"SECURITY SOLUTION SERVICE GRID TECHNOLOGY TEAM" CERTIFICATION AUTHORITY (SSSCA)

Certificate Policy

and

Certificate Practices Statements

Ver. 1.0

March 03, 2010

Grid Technology Team,
Security Solution Service LLC (SSS CA), Mongolia

Version history

Version	Author	Participator	Date	Comment
1.0	Esbold Unurkhaan	Khaltar Togtuun	2010.03.03	Initial document

1. INTRODUCTION

1.1 Overview

- Grid Technology Team of SSS (SSSCA), is the branch of Security Solution, Service LLC in Mongolia. Grid Technology Team operates a Certification Authority called SSS Certification Authority (CA) for Grid PKI services.
- This document is structured according to the RFC3647.
- Not all sections of RFC3647 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 the Grid Technology Team of SSS (SSS CA) for the operations of the SSSCA PKI service.
- This document will include both the Certificate Policy and the Certificate Practice Statement for the SSSCA which is a traditional X.509 Public Key Certificate
- An intent of the SSSCA is to issue identity and service certificates for use in grid.

1.1.1 Type of Certificates

SSSCA issues following types of certificates.

- ✓ Clients for identification
- ✓ Host certificate
- ✓ Web servers

1.2 Document name and identification

Document Title: **SSSCA Certificate Policy and Certificate Practices Statements**
Document Version : **1.0**
Document Date : **March 03, 2010**
Last Update Date: **until next version**

The OID is constructed as shown in the table below:

Table 1.1 The OID

OID	Object
1.3.6.1.4.1.55555	SSS GRID PMA (from IANA)
1.3.6.1.4.1.55555.1.1	SSS Grid Technology Team CA (SSSCA)
1.3.6.1.4.1.55555.1.1.1.0	Certification Practices Statements
1.3.6.1.4.1.55555.1.1.2	CA Certificate Policy
1.3.6.1.4.1.55555.1.1.2.1.0	Server CP
1.3.6.1.4.1.55555.1.1.2.2.0	Clients CP

1.3 PKI participants

SSSCA provides certificates for grid users and infrastructure, and community that are involved in Grid activities.

1.3.1 Certification authorities

No certificates will be issued to subordinate CAs.

1.3.2 Registration authorities

SSSCA manages the functions of its Registration Authority. Additional RA's may be created as required.

1.3.3 Subscribers

End Entities serviced by this PKI are any actors (people, machines, software) involved in SSSCA infrastructure activities. In practice these are computer systems, staffs from associated entities.

1.3.4 Relying parties

Users that are using the public keys in certificates issued by the SSSCA for signature verification and/or encryption, will be considered as relying parties.

1.3.5 Other participants

No stipulation

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued by the SSSCA may be used for applications suitable for X.509 certificates, e.g. Email signing and encryption, authentication and encryption of communications, authentication of users, hosts and services etc.

1.4.2 Prohibited certificate uses

No stiptulation

1.5 Policy administration

1.5.1 Organization administering the document

The SSSCA is responsible for the registration, maintenance, and interpretation of this CP/CPS.

1.5.2 Contact person

Dr. Khaltar Togtuun
Grid Technology Team,
Security Solution Service LLC
National Information Technology Park, 323. Sukhbaatar district, Ulaanbaatar, 13341, Mongolia.
Tel: +976-70113151
Fax: +976-11-450598
Email: info@sssmn.com
Url: www.sssmn.com/ca/

1.5.3 Person determining CPS suitability for the policy

The SSSCA general manager is responsible for determining the CPS suitability for the policy.

1.5.4 CPS approval procedures

The decision relates to the management of SSSCA will be performed by the coordinate committee called “SSS GRID Policy Management Authority (SSS GRID PMA)”, which consists of representatives of SSS Company
The SSS GRID PMA will be responsible for:

- Approve changed CP/CPS and submit it to ApgridPMA,
- Take countermeasure for compromise of the Certificate Authority(CA)’s private key,
- Take countermeasure for Emergency operations in disaster,
- Other Important matters.

