....	26
9.14	Governing Law.....	26
9.15	Compliance with Applicable Law .....	26
9.16	Miscellaneous Provisions.....	26
9.17	Other provisions .....	26
<b>APPENDIX A: UT-SYSTEM IdM FEDERATION .....</b>		<b>27</b>
<b>APPENDIX B: FORMAL REGISTRATION AUTHORITY (RA) AGREEMENT..</b>		<b>37</b>

# 1 INTRODUCTION

The Texas Advanced Computing Center (TACC) operates a Certification Authority called the TACC 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:

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

The TACC MICS CA relies on and leverages existing IdM infrastructures to simply and securely generate short-term X.509v3 end entity certificates to individuals authenticated by those IdMs. 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

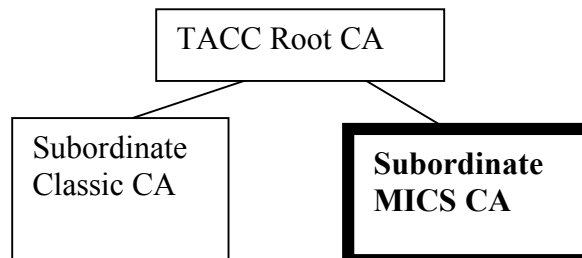
Structured according to RFC 3647, this document describes policy and practices of TACC MICS CA PKI services. The Certificate Policy (CP) describes the requirements for operation of the PKI and for granting PKI credentials as well as lifetime management of those credentials. The Certificate Practices 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:	<b>TACC Member Integrated Credential Services (MICS) Grid CA Certificate Policy and Certification Practice Statement</b>
Document version:	<b>1.0</b>
Document date:	<b>3 April 2007</b>
OID:	1.3.6.1.4.1.17940.5.3.1 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) ut-austin(17940) tacc(5) micsca(3) cps(1) version 1}

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

## 1.3 PKI Participants

TACC will manage and operate the TACC PKI. This includes the off-line Root CA, the on-line HSM-protected TACC Classic Grid CA, the on-line HSM-protected TACC MICS CA, Security Officers located at TACC and Registration Authorities (RAs) located at TACC and at distributed sites. TACC web-based User Portals and Registration Authority (RA) web applications support user certificate requests and management. Web browsers are the responsibility of the client, not TACC.

- Certificate Authorities: The TACC MICS CA certificate is signed by the TACC Root CA and issues only short-term user end entity certificates.
- Registration Authorities: RAs are formally authorized to perform in-person vetting of individual users according to minimum standards and service levels. RAs may be part of an existing IdM infrastructure, or they may be established via formal agreement with the TACC CA. (See Appendix B.)
- Subscribers: Only users registered at NIST 800-63 level of assurance of Level 2 may receive certificates from the TACC MICS CA. Level 2 requires in-person vetting and presentation of identity documents.
- Relying Parties: Relying parties must verify certificates issued by the TACC MICS CA and check that they have not expired.

## **1.4 Certificate Usage**

Usage of a TACC MICS CA short-lived RFC3820 X.509 v3 end entity user certificate includes but is not limited to login authentication, job submission, encrypted email and SSL encryption.

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  
Commons Center 1.154D, J.J. Pickle Research Campus  
10100 Burnet Road (R8700), Building 137  
Austin, TX 78758-4497  
Telephone: (512) 475-9411  
Fax: (512) 475-9445  
Email: [ca@tacc.utexas.edu](mailto:ca@tacc.utexas.edu)

## **1.6 Definitions and Acronyms**

No stipulation.

# **2 PUBLICATION AND REPOSITORY RESPONSIBILITIES**

## **2.1 Repositories**

It is the responsibility of the TACC MICS CA to publish the following information:

- TACC MICS CP/CPS document
- The TACC MICS Subject CA certificate (signing policy)
- The self-signed TACC Root CA certificate that acts as the trust anchor for all TACC PKI infrastructure
- End entity Certificate Disclosure statement summary indicating end entity certificate length, lifetime and extensions.
- Official contact email address for inquiries and fault reporting ([ca@tacc.utexas.edu](mailto:ca@tacc.utexas.edu))
- A physical and postal contact address.

