

Certification Authority  
TSU CA

Certificate Policy  
and  
Certification Practice Statement

Version 0.0.0

July 26, 2013

## CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>8</b>
1.1	OVERVIEW .....	8
1.2	DOCUMENT NAME AND IDENTIFICATION.....	8
1.3	PKI PARTICIPANTS.....	9
	1.3.1 <i>Certification Authorities</i> .....	9
	1.3.2 <i>Registration Authorities</i> .....	9
	1.3.3 <i>Subscribers</i> .....	9
	1.3.4 <i>Relying parties</i> .....	9
	1.3.5 <i>Other participants</i> .....	9
1.4	CERTIFICATE USAGE .....	9
	1.4.1 <i>Appropriate certificate uses</i> .....	9
	1.4.2 <i>Prohibited certificate uses</i> .....	9
1.5	POLICY ADMINISTRATION .....	9
	1.5.1 <i>Organization administering the document</i> .....	9
	1.5.2 <i>Contact Person</i> .....	10
	1.5.3 <i>Person determining CPS suitability for the policy</i> .....	10
	1.5.4 <i>CPS approval procedures</i> .....	10
1.6	DEFINITIONS AND ACRONYMS .....	10
	1.6.1 <i>Definitions</i> .....	10
	<b>AUTHENTICATION.....</b>	<b>10</b>
<b>2</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>12</b>
2.1	REPOSITORIES .....	12
2.2	PUBLICATION OF CA INFORMATION.....	12
2.3	TIME OR FREQUENCY OF PUBLICATION.....	12
2.4	ACCESS CONTROL ON REPOSITORIES .....	12
<b>3</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>13</b>
3.1	NAMING.....	13
	3.1.1 <i>Types of names</i> .....	13
	3.1.2 <i>Need for names to be meaningful</i> .....	13
	3.1.3 <i>Anonymity or pseudonymity of subscribers</i> .....	13
	3.1.4 <i>Rules for interpreting various name forms</i> .....	13
	3.1.5 <i>Uniqueness of names</i> .....	13
	3.1.6 <i>Recognition, authentication and role of trademarks</i> .....	13
3.2	INITIAL IDENTITY VALIDATION.....	13
	3.2.1 <i>Method to prove possession of private key</i> .....	13
	3.2.2 <i>Authentication of organization identity</i> .....	13
	3.2.3 <i>Authentication of individual identity</i> .....	14
	3.2.4 <i>on-verified subscriber information</i> .....	14
	3.2.5 <i>Validation of Authority</i> .....	14
	3.2.6 <i>Criteria of interoperation</i> .....	14
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS .....	14
	3.3.1 <i>Identification and authentication for routine re-key</i> .....	14
	3.3.2 <i>Identification and authentication for re-key after revocation</i> .....	14
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST .....	15
<b>4</b>	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>15</b>
4.1	CERTIFICATE APPLICATION.....	15
	4.1.1 <i>Who can submit a certificate application</i> .....	15
	<i>Any user who has completed the enrollment process described in section 4.1.2...</i>	15
	4.1.2 <i>Enrollment process and responsibilities</i> .....	15

4.2	CERTIFICATE APPLICATION PROCESSING .....	15
	4.2.1 <i>Performing identification and authentication functions</i> .....	15
	4.2.2 <i>Approval or rejection of certificate applications</i> .....	16
	4.2.3 <i>Time to process certificate applications</i> .....	16
4.3	CERTIFICATE ISSUANCE.....	16
	4.3.1 <i>CA actions during certificate issuance</i> .....	16
	4.3.2 <i>Notification to subscriber by the CA of issuance of certificate</i> .....	16
4.4	CERTIFICATE ACCEPTANCE.....	16
	4.4.1 <i>Conduct constituting certificate acceptance</i> .....	16
	4.4.2 <i>Publication of the certificate by the CA</i> .....	17
	4.4.3 <i>Notification of certificate issuance by the CA to other entities</i> .....	17
4.5	KEY PAIR AND CERTIFICATE USAGE .....	17
	4.5.1 <i>Subscriber private key and certificate usage</i> .....	17
	4.5.2 <i>Relying party public key and certificate usage</i> .....	17
4.6	CERTIFICATE RENEWAL .....	17
	4.6.1 <i>Circumstance for certificate renewal</i> .....	17
	4.6.2 <i>Who may request renewal</i> .....	17
	4.6.3 <i>Processing certificate renewal requests</i> .....	17
	4.6.4 <i>Notification of new certificate issuance to subscriber</i> .....	17
	4.6.5 <i>Conduct constituting acceptance of a renewal certificate</i> .....	17
	4.6.6 <i>Publication of the renewal certificate by the CA</i> .....	18
	4.6.7 <i>Notification of certificate issuance by the CA to other entities</i> .....	18
4.7	CERTIFICATE RE-KEY.....	18
	4.7.1 <i>Circumstance for certificate re-key</i> .....	18
	4.7.2 <i>Who may request certification of a new public key</i> .....	18
	4.7.3 <i>Processing certificate re-keying requests</i> .....	18
	4.7.4 <i>Notification of new certificate issuance to subscriber</i> .....	18
	4.7.5 <i>Conduct constituting acceptance of a re-keyed certificate</i> .....	18
	4.7.6 <i>Publication of the re-keyed certificate by the CA</i> .....	18
	4.7.7 <i>Notification of certificate issuance by the CA to other entities</i> .....	18
4.8	CERTIFICATE MODIFICATION .....	18
	4.8.1 <i>Circumstance for certificate modification</i> .....	18
	4.8.2 <i>Who may request certificate modification</i> .....	18
	4.8.3 <i>Processing certificate modification requests</i> .....	19
	4.8.4 <i>Notification of new certificate issuance to subscriber</i> .....	19
	4.8.5 <i>Conduct constituting acceptance of modified certificate</i> .....	19
	4.8.6 <i>Publication of the modified certificate by the CA</i> .....	19
	4.8.7 <i>Notification of certificate issuance by the CA to other entities</i> .....	19
4.9	CERTIFICATE REVOCATION AND SUSPENSION .....	19
	4.9.1 <i>Circumstances for revocation</i> .....	19
	4.9.2 <i>Who can request revocation</i> .....	19
	4.9.3 <i>Procedure for revocation request</i> .....	19
	4.9.4 <i>Revocation request grace period</i> .....	19
	4.9.5 <i>Time within which CA must process the revocation request</i> .....	19
	4.9.6 <i>Revocation checking requirement for relying parties</i> .....	19
	4.9.7 <i>CRL issuance frequency</i> .....	20
	4.9.8 <i>Maximum latency for CRLs</i> .....	20
	4.9.9 <i>On-line revocation/status checking availability</i> .....	20
	4.9.10 <i>On-line revocation checking requirements</i> .....	20
	4.9.11 <i>Other forms of revocation advertisements available</i> .....	20
	4.9.12 <i>Special requirements re-key compromise</i> .....	20
	4.9.13 <i>Circumstances for suspension</i> .....	20
	4.9.14 <i>Who can request suspension</i> .....	20
	4.9.15 <i>Procedure for suspension request</i> .....	20