1.6 Definitions and acronyms

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

Web server certificates can be used to identify a web server and for encryption of communication (SSL/TLS).
Host certificates can be used to identify a specific host and for encryption of communication (SSL/TLS)
SSS Grid PMA – SSS Policy Administration Authority is established by the SSS Steering Committee and consists 3 persons including SSSCA general manager.
SSSCA- SSS Certificate Authority includes both Certificate Authority and Registration Authority

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The online repository of information from the SSSCA is accessible at the URI http://www.sssmn/ca

2.2 Publication of certification information

The SSSCA shall maintain a web server for public access and web site includes followings:

- The SSSCA root certificate, and all previous ones necessary to check still valid certificates
- The certificates issued by the PKI
- A Certificate Revocation List
- A copy of the most recent version of this policy and all previous versions
- The official contact e-mail address and physical contact address
- Other relevant information to the SSSCA service

2.3 Time or frequency of publication

Certificates will be published as soon as they are issued.
CRLs are issued immediately, within one working day, after every certificate revocation or 7 days before expiration.
New versions of CP/CPS will be published as soon as they have been approved.

2.4 Access controls on repositories

The information on the SSSCAweb site are accessible without any restriction. If misuse of the data is evident, access controls may been acted inorder to protect the owners of certificates. Web site maintenance period take 1 hour per week and schedule will be published on this website and during maintenance time blocked any access.

3. IDENTIFICATION AND AUTHENTICATION (11)

3.1 Naming

3.1.1 Types of names

The subject names for the certificate applicants shall follow the X.509 standard:

a) In case of personal certificate the subject name must include the person's full name.
b) In case of host/server certificate the subject name must include the FQDN of the host/server.

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of subscribers

SSSCA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

a) Each entity has a clear and unique Distinguished Name in the certificate subject field.
b) Any name under this document will have "C=MN, O=SSSCA". The subscribers class, defined as "people" or "host" shall be attached in the form "O=Grid Team". The "people" class will contain certificates for subscribers that are natural persons. The "host" class will contain certificates for subscribing entities that are automated systems or applications.
c) For a user certificate the common name (CN) name must be the full name of the subscriber.
d) In case the subscriber belongs to the "host class" the subject name must be the FQDN of the host/server.

3.1.5 Uniqueness of names

The name listed in a certificate shall be unambiguous and unique for all certificates issued by the SSSCA. If the name presented by the subscriber is not unique, additional numbers or letters may be appended to the name to ensure uniqueness. Certificates must apply to unique individuals or resources. Users must not share certificates.

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

SSSCA confirms the possession of a private key by verification of the CSR signature.

3.2.2 Authentication of organization identity

SSSCA shall verify the requesting party's certificate issued by Mongolian National Registration Authority.

3.2.3 Authentication of individual identity

Certificates will be issued to Subscribers of the SSSCA. The process used to establish an individual's identity and their appropriateness to have a certificate.

3.2.4 Non-verified subscriber information

No stipulation

3.2.5 Validation of authority

See section 3.2.2 & 3.2.3

3.2.6 Criteria for interoperation

No stipulation

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Enrollment request is necessary if the certificate is expired or rekey. The SSSCA will send enrollment reminders at least a month before expiration. End-entity certificates must be rekeyed after ….. years and renewed after … years. After expiration of the certificate no rekey is possible; a new application for Initial registration must be made instead.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a key, no re-key is possible. A new application for initial registration must be made.