## 2.2 Publication of Certification Information

The TACC MICS CA publishes required information on its public website at URL: <http://www.tacc.utexas.edu/CA/>. As a member of the TAGPMA, the TACC Root CA grants the IGTF and its PMAs the right of unlimited redistribution of information.

## 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.

## 2.4 Access Controls on Repositories

The online repository is maintained on a best effort basis and is available substantially 24 hours per day, 7 days per week, subject to reasonable scheduled maintenance. Outside the period 08:00-17:00 Monday-Friday it may run unattended “ at risk”. The TACC MICS CA does not impose any access control on its CP/CPS or PKI Disclosure Statement.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

DC = edu; DC = utexas; DC = tacc  
O = TACC; OU = TACC MICS CA  
----- *{added if RA not at TACC}*  
O = **{specific IDM}** OU = **{campus RA/IdP}**  
-----  
CN = *{unique CN from array}*  
SubjectAltName = *{email supplied by IdP}*

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

The fixed component is common to all certificates issued by the TACC 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=TACC/OU=TACC MICS CA

The variable component contains an organization and organizational unit pair that indicates the IDM or distributed RA who vetted the end entity. Some examples:

- /O=UT-System Federation/OU={campus}
- /O=TIGRE/OU=TTU
- /O=TeraGrid/OU={TeraGrid site}

In order to maintain unique DNs while also maximizing DN filtering options within the TACC PKI, Common Names (CNs) must uniquely map to one and only one individual whether used by the TACC MICS CA or the TACC Classic CA. Therefore, a single array of all existing CNs is checked for no matches before any new CN may be assigned and added to the array. Binding of CN to individual end entity is permanent for the lifetime of TACC PKI.

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

- Numbers: 0 – 9
- Characters: a – z and A – Z
- Special characters in user certificates: space and hyphen
- Special characters in host or service certificates: period and slash (/)

### **3.2 Initial Identity Validation**

Certificate subscribers must initially prove their identity to a designated Registration Authority (RA). Each user must establish identity by presenting qualifying government-issued photo-identification documents at an initial in-person meeting.

RAs 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 Appendices). All designated RAs must use the same web application provided by TACC to perform all RA functions. Data collection functions during initial identity validation include:

- In-Person Identity Vetting: All RAs will set a Level of Assurance (LoA) attribute as defined by NIST SP800-63 where Level  $\geq 2$  indicates in-person identity vetting with presentation of government issued documents. Where an approved IdM infrastructure exists, the RA web application will not require presentation of documentation for users already having LoA Level  $\geq 2$ . Identities who possess a LoA attribute Level=1 shall not obtain valid credentials from the TACC MICS CA unless in-person identity vetting verifiably occurred separately from the IdM.
- User Contact Info: Sufficient information shall be stored at initial registration to enable contact with the registered identity owner.
- 2<sup>nd</sup> Element Security Info: Five user-specific questions and answers shall be setup during the initial registration process. The user may answer questions from a list

of suggested questions for up to 3 out of 5 authentication elements. The user must supply 2 unique authentication questions and answers but may provide all five.

Information collected during initial identity validation must be treated as private data and stored securely according to UTS165 “Information Resources Use and Security Policy”.

### **3.3 Identification and Authentication for Re-key Requests**

Short certificate lifetimes make certificate re-key requests irrelevant to the TACC MICS CA.

### **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 RA may use the TACC RA web application to suspend or revoke a user’s ability to request a TACC MICS CA certificate.

## **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 document verification
- initial registration with a designated TACC RA

may request a short-term X.509 user end-entity certificate by clicking on a “Get short-term TACC X.509 certificate” button within their grid portal.

### **4.2 Certificate Application Processing**

The grid portal front end attempts to authenticate users against an approved IdM infrastructure as described in attached Appendices. The requesting user’s Level of Assurance (LOA) attribute must be greater than or equal to 2.