4.9.16	<i>Limits on suspension period</i> .....	20
4.10	CERTIFICATE STATUS SERVICES.....	20
4.10.1	<i>Operational characteristics</i> .....	20
4.10.2	<i>Service availability</i> .....	20
4.10.3	<i>Optional features</i> .....	20
4.11	END OF SUBSCRIPTION.....	21
4.12	KEY ESCROW AND RECOVERY.....	21
4.12.1	<i>Key escrow and recovery policy and practices</i> .....	21
4.12.2	<i>Session key encapsulation and recovery policy and practices</i> .....	21
<b>5</b>	<b>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS</b> .....	<b>21</b>
5.1	PHYSICAL CONTROLS .....	21
5.1.1	<i>Site location and construction</i> .....	21
5.1.2	<i>Physical access</i> .....	21
5.1.3	<i>Power and air conditioning</i> .....	21
5.1.4	<i>Water exposures</i> .....	21
5.1.5	<i>Fire prevention and protection</i> .....	21
5.1.6	<i>Media storage</i> .....	21
5.1.7	<i>Waste disposal</i> .....	21
5.1.8	<i>Off-site backup</i> .....	21
5.2	PROCEDURAL CONTROLS .....	22
5.2.1	<i>Trusted roles</i> .....	22
5.2.2	<i>Number of persons required per task</i> .....	22
5.2.3	<i>Identification and authentication for each role</i> .....	22
5.2.4	<i>Roles requiring separation of duties</i> .....	22
5.3	PERSONNEL CONTROLS.....	22
5.3.1	<i>Qualifications, experience, and clearance requirements</i> .....	22
5.3.2	<i>Background check procedures</i> .....	22
5.3.3	<i>Training requirements</i> .....	22
5.3.4	<i>Retraining frequency and requirements</i> .....	22
5.3.5	<i>Job rotation frequency and sequence</i> .....	22
5.3.6	<i>Sanctions for unauthorized actions</i> .....	22
5.3.7	<i>Independent contractor requirements</i> .....	23
5.3.8	<i>Documentation supplied to personnel</i> .....	23
5.4	AUDIT LOGGING PROCEDURES .....	23
5.4.1	<i>Types of events recorded</i> .....	23
5.4.2	<i>Frequency of processing log</i> .....	23
5.4.3	<i>Retention period for audit log</i> .....	23
5.4.4	<i>Protection of audit log</i> .....	23
5.4.5	<i>Audit log backup procedures</i> .....	23
5.4.6	<i>Audit collection system (internal vs. external)</i> .....	23
5.4.7	<i>Notification to event-causing subject</i> .....	23
5.4.8	<i>Vulnerability assessments</i> .....	23
5.5	RECORDS ARCHIVAL.....	24
5.5.1	<i>Types of records archived</i> .....	24
5.5.2	<i>Retention period for archive</i> .....	24
5.5.3	<i>Protection of archive</i> .....	24
5.5.4	<i>Archive backup procedures</i> .....	24
5.5.5	<i>Requirements for time-stamping of records</i> .....	24
5.5.6	<i>Archive collection system (internal or external)</i> .....	24
5.5.7	<i>Procedures to obtain and verify archive information</i> .....	24
5.6	KEY CHANGEOVER .....	24
5.7	COMPROMISE AND DISASTER RECOVERY.....	24
5.7.1	<i>Incident and compromise handling procedures</i> .....	24

5.7.2	<i>Computing resources, software, and/or data are corrupted</i>	25
5.7.3	<i>Entity private key compromise procedures</i>	25
5.7.4	<i>Business continuity capabilities after a disaster</i>	25
5.8	CA OR RA TERMINATION	25
<b>6</b>	<b>TECHNICAL SECURITY CONTROLS</b>	<b>25</b>
6.1	KEY PAIR GENERATION AND INSTALLATION	25
6.1.1	<i>Key pair generation</i>	25
6.1.2	<i>Private key delivery to subscriber</i>	25
6.1.3	<i>Public key delivery to certificate issuer</i>	25
6.1.4	<i>CA public key delivery to relying parties</i>	25
6.1.5	<i>Key sizes</i>	25
6.1.6	<i>Public key parameters generation and quality checking</i>	25
6.1.7	<i>Key usage purposes (as per X.509 v3 key usage field)</i>	26
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	26
6.2.1	<i>Cryptographic module standards and controls</i>	26
6.2.2	<i>Private key (n out of m) multi-person control</i>	26
6.2.3	<i>Private key escrow</i>	26
6.2.4	<i>Private key backup</i>	26
6.2.5	<i>Private key archival</i>	26
6.2.6	<i>Private key transfer into or from a cryptographic module</i>	26
6.2.7	<i>Private key storage on cryptographic module</i>	26
6.2.8	<i>Method of activating private key</i>	26
6.2.9	<i>Method of deactivating private key</i>	26
6.2.10	<i>Method of destroying private key</i>	26
6.2.11	<i>Cryptographic Module Rating</i>	26
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	26
6.3.1	<i>Public key archival</i>	26
6.3.2	<i>Certificate operational periods and key pair usage periods</i>	27
6.4	ACTIVATION DATA	27
6.4.1	<i>Activation data generation and installation</i>	27
6.4.2	<i>Activation data protection</i>	27
6.4.3	<i>Other aspects of activation data</i>	27
6.5	COMPUTER SECURITY CONTROLS	27
6.5.1	<i>Specific computer security technical requirements</i>	27
6.5.2	<i>Computer security rating</i>	27
6.6	LIFE CYCLE TECHNICAL CONTROLS	27
6.6.1	<i>System development controls</i>	27
6.6.2	<i>Security management controls</i>	27
6.6.3	<i>Life cycle security controls</i>	27
6.7	NETWORK SECURITY CONTROLS	28
6.8	TIME-STAMPING	28
<b>7</b>	<b>CERTIFICATE, CRL, AND OCSP PROFILES</b>	<b>28</b>
7.1	CERTIFICATE PROFILE	28
7.1.1	<i>Version number(s)</i>	28
7.1.2	<i>Certificate extensions</i>	28
7.1.3	<i>Algorithm object identifiers</i>	28
7.1.4	<i>Name forms</i>	28
7.1.5	<i>Name constraints</i>	29
7.1.6	<i>Certificate policy object identifier</i>	29
7.1.7	<i>Usage of Policy Constraints extension</i>	29
7.1.8	<i>Policy qualifiers syntax and semantics</i>	29
7.1.9	<i>Processing semantics for the critical Certificate Policies extension</i>	29