3.4 Identification and authentication for revocation request

Revocation request is confirmed that user and organization is authenticated by certificates issued based on this CPS. (see section 3.2.2 & 3.2.3)

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Below is a list of people who may submit certificate applications

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity

4.1.2 Enrollment process and responsibilities

Users need to create a key pair on user's machine according to the procedures described in "SSSCA Enrollment Manual", then send a certificate signing request which contains the public key to the RA server on-line. Communication path to this enrollment is encrypted using SSL. Detailed instruction for certificate enrollment is described in "SSSCA Enrollment Manual" which is available on the SSSCA web site.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Users must present application form to the RA by hand-written paper and register it RA office of SSSCA.

4.2.2 Approval or rejection of certificate applications

RA examines the request according to this document [3.2.2 and 3.2.3]. If the application is approved, then the RA will inform the SSSCA that the request has been approved.

RA will reject when subscriber information in terms of section 3.2 cannot be completed

4.2.3 Time to process certificate applications

After the verification of the certificate request has been completed, the certificate is issued. In normal case, this will not take more than five (05) working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CSR shall be transferred to the computer which holds the private key of SSSCA and which is not connected to any network. On this system the certificate is created and signed. The signed certificate shall then be transferred back to the SSSCA online server.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The SSSCA shall then send the certificate to the requesting party in an e-mail signed by the SSSCA agent's certified private key. It shall also send an acknowledgement of the issuance to the appropriate RA.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Upon receipt of the e-mail with the certificate the requesting party shall check the signature of the e-mail. He/she shall then sign an arbitrary file with his/her private key and check the signature with the returned certificate and/or encrypt a

file using the public key of the certificate and decrypting it with the private key. The requesting party shall notify the SSSCA of the result of the check for

useability of the certificate in conjunction with the private key in its possession.
If it was successful and there are no objections to other aspects of the certificate,
the subscriber must in form the SSSCA and the appropriate RA that he/she accepts the certificate. In case of rejection of the certificate, the requesting
party must in form the CA and the RA of the rejection and explain the reasons.
Certificates whose acceptance have not been confirmed within a month shall be
revoked by the SSSCA.

4.4.2 Publication of the certificate by the CA
Upon receipt of a certificate acceptance the SSSCA shall make available the certificate on its repository (see2.1).

4.4.3 Notification of certificate issuance by the CA to other entities
SSSCA does not notify any other entities about a certificate issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage
Certificates issued by the SSSCA and their associated private keys must only be used according to the permissions stated in section 1.4.1. They must only be used according to the key usage fields of the certificate. When a certificate is revoked or has expired the associated private key shall not be used anymore.

4.5.2 Relying party public key and certificate usage
A relying party must, upon being presented with a certificate issued by the SSSCA check
a) its validity by
- checking that it trusts the CA that issued the certificate,
- checking that the certificate hasn't expired,
- consulting the SSSCA CRL in effect at the time of use of the certificate.

b) the appropriate usage as outlined in the CP pointed to by the certificate and in
the usage keys included in the certificate.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal
SSSCA will not renew subscribers certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.2 Who may request renewal
See section 4.6.1

4.6.3 Processing certificate renewal requests
See section 4.6.1

4.6.4 Notification of new certificate issuance to subscriber
See section 4.6.1

4.6.5 Conduct constituting acceptance of a renewal certificate
See section 4.6.1

4.6.6 Publication of the renewal certificate by the CA
See section 4.6.1

4.6.7 Notification of certificate issuance by the CA to other entities
See section 4.6.1

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key
Subscribers must regenerate their key pair in the following circumstances:
a) expiration of their certificate signed by the SSSCA;
b) revocation of their certificate by the SSSCA;
c) compromise of their private key.
d) change in the certificate parameters.

4.7.2 Who may request certification of a new public key
The owner of a valid SSSCA certificate may request the certification of a new public key.

4.7.3 Processing certificate re-keying requests
Upon receipt of the request endorsed by the appropriate RA, the SSS CA shall process the renewal as it processes an initial certification request.

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
Certificates must not be modified. The old certificate must be revoked, and a new key pair must be generated and a request for the modified certificate contents must be submitted with the new public key.