When a validated user’s 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 2<sup>nd</sup> element authentication question and will only proceed if the user provides the answer collected at initial registration. In the event that TACC is operating in an elevated security mode, all users will be asked a 2<sup>nd</sup> element authentication question.

### **4.3 Certificate Issuance**

Upon successful user authentication, back-end processing begins with acceptance of retrieved user attributes. The portal back-end communicates securely with the TACC MICS CA server, using one of the user attributes as a key to query an array of unique CNs. The resulting CN, uniquely mapped to the requesting user, becomes part of the subject DN of a Certificate Signing Request (CSR) in PKCS#10 format that is submitted

to the TACC MICS CA server. The TACC MICS CA server shall receive the CSR from the portlet back-end and use OpenSSL to create a certificate signed with the private key of the TACC MICS CA. The resulting signed certificate is then loaded into a MyProxy server. Requests for short-term X.509 user end entity certificates are processed automatically from the grid portal in the order received in close to real-time.

The TACC MICS CA server automatically sends notification to the user's *email* when a short-term X.509 certificate is issued. Email content indicates the creation time, certificate lifetime and MyProxy server name associated with the certificate.

#### **4.4 Certificate Acceptance**

Retrieval of a certificate from the MyProxy server either by the user or on behalf of the user via portal software is considered acceptance.

#### **4.5 Key pair and certificate usage**

Since the TACC MICS CA only generates short-term X.509 user end entity certificates, it generates a new key pair for each certificate based on:

1. A unique and static binary attribute associated with the user and treated as the user's public key.
2. A high-entropy dynamic attribute associated with the user (e.g., a session handle) that is treated as the user's private key.

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**

Short-term end entity certificates may only be renewed if the user re-authenticates.

#### **4.7 Certificate Re-key**

Not applicable.

#### **4.8 Certificate Modification**

Not applicable.

#### **4.9 Certificate Revocation and Suspension**

Short-term X.509 certificates are not revoked or suspended, but are allowed to expire.

#### **4.10 Certificate Status Services**

Not 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 one core of a dual-core Dell 2850 machine that contains a FIPS 140 level 3 capable Hardware Security Module (the SafeNet ProtectServer Gold PCI). 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. While the TACC RA portal application server based on apache-tomcat runs on a different system than the CA, it also resides in the same or a similarly protected locked rack.

Only TACC Security Officers and recognized auditors have access to the TACC MICS CA. The TACC MICS CA uses both a *shorewall* software firewall and a HotBrick VPN 800/2G hardware firewall to protect and monitor network access.

The SafeNet ProtectServer Gold PCI HSM provides a tamper-protected log of issued certificates and 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. 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. Backups of all host or service keys will be stored on PCI smart card media or removable disk drives and placed in this safe located inside the locked rack. Access to this safe will be logged.

#### **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 RAs. (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 RAs must have official standing with both the TACC MICS CA and the organization hosting the RA 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 and creation
- HSM events (tamper detection, device errors, slot operations, SO, Admin and User access)
- Login/logout/reboot of the CA server

The user and RA portal application 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 MICS CA audit logs are stored on the tamper-proof HSM. Logs can be securely exported to the TACC Security Officers on a weekly basis or upon individual request.

### **5.4.3 Retention Period for Audit Log**

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

#### **5.4.4 Protection of Audit Log**

CA and RA events in the audit logs are stored on the tamper-proof HSM. Audit logs are viewable only by TACC Security Officer personnel or internal or external auditors.

#### **5.4.5 Audit Log Backup Procedures**

The TACC MICS CA audits logs are routinely backed up in encrypted form according to best practices for data backup onto the TACC hierarchical storage manager archive system.

#### **5.4.6 Audit Collection System (internal vs. external)**

TACC MICS CA audit logs may be burned to CDROMs suitable for either internal or external review.

#### **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.

#### **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**

Not applicable.

## **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 network identity 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 2<sup>nd</sup> element question that was setup during initial registration.