7.2	CRL PROFILE .....	29
	7.2.1 <i>Version number(s)</i> .....	29
	7.2.2 <i>CRL and CRL entry extensions</i> .....	29
7.3	OCSP PROFILE .....	29
	7.3.1 <i>Version number(s)</i> .....	29
	7.3.2 <i>OCSP extensions</i> .....	29
<b>8</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>29</b>
8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT .....	29
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR .....	30
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY .....	30
8.4	TOPICS COVERED BY ASSESSMENT .....	30
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	30
8.6	COMMUNICATION OF RESULTS .....	30
<b>9</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>30</b>
9.1	FEES .....	30
	9.1.1 <i>Certificate issuance or renewal fees</i> .....	30
	9.1.2 <i>Certificate access fees</i> .....	30
	9.1.3 <i>Revocation or status information access fees</i> .....	30
	9.1.4 <i>Fees for other services</i> .....	30
	9.1.5 <i>Refund policy</i> .....	30
9.2	FINANCIAL RESPONSIBILITY .....	30
	9.2.1 <i>Insurance coverage</i> .....	31
	9.2.2 <i>Other assets</i> .....	31
	9.2.3 <i>Insurance or warranty coverage for end-entities</i> .....	31
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION .....	31
	9.3.1 <i>Scope of confidential information</i> .....	31
	9.3.2 <i>Information not within the scope of confidential information</i> .....	31
	9.3.3 <i>Responsibility to protect confidential information</i> .....	31
9.4	PRIVACY OF PERSONAL INFORMATION .....	31
	9.4.1 <i>Privacy plan</i> .....	31
	9.4.2 <i>Information treated as private</i> .....	31
	9.4.3 <i>Information not deemed private</i> .....	31
	9.4.4 <i>Responsibility to protect private information</i> .....	31
	9.4.5 <i>Notice and consent to use private information</i> .....	31
	9.4.6 <i>Disclosure pursuant to judicial or administrative process</i> .....	32
	9.4.7 <i>Other information disclosure circumstances</i> .....	32
9.5	INTELLECTUAL PROPERTY RIGHTS .....	32
9.6	REPRESENTATIONS AND WARRANTIES .....	32
	9.6.1 <i>CA representations and warranties</i> .....	32
	9.6.2 <i>RA representations and warranties</i> .....	32
	9.6.3 <i>Subscriber representations and warranties</i> .....	32
	9.6.4 <i>Relying party representations and warranties</i> .....	32
	9.6.5 <i>Representations and warranties of other participants</i> .....	32
9.7	DISCLAIMERS OF WARRANTIES .....	32
9.8	LIMITATIONS OF LIABILITY .....	32
9.9	INDEMNITIES .....	32
9.10	TERM AND TERMINATION .....	33
	9.10.1 <i>Term</i> .....	33
	9.10.2 <i>Termination</i> .....	33
	9.10.3 <i>Effect of termination and survival</i> .....	33
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .....	33
9.12	AMENDMENTS .....	33
	9.12.1 <i>Procedure for amendment</i> .....	33

9.12.2	<i>Notification mechanism and period</i> .....	33
9.12.3	<i>Circumstances under which OID must be changed</i> .....	33
9.13	DISPUTE RESOLUTION PROVISIONS.....	33
9.14	GOVERNING LAW .....	33
9.15	COMPLIANCE WITH APPLICABLE LAW .....	33
9.16	MISCELLANEOUS PROVISIONS .....	33
9.16.1	<i>Entire agreement</i> .....	33
9.16.2	<i>Assignment</i> .....	33
9.16.3	<i>Severability</i> .....	34
9.16.4	<i>Enforcement (attorneys' fees and waiver of rights)</i> .....	34
9.16.5	<i>Force Majeure</i> .....	34
9.17	OTHER PROVISIONS .....	34

## 1 INTRODUCTION

This document is structured according to RFC 3647 [RFC3647]. Not all sections of RFC 3647 are used. Sections that are not included have a default value of “No stipulation”. This document describes the set of rules and procedures established by TSU (Ivane Javakhishvili Tbilisi State University, Georgia) for the operations of the Georgian Grid Certification Authority (TSU CA) service. The data center housing the TSU CA server is located in Georgian Research and Educational Networking Association GRENA.

This document will include both the Certificate Policy and the Certification Practice Statement for the TSU CA. The general architecture is a single certification authority and several registration authorities.

### 1.1 OVERVIEW

The main goal of TSU CA is to facilitate the needs of the distributed computing in Georgia. TSU CA will work in close cooperation with the Georgian Research and Educational Networking Association GRENA, which is providing GRID services to research and education community of Georgia.

This document describes the set of rules and operational practices that will be used by the TSU CA for issuing certificates.

### 1.2 DOCUMENT NAME AND IDENTIFICATION

Title:	TSU CA Certificate Policy (CP) and Certification Practice Statement (CPS)	
Version:	0.0.0, July 26, 2013	
Expiration:	This document is valid until further notice	
OID assigned:	1.3.6.1.4.1.xxxxx.1.0.0.0	
OID structure:		
	1.3.6.1.4.1	<b>IANA</b>
		iso(1). org(3). dod(6). internet(1). private(4). enterprise(1)
	xxxxx	TSU
	1	TSU CA
	0	CP/CPS
	0	Major CP/CPS version number
	0	Minor CP/CPS version number



### **1.3 PKI PARTICIPANTS**

#### **1.3.1 Certification Authorities**

TSU CA, issues certificates directly to End Entities and does not issue certificates to subordinate Certification Authorities. See section 1.3.3 for further information regarding the scope of the TSU CA.

#### **1.3.2 Registration Authorities**

The procedures of identification and authentication of the certificate applicants are performed by trusted individuals (Registration Authorities), appointed by the TSU CA. At any time the current list of valid Registration Authorities will be available at the TSU CA web site.

#### **1.3.3 Subscribers**

TSU CA issues certificates to Georgian academics and research communities including national or international Grid activities, which require access to the Grid or other Computing Infrastructures. TSU CA issues personal, host and service certificates.

#### **1.3.4 Relying parties**

Users or providers of Computing Infrastructure services that are using the certificates issued by the TSU CA for signature verification and/or encryption, are considered relying parties.

#### **1.3.5 Other participants**

No stipulation.

### **1.4 CERTIFICATE USAGE**

The ownership of a TSU certificate does not imply access to any kind of resources.

#### **1.4.1 Appropriate certificate uses**

Certificates issued by the TSU CA are only valid in the context of research and educational activities.

#### **1.4.2 Prohibited certificate uses**

Any other kind of usage such as financial transactions is strictly forbidden.

### **1.5 POLICY ADMINISTRATION**

#### **1.5.1 Organization administering the document**

Ivane Javakhishvili Tbilisi State University (TSU) and Georgian Research and Educational Networking Association (GRENA) are responsible for the management, registration, maintenance and interpretation of TSU CA. The TSU CA address for operational issues is:

Iv. Javakhishvili Tbilisi State University 1, Chavchavadze Ave.  
0179, Tbilisi Georgia  
Phone: (+995 32) 2251865  
Fax: (+995 32) 2251865  
Email: [grid-ca@grena.ge](mailto:grid-ca@grena.ge)

**1.5.2 Contact Person**

The contact person for questions about this document or any other TSU CA related issues is:

Mikheil Makhviladze  
 Iv. Javakhishvili Tbilisi State University  
 1, Chavchavadze Ave.  
 0179 Tbilisi  
 Georgia

Phone: (+995 32) 2251865  
 Email: [mikheil.makhviladze@tsu.ge](mailto:mikheil.makhviladze@tsu.ge)

Tamar Gogua  
 Iv. Javakhishvili Tbilisi State University  
 1, Chavchavadze Ave.  
 0179 Tbilisi  
 Georgia

Phone: (+995 32) 2222473  
 Fax: (+995 32) 2222473  
 Email: [tamar.gogua@tsu.ge](mailto:tamar.gogua@tsu.ge)

**1.5.3 Person determining CPS suitability for the policy**

The manager of the TSU CA (see 1.5.2) is responsible for determining the CPS suitability for the policy.