4.8.2 Who may request certificate modification
Not applicable.

4.8.3 Processing certificate modification requests
Not applicable.

4.8.4 Notification of new certificate issuance to subscriber
Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate
Not applicable.

4.8.6 Publication of the modified certificate by the CA
Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities
Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation
A certificate must be revoked if:

a) its associated private key has been (or is suspected to be) compromised or lost
b) its contents have become or proved to be inaccurate
c) it is not needed any more
d) the consenting organisation/unit withdraws its consent

Should the private key of the SSSCA be compromised or lost all certificates signed with it shall be revoked.

4.9.2 Who can request revocation
A certificate revocation can be requested by

a) the owner of the certified key
b) the SSSCA or any RA that has proof of a compromise
c) the organization that wants to revoke its consent to its inclusion in the certificate

4.9.3 Procedure for revocation request
Revocation request must be made by the owner of the certificate, properly authenticated, using the online revocation facilities. In case of emergency, the owner of the certificate must go to the RA as soon as possible and ask the appropriate RA to request revocation.
Before revoking a certificate the SSSCA shall authenticate the source of the request by using signed e-mails.

4.9.4 Revocation request grace period
There is no grace period defined for a revocation request. The SSSCA shall process the authenticated request with priority and publish the revocation as fast as possible.

4.9.5 Time within which CA must process the revocation request
The SSSCA time for processing revocation request is within one working day normally.

4.9.6 Revocation checking requirement for relying parties
Before using a certificate the relying party must validate it against the CRL most recently published in the SSSCA repository.

4.9.7 CRL issuance frequency (if applicable)
A new CRL is published in the SSSCA repository after every certificate revocation and at least 7 days before the expiration of the previous CRL.

4.9.8 Maximum latency for CRLs (if applicable)
The CRL shall be copied to a removable device immediately after creation on the offline CA system and transferred without delay to the on-line repository.

4.9.9 On-line revocation/status checking availability
The latest CRL is always available from the SSSCA web site. The SSSCA shall publish the CRL in effect in its repository (see 2.1). No other on-line checking is available now.

4.9.10 On-line revocation checking requirements
Relying parties must check the CRL before they use and trust certificate. No access control shall limit the possibility to check the CRL.

4.9.11 Other forms of revocation advertisements available
Currently no other forms of revocation advertisements are available.

4.9.12 Special requirements re key compromise
No stiptulation.

4.9.13 Circumstances for suspension
Not defined.

4.9.14 Who can request suspension
Not defined.

4.9.15 Procedure for suspension request
Not defined.

4.9.16 Limits on suspension period
Not defined.

4.10 Certificate status services

4.10.1 Operational characteristics
The SSSCA shall store in its public repository and make them available via its web site:

- the root CA certificate
- all valid certificates, and
- the most up-to-date CRL

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
The subscription ends with the expiry of the certificate if it is not renewed before that date. A subscription may end earlier if the subscriber requests a revocation of it's certificate.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices
No key escrow or recovery services are provided. The key owner must take all
steps to prevent a loss.

4.12.2 Session key encapsulation and recovery policy and practices
See Section 4.12.1.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The SSSCA is located at the address of the organization administering this document (see section 1.5.1).

5.1.2 Physical access

SSSCA machines are in a controlled environment where access is restricted to authorized personnel.

5.1.3 Power and air conditioning

The server room hosting the offline and the online SSSCA servers have air conditioning. The servers are powered via a UPS that allows to bridge power out ages of one hour.

5.1.4 Water exposures

No special exposures.

5.1.5 Fire prevention and protection

Fire alarm system installed in machine room regarding Mongolian law.

5.1.6 Media storage

Removable media shall be made duplication and stored in locked safe places to which only authorized personnel have access.

5.1.7 Waste disposal

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

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural controls

5.2.1 Trusted roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be Trusted Persons serving in a Trusted Position.

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

All SSSCA personnel shall have system administrator or analyst experience.