#### **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.

### **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**

The off-line TACC Root CA will be used to generate the key pair for the subordinate TACC MICS CA. The TACC MICS CA will subsequently use facilities provided with the ProtectServer Gold PCI HSM to securely store this private key; to include the public key in a CSR file written to USB drive for signing by the off-line TACC Root CA; and to sign certificates generated by OpenSSL. (In this way, the TACC PKI infrastructure can reissue the TACC MICS CA certificate in the event of a change of HSM hardware.

##### **6.1.2 Private Key Delivery to Subscriber**

Because the TACC MICS CA only generates short-term user end-entity certificates, it generates a new key pair for each certificate based on:

1. A unique and static binary attribute associated with the user and treated as the user's public key.
2. A high-entropy dynamic attribute associated with the user (e.g., a session handle) that is treated as the user's private key.

##### **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.

##### **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/>

### **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**

Not defined.

### **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
- Non-repudiation
- Data and key encryption
- Object integrity (especially messages)
- Session establishment
- 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 SafeNet ProtectServer Gold-PCI Hardware Security Module (HSM) accredited as FIPS 140 Level 3 compliant. This private key is stored in 3DES encrypted form on the tamperproof HSM card. 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 FIPS accredited OpenSSL and the ProtectServer Toolkit APIs. Backups of the encrypted private key occur only to smart cards. The keys for these smart cards, and the 3DES key used to encrypt the signing private key, are generated by the SafeNet ProtectServer Gold-PCI FIPS 140 Level 3 device (key generation is based on a hardware random number generator). 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 GSA safe accessible only to TACC Security Officers.

### **6.2.1 Cryptographic Module Standards and Controls**

The on-line TACC MICS CA server contains a SafeNet ProtectServer Gold PCI Hardware Security Module. This tamper-proof device meets FIPS 140 Level 3 validation. In addition, the on-line TACC MICS CA server uses the FIPS accredited version of OpenSSL. The TACC MICS CA private key is generated using OpenSSL FIPS version software.

TACC MICS CA personnel shall use one-time password or PIN access in addition to a strong passphrase of at least 15 characters.

An extra instance of the private key encrypted with a randomly generated passphrase of at least 15 characters shall be stored on removable media which must be stored in the

GSA safe.

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 Level 3 ProtectServer Gold PCI hardware Security Module (HSM).

### **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). The passphrase for activating the backup is locked in the GSA safe in a sealed envelope.

### **6.2.5 Private Key Archival**

The CA private key may be exported from the SafeNet ProtectServer Gold PCI HSM in encrypted form with an integrity preserving checksum to a PCI Smart card.

### **6.2.6 Private Key Transfer into or from a Cryptographic Module**

Only transfer methods supported by the SafeNet ProtectServer Gold-PCI 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 Level 3 SafeNet ProtectServer Gold PCI HSM.

The CA private key is activated by a passphrase. In the event of an emergency, the CA private key passphrase is kept in a sealed envelope in the GSA safe.

### **6.2.8 Method of Activating Private Key**

The TACC MICS CA private key becomes active by following SafeNet ProtectServer Gold-PCI HSM CA procedures.

### **6.2.9 Method of Deactivating Private Key**

The TACC MICS CA private key can be erased by following SafeNet ProtectServer Gold-PCI HSM CA procedures.

### **6.2.10 Method of Destroying Private Key**

Following SafeNet ProtectServer Gold-PCI HSM CA procedures to erase a private key also destroys it.

### **6.2.11 Cryptographic Module Rating**

SafeNet's ProtectServer Gold-PCI and Core Toolkit are in the Finalization stage of accreditation 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 and certificate passwords are protected by strong passphrases of at least 15 characters.

### **6.4.2 Activation Data Protection**

Activation data for the TACC MICS CA private key is also kept in a sealed envelope in a safe.

### **6.4.3 Other Aspects of Activation Data**

Not defined.

## **6.5 Computer Security Controls**

Only TACC Security Officers may access the on-line TACC MICS CA server. Designated personnel must use one-time passwords to gain root access to this 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 via RedHat's up2date subscription facility.

### **6.5.2 Computer Security Rating**

Not defined.

## **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**

User and RA portal application development software follows security best practices, operates under change management control and is subject to security compromise analysis. Released versions of portal applications contain embedded checksums as a countermeasure to unapproved modifications.