**1.5.4 CPS approval procedures**

New versions of the Certification Practice Statement are reviewed internally in order to verify their compliance with the IGTF minimum requirements for “classic X.509 CAs with secure infrastructures”. After a successful internal review the CPS is submitted to the EUGridPMA in order to go through the EUGridPMA accreditation procedure.

**1.6 DEFINITIONS AND ACRONYMS**

**1.6.1 Definitions**

AUTHENTICATION	The process of establishing that individuals or organizations are who they claim to be. This process corresponds to the second process involved in identification.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the

	authentication of electronic data interchange transactions.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.
Certification Authority (CA)	An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole lifetime.
Certification Practice Statement (CPS)	A statement of the practices, which a certification authority employs in issuing certificates.
End Entity (EE)	Subscribers (users, hosts and services) of the TSU CA
Identification	The process of establishing the identity of an individual or organization. It involves two subprocesses in the context of PKI. (1) Establishing that a given name corresponds to a real-world identity and (2) establishing that an individual or organization under that name is in fact the named individual or organization.
IGTF	International Grid Trust Federation
Registration Authority (RA)	An individual or group of people appointed by an organization that is responsible for Identification and Authentication of certificate subscribers, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
TSU	Ivane Javakhishvili Tbilisi State University
GRENA	Georgian Research and Educational Networking Association

## **2 PUBLICATION AND REPOSITORY RESPONSIBILITIES**

### **2.1 REPOSITORIES**

All the on-line and off-line repositories of the TSU CA are operated by TSU in cooperation with the GRENA. The TSU CA contact details for issues regarding the repositories is:

TSU Certification Authority  
1, Chavchavadze Ave.  
0179 Tbilisi  
Georgia  
Phone: (+995 32) 2222473  
Fax: (+995 32) 2222473  
Email: [grid-ca@grena.ge](mailto:grid-ca@grena.ge)

### **2.2 PUBLICATION OF CA INFORMATION**

The TSU CA maintains a secure on-line repository that is available to all Relying Parties through a web interface accessible <http://grid-ca.grena.ge> and which contains:

1. the TSU CA certificate for its signing key;
2. valid issued certificates that reference this policy;
3. the latest CRL;
4. a copy of the current and all previous versions of this document which specifies the CP and CPS;
5. a list with the current operational Registration Authorities;
6. other relevant information relating to certificates that refer to this Policy.

### **2.3 TIME OR FREQUENCY OF PUBLICATION**

Information shall be published promptly to the repository after such information is available to the CA. Certificates issued by the TSU CA, will be published in a searchable repository after the requester has successfully accepted the terms and conditions written in this document. Information relating to the revocation of a certificate will be published as described in section 4.9.7.

### **2.4 ACCESS CONTROL ON REPOSITORIES**

TSU CA does not impose any access control restrictions to the information available at its web site, namely the CA certificate, the latest CRL and all versions of this CP and CPS, under which TSU CA has issued End Entity certificates. The TSU CA web site is maintained in a best effort basis. Excluding disruption of service due to scheduled maintenance and unforeseen failures the site should be available 24×7.

## **3 IDENTIFICATION AND AUTHENTICATION**

### **3.1 NAMING**

#### **3.1.1 Types of names**

The subject names for the certificate applicants shall follow the X.500 standard:

- 1.in case of user certificate the subject name must include the name of the person in the commonName component;
- 2.in case of host certificate the subject name must include the DNS FQDN in the commonName component;
- 3.in case of service certificate the subject name must include the service name and the DNS FQDN separated by a / in the commonName component;

#### **3.1.2 Need for names to be meaningful**

The Subject Name must represent the subscriber in a way that is understandable by humans and must have a reasonable association with the authenticated name of the subscriber.

#### **3.1.3 Anonymity or pseudonymity of subscribers**

TSU CA neither issues nor signs pseudonymous or anonymous certificates.

#### **3.1.4 Rules for interpreting various name forms**

See section 3.1.1.

#### **3.1.5 Uniqueness of names**

The subject name listed in a certificate shall be unambiguous and unique for all end entities to whom certificates have been issued by the TSU CA. In the case of personal or robot certificates, additional numbers or letters may be appended to the real name of the subscriber or robot, when necessary, in order to ensure the uniqueness of the name within the domain of certificates issued by the TSU CA.

#### **3.1.6 Recognition, authentication and role of trademarks**

No stipulation.

### **3.2 INITIAL IDENTITY VALIDATION**

#### **3.2.1 Method to prove possession of private key**

The TSU CA proves possession of the private key that is the companion to the TSU CA root certificate by issuing certificates and signing CRLs. The TSU CA verifies the possession of the private key relating to certificates requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to the requester. A cryptographic challenge-response exchange may be used to prove possession of the private key at any point in time before certification of subscriber. The TSU CA will not generate the key pair on behalf of subscribers and will not accept or retain private keys generated by subscribers.

#### **3.2.2 Authentication of organization identity**

- If an organization wishes to establish an RA they must contact the CA. The CA verifies the eligibility of the organization.
- An organization/unit that wants to get a certificate for a natural person, a server or a service, has to announce this officially to the appropriate RA. The RA has to ascertain

that the organization or organizational unit exists and is entitled (see 1.3.3) to request a TSU certificate.

### **3.2.3 Authentication of individual identity**

Certificate of a person:

The subject should contact personally the RA or CA staff in order to validate his/her identity. The subject authentication is fulfilled by providing an official document for personal identification (ID-card, driving license or a passport), and a valid document proving subject's relation with an institute or organization, declaring that the subject is a valid end entity.

Certificate of a host or service:

Host or service certificates can only be requested by the administrator responsible for the particular host. In order to request a host or service certificate the following conditions must be met:

1. The host must have a valid FQDN.
2. The administrator must already possess a valid personal TSU certificate.
3. The administrator must provide a proof of his or hers relation to the host itself.

The subscriber requesting service from the TSU must present valid documents for personal identification (ID-card, driving license or a passport), and a valid document proving subject's relation with an institute or organization. TSU will archive photocopies of ID documents in case of user certificates and digitally signed e-mails in case of host or service certificates.

### **3.2.4 on-verified subscriber information**

Only information will be verified which is required for the various authentication procedures for the validation of identity (see section 3.2.3). Beyond this requirement, no further information shall be verified.

### **3.2.5 Validation of Authority**

The subscriber requesting services from the TSU CA must present valid documents stating his/her affiliation with the organization.

### **3.2.6 Criteria of interoperation**

No stipulation.