5.3.2 Background check procedures
Currently no stipulation.

5.3.3 Training requirements
Internal training is given to SSSCA CA/RA operators.

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

5.3.5 Job rotation frequency and sequence
No stipulation.

5.3.6 Sanctions for unauthorized actions
The SSSCA reserves the right to prosecute unauthorized actions to the extend provided by the provisions of the Mongolian law.

5.3.7 Independent contractor requirements
No stipulation.

5.3.8 Documentation supplied to personnel
All SSSCA personnel shall be provided with all documentation required for successfully performing their task.

5.4 Audit logging procedures

5.4.1 Types of events recorded
The following events shall be recorded:

a) SSSCA host
- login / logout / reboot
- creation and signing of certificates
  revocation of certificates
- boot and shutdown

b) SSSCA web online server
- receipt of certificate request
- issued certificates
- receipt of certificate revocation request
- validation of certificate request from RA
- revocation of certificate
- CRL issues

5.4.2 Frequency of processing log
The log files shall be analyzed once a month, or after a potential security breach is suspected or known; whichever comes first.

5.4.3 Retention period for audit log
The minimal retention period for the audit log is 3 years.

5.4.4 Protection of audit log

The audit logs shall only be accessible to the SSSCA operators and managers.

5.4.5 Audit log backup procedures
The audit logs shall be backed-up on a removable medium every night except on weekends and holidays when no activity happens on the offline host and only read access to the online repositories happens on the online server.

5.4.6 Audit collection system (internal vs. external)
The audit log accumulation system is internal to the SSSCA.

5.4.7 Notification to event-causing subject
Not defined.

5.4.8 Vulnerability assessments
Not defined.

5.5 Records archival

5.5.1 Types of records archived
See section 5.4.1

5.5.2 Retention period for archive
The minimum retention period is 3 years.

5.5.3 Protection of archive
The archive shall be accessible to the SSSCA operation and management personnel only.

5.5.4 Archive backup procedures
Records shall be backed up on removable media, which shall be stored in a room with restricted access.

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 SSSCA.

5.5.7 Procedures to obtain and verify archive information
Not defined.

5.6 Key changeover
To avoid interruption of validity of subordinate keys, the new ca private key is generated one year before the expiration of the old key. The new public key is available on the on-line repository, and new certificates can be issued.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

a) If the keys of an end entity are lost or compromised due to corruption of their computing basis, the appropriate RA must be informed immediately in order to start the certificate revocation process.

b) If an RA Operator' s private key is compromised or suspected to be compromised, the RA Operator or Manager must inform the CA and request the revocation of the RA Operator' s certificate.
c) If the CA' s private key is (or suspected to be) compromised, the CA will:
    - Inform the Registration Authorities, subscribers, relying parties, and cross-certifying CAs of which the CA is aware
    - Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key

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

The 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 CA is
corrupted, the following steps shall be performed:

- All CA software shall be backed-up on removable media after a new release of any of its components is installed.
- All data files of the offline CA shall be backed-up on a removable medium after each change, before the session is closed.

If any part of the running system is corrupted, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a readonly medium and estimated to be uncorrupted. If not all encrypted copies of the SSSCA private key are destroyed or lost, and are not compromised, the operation shall be re-established as soon as possible without need to revoke all issued certificates.

5.7.3 Entity private key compromise procedures

In case the key of an end entity or an RA is compromised, the corresponding certificate must be revoked. All relying parties known to accept the key should b informed by the owner of the key.
In case the private key of the SSSCA is compromised (or suspected to be), the CA shall:

- make every reasonable effort to notify subscribers and RAs,
- terminate issuing and distributing certificates and CRLs,
- request revocation of the compromised certificate,
- generate a new CA key pair and certificate and publish the certificate in the repository,
- revoke all certificates signed using the compromised key, and
- publish the new CRL on the SSSCA repository.