## **6.7 Network Security Controls**

All communication to the TACC MICS CA server occurs over encrypted SSL/TLS tunnels on known ports by authenticated users. Both a *shorewall* software firewall and a HotBrick VPN 2000/G hardware firewall monitor and filter network traffic. The hardware firewall performs stateful packet inspection.

## **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 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 end entity certificates as defined by RFC 3820 with the following Profile:

### **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): Digital Signature, 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 Classic CA certificate's public key)
- **keyUsage** (critical): digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
- Extended Key Usage: clientAuth, emailProtection, codeSigning, timeStamping
- Policy Identifier: 1.3.6.1.4.1.17940.5.3.1.1.0

### **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
- signature: sha1WithRSAEncryption 1.2.840.113549.1.1.5

### **7.2 CRL Profile**

Not Applicable.

### **7.3 OCSP Profile**

Not 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 to check operation compliance of CA staff against the CP/CPS document in effect. In addition, audit checks of RA compliance shall occur on a per campus basis annually. A list of CA and compliant designated RA personnel will be maintained.

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 may 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/RA 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**

### **9.1 Fees**

No fees are charged for the certification service for the TACC constituency and therefore there are no financial encumbrances.

### **9.2 Financial Responsibility**

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

### **9.3 Confidentiality of Business Information**

The TACC MICS CA will follow best practices to protect confidential information as specified by University of Texas policy UTS165 "Information Resources Use and Security Policy" (<http://www.utsystem.edu/policy/ov/uts165.html>).

### **9.4 Privacy of Personal Information**

Information included in issued certificates is not considered confidential. The TACC MICS CA collects a subscriber's name, work telephone numbers and e-mail address only to be able to contact subscribers. Personal information such as 2<sup>nd</sup> element questions and

answers are treated as confidential and protected according to Class I data guidelines. The TACC MICS CA will not disclose confidential information to any third party unless authorized to do so by the subscriber or when required by law enforcement officials who exhibit a valid subpoena. Disclosure to law enforcement officials must occur under the auspices of the UT-Austin Office of the Vice President for Institutional Relations and Legal Affairs at (512) 471-1241.

## 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

When issuing a short-term user end entity certificate, the TACC MICS CA is satisfied that the user identity has successfully authenticated to an approved IdM infrastructure.

By requesting a TACC MICS CA certificate a subscriber must:

- Use the certificate for AUP permitted purposes only
- Authorize the processing and conservation of personal data
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the passphrase associated with subscriber's IdM identity,
- Notify the TACC MICS CA or the home IdP if the passphrase is lost or compromised;

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;
- The certificate is used for permitted purposes only, and
- The certificate has not expired.

## 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: 2007

End date: 2012

### **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.

## **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**

No stipulation.

## **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**

No stipulation.

## **9.17 Other provisions**

No stipulation.