## **3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS**

### **3.3.1 Identification and authentication for routine re-key**

Expiration warnings will be issued to subscribers when re key time arrives. Re key before expiration can be accomplished by sending a re key request via a digitally signed e-mail using the current user certificate and submitting re-key request. Re key after expiration follows the same authentication procedure as requesting a new certificate. Once every five years the user has to be authenticated by an RA.

### **3.3.2 Identification and authentication for re-key after revocation**

After the revocation of a certificate, the subscriber must generate a new key pair in order to request for a new certificate and follow the rules specified in section 3.2.3.

### 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

If an organization wishes to establish an RA they must contact the CA. The CA verifies the eligibility of the organization.

An organization/unit that wants to get a certificate for a natural person, a server or a service, has to announce this officially to the appropriate RA. The RA has to ascertain that the organization or organizational unit exists and is entitled (see 1.3.3) to request a TSU certificate.

If the revocation request is for a host or service certificate, then the e-mail must be signed by the private key corresponding to the certificate of the person responsible of the host or service.

## 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 CERTIFICATE APPLICATION

#### 4.1.1 Who can submit a certificate application

**Any user who has completed the enrollment process described in section 4.1.2**

#### 4.1.2 Enrollment process and responsibilities

Users can enroll to the TSU CA Identity Management System via the TSU CA web portal. During the enrollment process the user is required to provide the following details: first name, last name, organization, e-mail address and telephone number. Upon successful verification of the user's email address, the user is considered to have completed the enrollment process with the TSU CA System. It is the responsibility of the user to keep this information up to date. All users who have successfully enrolled with the TSU CA, are able to submit certificate applications.

**User Certificate:** The users can request to have their public keys signed via the TSU CA website or via e-mail. Upon successful submission of the certificate request, the user receives an email which acknowledges the receipt of the certificate request and which includes a randomly generated hash string which uniquely identifies the certificate request. For the first time and since then at least every 5 years, the subscriber must have his/her identity vetted by the RA serving his/her organization following the procedure described in section 3.2.3. After successfully completing the identity vetting procedure, the RA will approve the certificate request on the TSU CA web portal.

**Server or Service Certificate:** The requester must already be in the possession of a valid certificate, issued by an IGTF accredited CA, before requesting a server or service certificate. The submission of the certificate request will be performed via the TSU CA web portal or via signed e-mail. The certificate request will be forwarded to the RA serving the requester's organization in order to approve or disapprove the request.

### 4.2 CERTIFICATE APPLICATION PROCESSING

#### 4.2.1 Performing identification and authentication functions

For the first time and after that at least once every 5 years, a subscriber must be authenticated by the RA serving his/her organization following the procedure described in section 3.2.3. After successful authentication the RA will approve the certificate request at the TSU CA web portal. If the subscriber requires to re key his/her certificate, then he/she must follow the procedures described in section 4.7.

All certificate applications will be authenticated and validated by the TSU CA and RAs. In the case of a new user certificate, the request will be authenticated by checking if the hash [see section 4.1.2] that the requester has supplied is correct. In all the other cases (re key of user certificate while current certificate is valid, request for host or service certificate) the

authentication of the certificate application will take place by checking that the requester has a valid TSU CA certificate. Upon successful authentication, the certificate application will be forwarded to the RA in order to validate the information included in the certificate request.

#### **4.2.2 Approval or rejection of certificate applications**

The necessary provisions that must be followed in any certificate application request from Georgia in order to be approved:

1. the certificate application must be authenticated first by the RA as described in section 4.2.1;
2. the subject must be an acceptable End Entity, as defined by this Policy;
3. the request must obey the TSU CA distinguished name scheme;
4. the distinguished name must be unambiguous and unique;
5. the private key must be at least 1024 bits long.

If the certificate request does not meet one or more of the above criteria, it will be rejected and signed notification e-mail will be sent by the RA to the subject with carbon copy to e-mail address of the CA.

#### **4.2.3 Time to process certificate applications**

Each certificate application will take no more than 2 working days to be processed.

### **4.3 CERTIFICATE ISSUANCE**

#### **4.3.1 CA actions during certificate issuance**

Right after the subscriber's certificate is issued, an email will be sent to the relevant RA manager informing him/her about the action.

#### **4.3.2 Notification to subscriber by the CA of issuance of certificate**

Right after the subscriber's certificate is issued, an e-mail will be sent to him/her with information on how to download his/her certificate from the TSU CA online repository. In the same e-mail the subscriber will be requested to acknowledge his/her adherence to this policy.

### **4.4 CERTIFICATE ACCEPTANCE**

#### **4.4.1 Conduct constituting certificate acceptance**

The subscriber must log in the TSU CA web portal within 5 working days from the day that his/her certificate was issued and complete the certificate acceptance procedure in which (s)he will be stating that (s)he:

1. has read this policy and accepts to adhere to it;
2. accepts his/her certificate signed by the TSU CA;
3. assumes the responsibility to notify the TSU CA immediately:
  - in case of possible private key compromise;
  - when the certificate is no longer required;
  - when the information in the certificate becomes invalid.

Alternatively the subscriber may complete the certificate acceptance procedure by sending a signed e-mail with 5 working days from the day that his/her certificate was issued in which (s)he will stating what as described above.



#### **4.4.2 Publication of the certificate by the CA**

All the certificates issued by the TSU CA and whose requesters have accepted the terms and conditions of this document, will be published in an on-line repository operated by the TSU CA, which will be accessible via a search web form.

#### **4.4.3 Notification of certificate issuance by the CA to other entities**

The RA that has handled communication with the subscriber will be notified of the certificate issuance.

### **4.5 KEY PAIR AND CERTIFICATE USAGE**

#### **4.5.1 Subscriber private key and certificate usage**

The subscribers' private keys along with the certificates issued by the TSU CA can be used for:

1. email signing/verifying and encryption/decryption (S/MIME);
2. server authentication and encryption of communications;
3. authentication purposes in Grid and other Computing Infrastructures.

#### **4.5.2 Relying party public key and certificate usage**

Relying parties can use the public keys and certificates of the subscribers for:

1. email encryption and signature verification (S/MIME);
2. server authentication and encryption of communications;
3. authentication purposes in Grid and other Computing Infrastructures.

Relying parties must download the CRL at least once a day and implement its restrictions while validating certificates.

### **4.6 CERTIFICATE RENEWAL**

#### **4.6.1 Circumstance for certificate renewal**

TSU CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

#### **4.6.2 Who may request renewal**

TSU CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

#### **4.6.3 Processing certificate renewal requests**

TSU CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

#### **4.6.4 Notification of new certificate issuance to subscriber**

TSU CA will not renew subscribers certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

#### **4.6.5 Conduct constituting acceptance of a renewal certificate**

TSU CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

#### **4.6.6 Publication of the renewal certificate by the CA**

TSU CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

#### **4.6.7 Notification of certificate issuance by the CA to other entities**

TSU CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

### **4.7 CERTIFICATE RE-KEY**

#### **4.7.1 Circumstance for certificate re-key**

Subscribers must generate a new key pair for each certificate they request to be signed by the TSU CA.

#### **4.7.2 Who may request certification of a new public key**

Same as in section 4.1.1

#### **4.7.3 Processing certificate re-keying requests**

Expiration warnings will be issued to subscribers when re key time arrives. Re key before expiration can be accomplished by logging on the TSU CA web portal with their personal certificates and submit a new certificate request or by sending a digitally signed e-mail to the RA serving their organization. Re key after expiration follows the same authentication procedure as for a new certificate. At least once every 5 years the subscriber must go through the same authentication procedure as the one described for a new certificate.

In case the request for re-key a personal certificate is due to revocation or expiration of the existing certificate or compromise of the private key the subscriber must follow the same procedure as for requesting a new certificate.

#### **4.7.4 Notification of new certificate issuance to subscriber**

Same as in section 4.3.2

#### **4.7.5 Conduct constituting acceptance of a re-keyed certificate**

Same as in section 4.4.1

#### **4.7.6 Publication of the re-keyed certificate by the CA**

Same as in section 4.4.2

#### **4.7.7 Notification of certificate issuance by the CA to other entities**

Same as in section 4.4.3

### **4.8 CERTIFICATE MODIFICATION**

#### **4.8.1 Circumstance for certificate modification**

TSU CA does not modify signed End Entity certificates.

#### **4.8.2 Who may request certificate modification**

TSU CA does not modify signed End Entity certificates.

#### **4.8.3 Processing certificate modification requests**

TSU CA does not modify signed End Entity certificates.

#### **4.8.4 Notification of new certificate issuance to subscriber**

TSU CA does not modify signed End Entity certificates.

#### **4.8.5 Conduct constituting acceptance of modified certificate**

TSU CA does not modify signed End Entity certificates.

#### **4.8.6 Publication of the modified certificate by the CA**

TSU CA does not modify signed End Entity certificates.

#### **4.8.7 Notification of certificate issuance by the CA to other entities**

TSU CA does not modify signed End Entity certificates.

### **4.9 CERTIFICATE REVOCATION AND SUSPENSION**

#### **4.9.1 Circumstances for revocation**

A certificate will be revoked in the following circumstances:

1. the subject of the certificate has ceased being an eligible end entity for certification, as described in this policy;
2. the subject does not require the certificate any more;
3. the private key has been lost or compromised;
4. the information in the certificate is wrong or inaccurate;
5. the system or the robot to which the certificate has been issued has been retired;
6. the subject has failed to comply with the rules of this policy.

#### **4.9.2 Who can request revocation**

The revocation of the certificate can be requested by:

1. the certificate owner;
2. any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data.

#### **4.9.3 Procedure for revocation request**

The entity requesting the revocation of a certificate is authenticated by logging on the TSU CA website using a valid TSU CA certificate or by verifying the digital signature in the e-mail request. Otherwise authentication will be performed with the same procedure as described in section 3.2.3.

#### **4.9.4 Revocation request grace period**

No stipulation.

#### **4.9.5 Time within which CA must process the revocation request**

TSU CA will process all revocation requests within 1 working day.

#### **4.9.6 Revocation checking requirement for relying parties**

Relying parts must download the CRL from the online-repository [section 2.2] at least once a day and implement its restrictions while validating certificates.

#### **4.9.7 CRL issuance frequency**

1. CRLs will be published in the on-line repository as soon as issued and at least once every 23 days;
2. The minimum CRL lifetime is 7 days;
3. CRLs are issued at least 7 days before expiration.

#### **4.9.8 Maximum latency for CRLs**

No stipulation.

#### **4.9.9 On-line revocation/status checking availability**

TSU CA operates an on-line repository that contains all the CRLs that have been issued. Promptly following revocation, the CRL or certificate status database in the repository, as applicable, shall be updated.

#### **4.9.10 On-line revocation checking requirements**

Currently there are no on-line revocation/status services offered by the TSU CA.

#### **4.9.11 Other forms of revocation advertisements available**

No stipulation.

#### **4.9.12 Special requirements re-key compromise**

No stipulation.

#### **4.9.13 Circumstances for suspension**

TSU CA does not suspend certificates.

#### **4.9.14 Who can request suspension**

TSU CA does not suspend certificates.

#### **4.9.15 Procedure for suspension request**

TSU CA does not suspend certificates.

#### **4.9.16 Limits on suspension period**

TSU CA does not suspend certificates.

### **4.10 CERTIFICATE STATUS SERVICES**

#### **4.10.1 Operational characteristics**

See section 4.9.9.

#### **4.10.2 Service availability**

The on-line repository is maintained on best effort basis with intended availability of 24x7.

#### **4.10.3 Optional features**

No stipulation.

#### **4.11 END OF SUBSCRIPTION**

No stipulation.

#### **4.12 KEY ESCROW AND RECOVERY**

##### **4.12.1 Key escrow and recovery policy and practices**

No stipulation.

##### **4.12.2 Session key encapsulation and recovery policy and practices**

No stipulation.

### **5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

#### **5.1 PHYSICAL CONTROLS**

##### **5.1.1 Site location and construction**

The TSU CA is hosted at the Georgian Research and Educational Networking Association GRENA.

##### **5.1.2 Physical access**

Physical access to the TSU CA is restricted to authorized personnel only.

##### **5.1.3 Power and air conditioning**

The TSU CA signing machine and the CA web portal are both protected by the Uninterruptible Power Supply and the Power Generator of the Data Center. The Data Center hosting the CA services is equipped with environmental controls that ensure the proper cooling and ventilation.

##### **5.1.4 Water exposures**

Due to the location of the TSU CA facilities, floods are not expected.

##### **5.1.5 Fire prevention and protection**

The Data Center where TSU CA is hosted, is located in a public building adhering to the Georgian laws regarding fire prevention and protection in public buildings.

##### **5.1.6 Media storage**

1. The TSU CA private key is kept in several removable storage media;
2. Backup copies of CA related information may be kept in off-line media such as magnetic tape cartridges, floppies and CD-ROMs.

##### **5.1.7 Waste disposal**

Waste carrying potential confidential information such as magnetic tape cartridges, floppies and CD-ROMs are physically destroyed before being trashed.

##### **5.1.8 Off-site backup**

No off-site backups are currently performed.

## **5.2 PROCEDURAL CONTROLS**

### **5.2.1 Trusted roles**

All employees, contractors, and consultants of the TSU CA (collectively “personnel”) that have access to or control over cryptographic operations that may materially affect the CA’s issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA’s repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA’s operations.

### **5.2.2 Number of persons required per task**

No stipulations.

### **5.2.3 Identification and authentication for each role**

No stipulations.

### **5.2.4 Roles requiring separation of duties**

No stipulations.

## **5.3 PERSONNEL CONTROLS**

### **5.3.1 Qualifications, experience, and clearance requirements**

TSU CA employees meet all requisite requirements with regard to confidentiality, integrity, reliability and professional skills. All employees have general training and qualification in the field of information sciences, and, depending on the role they fulfil, also have in-depth knowledge of the following fields:

- a) IT security technology, cryptography, electronic signatures, PKI,
- b) International standards, technical standards,
- c) National and international law,
- d) Unix/Linux operating systems, TCP/IP networks and relational databases.