# APPENDIX A: UT-SYSTEM IdM FEDERATION

## A.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.

## A.2 General Architecture

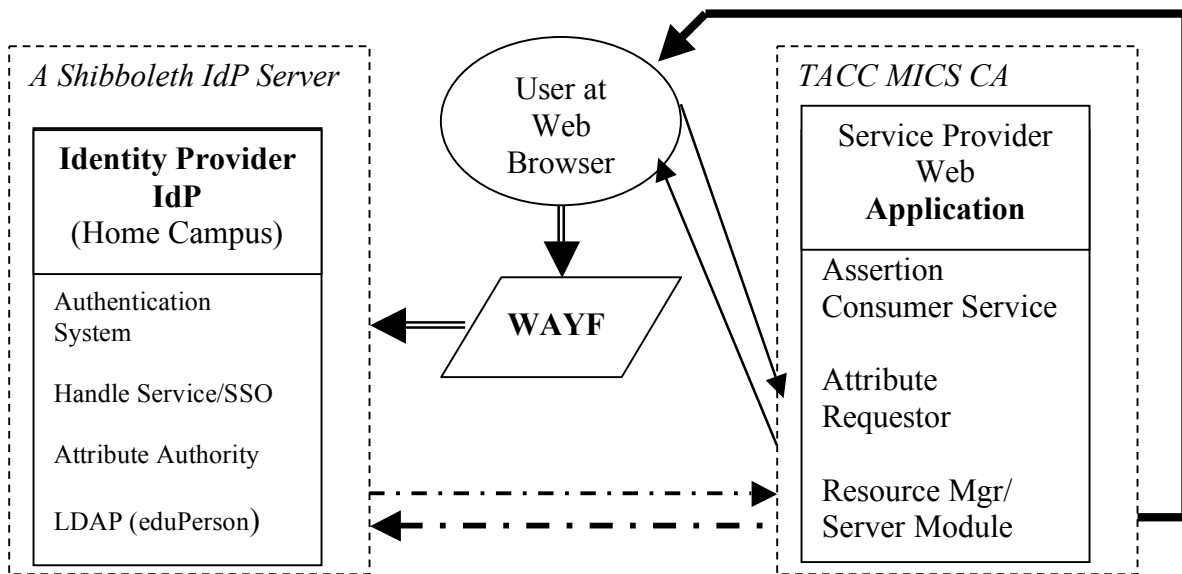


Figure A-1 TACC MICS CA Front-end and Shibboleth Architecture

**Table A-1 How Shibboleth Works**

<i>Step</i>	<i>Component</i>	<i>Function</i>
1	User Web Browser	User requests access to an application or service via a web browser over an SSL/TLS channel.
2	TACC MICS CA front-end (Resource Mgr)	The Resource Manager Application/Service provider recognizes that access requires a Shibboleth session.
3	WAYF	User request is redirected to a Where Are You From (WAYF) server so that user can identify which organization within the federation can authenticate him/her.
4	Home IdP Handle Service/SSO	User request is forwarded to the Handle Server (HS) Single Signon (SSO) that is part of his/her campus IdP.
5	Home IdP Authentication System	Home campus authentication system determines whether user identity is known.
6	Home IdP Handle Service/SSO;	Handle Server sends unique session handle over 2 <sup>nd</sup> SSL/TLS channel to Assertion Consumer Service at Service Provider.
7	MICS CA front-end; Attribute Requestor	Attribute Requestor at Service Provider uses that same session handle to request attributes needed by the application.
8	Home IdP Attribute Authority	Attribute Authority checks Attribute Release Policy to determine whether attributes may be released.
9	SSL/TLS channel from IdP to MICS CA front-end	If Identity Provider's Attribute Release Policy allows, Attribute Authority queries backend LDAP database and returns attributes back to Attribute Requestor over 2 <sup>nd</sup> SSL/TLS channel.
10	SSL/TLS channel from MICS CA front-end to user's browser	If returned attributes pass web application filters, then user gains access to application or service.

## **A.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](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.

## **A.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.

## **A.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
- cn

- eduPersonTargetedID
- LOA
- Email
- Phone
- Address at Institution
- eduPersonEntitlement(PIeligible)

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 2<sup>nd</sup> element questions setup during initial registration. If the user's answer matches, then processing continues.

Once all identity filters are checked and pass, the TACC MICS CA accepts the user's identity and uses his/her eduPersonTargetedID to query an array of unique DNs. This DN, uniquely mapped to this user, is used to construct a CSR that will be submitted to the TACC MICS CA server.

#### **A.2.4 Identity Translation to X.509 Certificate**

```

DC = edu; DC = utexas; DC = tacc
O = UT-Austin; OU=TACC MICS CA
----- {added if RA not at TACC}
O = {RA-org}; OU = {RA-dept}
O = {UT-System IDM}; OU = {campus IdP}
-----
CN = {Select DN from DNarray where Key=eduPersonTargetedID}
SubjectAltName = {email supplied by IdP}

```

#### **A.2.5 Chain of Trust Protection**

All communication with any home IdP occurs over a SSL/TLS channel. In addition, every IdP server and the TACC MICS CA front-end system all register and maintain their valid host certificates with the UT-System IdM metadata server.