### **5.3.2 Background check procedures**

No stipulation.

### **5.3.3 Training requirements**

Internal training is given to TSU CA/RA operators.

### **5.3.4 Retraining frequency and requirements**

TSU CA will perform operational audit of the CA/RA staff at least once per year. If the results of the operational audit are not satisfactory, retraining will be considered.

### **5.3.5 Job rotation frequency and sequence**

No stipulation.

### **5.3.6 Sanctions for unauthorized actions**

No stipulation.

### **5.3.7 Independent contractor requirements**

No stipulation.

### **5.3.8 Documentation supplied to personnel**

Documentation regarding all the operational procedures of the CA is supplied to personnel during the initial training period.

## **5.4 AUDIT LOGGING PROCEDURES**

### **5.4.1 Types of events recorded**

- System boots and shutdowns
- Interactive system logins
- periodic message digests of all system files
- requests for certificates
- identity verification procedures
- certificate issuing
- requests for revocation
- CRL issuing

### **5.4.2 Frequency of processing log**

Audit logs will be processed at least once per month.

### **5.4.3 Retention period for audit log**

Audit logs will be retained for a minimum of 3 years.

### **5.4.4 Protection of audit log**

Only authorized CA personnel is allowed to view and process audit logs. Audit logs are copied to an off line medium.

### **5.4.5 Audit log backup procedures**

Audit logs are copied to an off line medium, which is stored in safe storage.

### **5.4.6 Audit collection system (internal vs. external)**

The audit log accumulation system is internal to the TSU CA.

### **5.4.7 Notification to event-causing subject**

No stipulation.

### **5.4.8 Vulnerability assessments**

No stipulation.

## **5.5 RECORDS ARCHIVAL**

### **5.5.1 Types of records archived**

The following data and files will be archived by the TSU CA

1. all certificate application data, including certification and revocation;
2. all certificates and all CRLs or certificate status records generated;
3. the login/logout/reboot of the issuing machine.

### **5.5.2 Retention period for archive**

Logs will be kept for a minimum of three years.

### **5.5.3 Protection of archive**

Audit logs are copied to an off-line medium, which is stored in safe storage. Online logs are protected by ACLs in the file system used by operating system.

### **5.5.4 Archive backup procedures**

Audit events are copied to an off-line medium.

### **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)**

The archive collection system is internal to the TSU CA.

### **5.5.7 Procedures to obtain and verify archive information**

All certificate data published by TSU CA are publicly available. Data used for the registration and identification of subscribers are for internal use only. The integrity of TSU CA archives is verified:

- at the time the archive is prepared
- at the time of a programmed security audit
- at any other time when a full security audit is required.

## **5.6 KEY CHANGEOVER**

The CA's private signing key is changed periodically; from that time on only the new key will be used for certificate signing purposes. The overlap of the old and new key will be at least 1 year. For this overlapping period, the older but still valid certificate along with the corresponding private key will be available in order to verify digital signatures and issue CRLs.

## **5.7 COMPROMISE AND DISASTER RECOVERY**

### **5.7.1 Incident and compromise handling procedures**

If the CA private key is compromised or destroyed the CA will:

1. Notify subscribers, RAs and cross-certifying CAs;
2. Terminate the issuance and distribution of certificates and CRLs;
3. Notify relevant security contacts.



### **5.7.2 Computing resources, software, and/or data are corrupted**

No stipulation.

### **5.7.3 Entity private key compromise procedures**

No stipulation.

### **5.7.4 Business continuity capabilities after a disaster**

No stipulation.

## **5.8 CA OR RA TERMINATION**

Upon termination the TSU CA will:

1. Notify subscribers, RAs and cross-certifying CAs;
2. Terminate the issuance and distribution of certificates and CRLs;
3. Notify relevant security contacts;
4. Notify as widely as possible the end of the service.

## **6 TECHNICAL SECURITY CONTROLS**

### **6.1 KEY PAIR GENERATION AND INSTALLATION**

#### **6.1.1 Key pair generation**

Key pairs for CAs, RAs and subscribers must be generated in such a way that private key is not known by any other than the owner of the key pair. Each subscriber must generate his/her own key pair. TSU CA does not generate private keys on behalf of the subscribers.

#### **6.1.2 Private key delivery to subscriber**

The TSU CA does not generate private keys, hence does not deliver private keys.

#### **6.1.3 Public key delivery to certificate issuer**

The subscriber's public key must be transferred to the TSU CA in a way that ensures that it has not been altered.

#### **6.1.4 CA public key delivery to relying parties**

CA certificate can be downloaded from the TSU CA web site.

#### **6.1.5 Key sizes**

1. The minimum key length for an End Entity certificate is 1024 bit.
2. The minimum length for the TSU CA private key is 2048 bits.

#### **6.1.6 Public key parameters generation and quality checking**

No stipulation.

### **6.1.7 Key usage purposes (as per X.509 v3 key usage field)**

Keys may be used for authentication, non-repudiation, data encipherment, message integrity and session establishment. Certificates and CRLs are signed by the CA private key.

## **6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

### **6.2.1 Cryptographic module standards and controls**

No stipulation.

### **6.2.2 Private key (n out of m) multi-person control**

No stipulation.

### **6.2.3 Private key escrow**

No stipulation.

### **6.2.4 Private key backup**

The TSU CA private key is kept in encrypted form in media storage as described in section 5.1.6. All media is located in safe places where access is restricted to authorized personnel only.

### **6.2.5 Private key archival**

TSU CA does not archive private keys.

### **6.2.6 Private key transfer into or from a cryptographic module**

TSU CA does not use any kind of cryptographic module.

### **6.2.7 Private key storage on cryptographic module**

TSU CA does not use any kind of cryptographic module.

### **6.2.8 Method of activating private key**

The private key of the TSU CA is activated by using a pass phrase. See section 6.4.1.

### **6.2.9 Method of deactivating private key**

No stipulation.

### **6.2.10 Method of destroying private key**

No stipulation.

### **6.2.11 Cryptographic Module Rating**

No stipulation.

## **6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT**

### **6.3.1 Public key archival**

No stipulation.

### **6.3.2 Certificate operational periods and key pair usage periods**

All certificates issued to subscribers by the TSU CA will have a maximum lifetime of 1 year. The lifetime of the TSU CA root certificate must be no more than 10 years and no less than 2 years.

## **6.4 ACTIVATION DATA**

### **6.4.1 Activation data generation and installation**

TSU CA does not generate activation data for subscribers. It's upon the subscriber to generate a secure pass phrase, at least 12 characters long, in order to be used as activation data for his/her private key.

The pass phrase used to activate the TSU CA private key is generated on the computer used for the CA signing operations and must be at least 15 characters long. Every 180 days the pass phrase is regenerated by one of the TSU CA Operators.

### **6.4.2 Activation data protection**

- The subscriber is responsible to protect the activation data for his/her private key.
- The TSU CA uses a pass phrase to activate its private key, which is known only by the TSU CA Manager and the TSU CA Operators. A copy of the pass phrase in written form is sealed in an envelope and kept in a safe. Access to the safe is restricted only to the TSU CA Manager and Operators. Old activation data is destroyed according to current best practices.

### **6.4.3 Other aspects of activation data**

Not defined.

## **6.5 COMPUTER SECURITY CONTROLS**

### **6.5.1 Specific computer security technical requirements**

1. The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;
2. active monitoring is performed to detect unauthorized software changes;
3. CA systems configuration is reduced to the bare minimum;
4. the signing machine is kept powered off between uses;
5. the signing machine is not connected to any kind of networks.

### **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**

No stipulation.

## 6.7 NETWORK SECURITY CONTROLS

1. The CA signing machine is kept off-line;
2. CA/RA machines other than the signing machine are protected by a firewall;
3. Passive monitoring is performed in order to detect malicious network activity.

## 6.8 TIME-STAMPING

No stipulation.

## 7 CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1 CERTIFICATE PROFILE

#### 7.1.1 Version number(s)

All certificates that reference this Policy will be issued in the X.509 version 3 format and will include a reference to the O.I.D. of this Policy within the appropriate field.

#### 7.1.2 Certificate extensions

End Entity certificates:

1. Basic constraints (Critical): Not a CA.
2. Key usage (Critical): Digital signature, key encipherment, data encipherment.
3. Subject key identifier
4. Authority key identifier
5. Subject alternative name
6. Issuer alternative name
7. CRL distribution points
8. Certificate policies

#### 7.1.3 Algorithm object identifiers

1. Hash Function: id-sha1 1.3.14.3.2.26
2. RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
3. Signature Algorithm: sha1WithRSAEncryption 1.2.840.113549.1.1.5

#### 7.1.4 Name forms

Issuer:C=GE

O=TSU

CN=TSU-CA

Subject:C=GE

O=INSTITUTE,

CN=SUBJECT NAME

### **7.1.5 Name constraints**

Subject attribute constraints:

**Country:** Must be “GE” .

**Organization:** Must be the name of the institute of the subject.

**CommonName:** First name and last name of the subject for user certificates, DNS FQDN for server or service certificates. In the latter case the DNS FQDN may be prefixed by the value 'host' or the service name separated with a '/' from the DNS FQDN.

### **7.1.6 Certificate policy object identifier**

TSU CA identifies this policy with the object identifier (O.I.D) specified in section 1.2.

### **7.1.7 Usage of Policy Constraints extension**

No stipulation.

### **7.1.8 Policy qualifiers syntax and semantics**

No stipulation.

### **7.1.9 Processing semantics for the critical Certificate Policies extension**

No stipulation.

## **7.2 CRL PROFILE**

### **7.2.1 Version number(s)**

All CRLs will be issued in X.509 version 2 format.

### **7.2.2 CRL and CRL entry extensions**

No stipulation

## **7.3 OCSP PROFILE**

No stipulation.

### **7.3.1 Version number(s)**

No stipulation.

### **7.3.2 OCSP extensions**

No stipulation.

## **8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

### **8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT**

The TSU CA may be audited by other trusted CAs to verify its compliance with the rules

and procedures specified in this document. Any costs associated with such an audit must be covered by the requesting party.

## **8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR**

No stipulation

## **8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY**

No stipulation

## **8.4 TOPICS COVERED BY ASSESSMENT**

No stipulation

## **8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY**

No stipulation

## **8.6 COMMUNICATION OF RESULTS**

No stipulation

# **9 OTHER BUSINESS AND LEGAL MATTERS**

## **9.1 FEES**

### **9.1.1 Certificate issuance or renewal fees**

No fees shall be charged.

### **9.1.2 Certificate access fees**

No fees shall be charged.

### **9.1.3 Revocation or status information access fees**

No fees shall be charged.

### **9.1.4 Fees for other services**

No fees shall be charged.

### **9.1.5 Refund policy**

No fees shall be charged.

## **9.2 FINANCIAL RESPONSIBILITY**

TSU CA denies any financial responsibilities for damages or impairments resulting from its operation.

**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**

No stipulation.

**9.4 PRIVACY OF PERSONAL INFORMATION**

TSU CA does not collect any confidential or private information.

**9.4.1 Privacy plan**

No stipulation.

**9.4.2 Information treated as private**

No stipulation.

**9.4.3 Information not deemed private**

TSU CA collects the following information which is not deemed as private:

1. subscriber's e-mail address;
2. subscriber's name;
3. subscriber's organization;
4. subscriber's certificate;

subscriber's work phone number.

**9.4.4 Responsibility to protect private information**

TSU CA has no responsibility to protect private information as all the information it collects is public.

**9.4.5 Notice and consent to use private information**

No stipulation.

#### **9.4.6 Disclosure pursuant to judicial or administrative process**

No stipulation.

#### **9.4.7 Other information disclosure circumstances**

No stipulation.

### **9.5 INTELLECTUAL PROPERTY RIGHTS**

RFC 3647;

### **9.6 REPRESENTATIONS AND WARRANTIES**

#### **9.6.1 CA representations and warranties**

No stipulation.

#### **9.6.2 RA representations and warranties**

No stipulation.

#### **9.6.3 Subscriber representations and warranties**

No stipulation.

#### **9.6.4 Relying party representations and warranties**

No stipulation.

#### **9.6.5 Representations and warranties of other participants**

No stipulation.

### **9.7 DISCLAIMERS OF WARRANTIES**

TSU CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

### **9.8 LIMITATIONS OF LIABILITY**

1. TSU CA guarantees to control the identity of the certification requests according to the procedures described in this document;
2. TSU CA guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. TSU CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates ;
4. TSU CA denies any kind of responsibilities for damages or impairments resulting from its operation.

### **9.9 INDEMNITIES**

No stipulation.



## **9.10 TERM AND TERMINATION**

### **9.10.1 Term**

No stipulation.

### **9.10.2 Termination**

No stipulation.

### **9.10.3 Effect of termination and survival**

No stipulation.

## **9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS**

No stipulation.

## **9.12 AMENDMENTS**

### **9.12.1 Procedure for amendment**

No stipulation.

### **9.12.2 Notification mechanism and period**

No stipulation.

### **9.12.3 Circumstances under which OID must be changed**

No stipulation.

## **9.13 DISPUTE RESOLUTION PROVISIONS**

Legal disputes arising from the operation of the TSU CA will be resolved according to the Georgian Law.

## **9.14 GOVERNING LAW**

The enforceability, construction, interpretation, and validity of this policy shall be governed by the Georgian Law.

## **9.15 COMPLIANCE WITH APPLICABLE LAW**

No stipulation.

## **9.16 MISCELLANEOUS PROVISIONS**

### **9.16.1 Entire agreement**

No stipulation.

### **9.16.2 Assignment**

No provisions.

**9.16.3 Severability**

No stipulation.

**9.16.4 Enforcement (attorneys' fees and waiver of rights)**

No stipulation.

**9.16.5 Force Majeure**

No stipulation.

**9.17 OTHER PROVISIONS**

No stipulation.