### **A.3 Identity Procedures**

#### **A.3.1 Maintenance of Unique Identity within the TACC MICS CA**

The TACC MICS CA maintains one array of unique DNs keyed to the user's network 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. The network identity maintained and provided by UT-System IdM Federation is expressed by *eduPersonTargetedID*.

### **A.3.2 Method 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".
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).
    - o **Network transmitted passwords can only support Level One or Level Two assurance assertions.**
      - The network transmitted password authentication system
      - 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.

### ***A.3.3 Method to Prevent Re-Issuance of Identity’s DN to a Different End Entity***

It is the intention of the UT-System IdM Federation to avoid re-issuance of any eduPersonTargetedID to a different end entity. The TACC MICS CA makes specific checks to detect the unlikely event that an eduPersonPrincipleName may have been reissued to a different individual: Before a DN is mapped to a UT-System IdM user, front end access software checks that the eduPersonTargetedID, email, phone and address received from the IdP all match those elements in the unique DN array. If any discrepancy is discovered, the Security Officer is notified and the user receives a message indicating that a problem has occurred.

### ***A.3.4 Method of Identity Accountability and Traceback***

Operators of the TACC MICS CA can contact any subscriber using the *email*, *phone* and *address* values maintained and provided by the UT-System IdM Federation. 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 notify identity authorities at the user’s home IdP.

### ***A.3.5 Method of Protecting Re-usable Private Information for Authentication***

The TACC MICS CA relies on institution maintained and protected email, phone and address information. Normally, this information is considered public and appears in public directories.

Any information collected by RA personnel during initial registration is considered private and is protected according to UTS165 “Information Resources Use and Security Policy”.

### **A.3.6 Notification to End-entities of Certificate Issuance**

The TACC MICS CA server automatically sends notification to the user’s *email* when a short-term X.509 certificate is issued. Email content indicates the creation time, certificate lifetime and MyProxy server name associated with the certificate.

In the event that notification email bounces, the TACC MICS CA operators will attempt to contact the user by *phone*. If no contact can be made within 24 hours, the TACC MICS CA reserves the right to suspend that user’s ability to create X.509 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 also notify identity authorities at the user’s home IdP.

### **A.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 2<sup>nd</sup> element authentication question and will only proceed if the user provides the answer collected at initial registration.

### **A.3.8 Provisioning and Use of Second Authentication Element**

The 2<sup>nd</sup> 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 2<sup>nd</sup> 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 2<sup>nd</sup> authentication element is one of five user-specific questions and answers that are setup during the initial registration process. The user may answer questions from a list of suggested questions for up to 3 out of 5 authentication elements. The user must supply 2 unique authentication questions and answers and may provide all five authentication elements.

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

## **APPENDIX B: FORMAL REGISTRATION AUTHORITY (RA) AGREEMENT**

The Registration Authority for a given site or organization must be a paid employee of the Physical Organization hosting that Registration Authority with authorization to validate individuals who belong to the Physical Organization. For example, the TACC MICS CA will accept the following letter, on organization letterhead, as a formal agreement establishing a Registration Authority:

To whom it may concern:

    {individual's name}     is authorized to perform in-person identity validation according to established, required identity assurance procedures to enable individuals affiliated with   {Organization Name}   to acquire X.509 identity credentials from TACC CAs. I certify that     {individual's name}     is a paid employee of   {Organization Name}   and has management approval to perform in-person identity validation from   {date}   until   {date}  .

I also acknowledge that     {individual's name}     must view identity documents (e.g., passports, driver's licenses and campus ID) and may be required to record information about those documents while protecting identity data from theft or abuse.

Signed:

1. RA
2. RA's manager
3. Campus/Organization Authority

Upon receipt of this formal agreement, the TACC CA Security Officer will provide a "TACC CA Registration Authority (RA)" Web application the the designated RA This application enables:

- Initial registration for user, hosts and services
- Registration update for user, hosts and services
- Revocation or suspension of user X.509 credentials

RAs must run this application on a system having a TACC Classic CA host certificate and must adhere also to the TACC CA Subscribers' Obligations.