5.7.4 Business continuity capabilities after a disaster

Not defined.

5.8 CA or RA termination

Before SSSCA terminates its services, it will:

- Inform the RAs, subscribers and relying parties the CA is aware;
- Inform the APGridPMA;
- Make information of its termination widely available;
- Stop issuing certificates

- Revoke all certificates
- Issue an publish CRL
- Destroy its private keys and all copies

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for the SSSCA is generated by authorized CA staff on a computer which is not connected to the network. The keys are generated by dedicated software. The key pairs for natural-person (including RA agents), host or service certificates are generated by the requesting parties themselves on their system.

6.1.2 Private key delivery to subscriber

Each subscriber must generate his/her own key pair. The CA does not generate private keys for its subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribers public keys are delivered to the issuing CA by the HTTPS protocol via the SSSCA web interface.

6.1.4 CA public key delivery to relying parties

The SSSCA certificate can be downloaded from the repository(see 2.1).

6.1.5 Key sizes

Keys of length less than 1024 bits are not accepted. The SSSCA key is of length 2048 bits.

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:

a) With an end-entity certificate for
- authentication
- non-repudiation
- data and key encipherment
- message integrity
- session establishment
- proxy creation and signing

b) With the self-signed CA certificate
- certificate signing
- CRL signing

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

CA private key is protected by HSM compliant with FIPS140-1 Level 3. The encrypted

private key shall be stored on the offline computer of the SSSCA.

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

This CA and its subsidiaries do not yet support private key (n out of m) muti-person control. But the SSSCA implements multi-person control for the access to the CA

server as described in 5.1.2. Backup copy of the CA's private key is under (2 out of 3) multi-person control.

6.2.3 Private key escrow
No stipulation.

6.2.4 Private key backup
The SSSCA root private key is kept encrypted in removable devices and the removable devices are protected in a safebox located in SSS machine room (CP/CPS 5.1.2).

6.2.5 Private key archival
The SSSCA private key is kept encrypted in removable devices and the removable devices are protected in a safebox located in SSS machine room (CP/CPS 5.1.2).

6.2.6 Private key transfer into or from a cryptographic module
No stipulation

6.2.7 Private key storage on cryptographic module
No stipulation

6.2.8 Method of activating private key
The CA private key is activated is done by providing the passphrase.

6.2.9 Method of deactivating private key
The plain private key shall only be stored in RAM and erased when the activity for which it is needed is finished.

6.2.10 Method of destroying private key
See section 6.2.9

6.2.11 Cryptographic Module Rating
No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival
The CA archives all issued certificates on removable media that is stored offline in a secure vault.

6.3.2 Certificate operational periods and key pair usage periods
There is no stipulation as to the validity of the generated key pair. Only the validity of the certificate issued by the SSSCA is defined by this CP/CPS document. Subscribers' certificates have a validity period of one year and the CA certificate has a validity period of 5 years.

6.4 Activation data

6.4.1 Activation data generation and installation
Each private key are protected by a strong passphrase consisting of at least 15 characters.

6.4.2 Activation data protection

The passphrase must only be known to the person who owns the encrypted private
key. Any backup of the private key passphrase ((machine read able or on paper)
must be stored in secured place.

6.4.3 Other aspects of activation data
Not defined

6.5 Computer security controls

6.5.1 Specific computer security technical requirements
No other services or software are loaded or operated on the CA server. The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of SSSCA staff.

6.5.2 Computer security rating
Not defined.

6.6 Life cycle technical controls

6.6.1 System development controls
Not defined.

6.6.2 Security management controls
Not defined.

6.6.3 Life cycle security controls
Not defined.

6.7 Network security controls
The signing machine is kept offline. All other CA computers are protected by a firewall and/or by removing all unnecessary services.

6.8 Time-stamping
All time stamping of entries created on the online servers at the SSSCA is based on the network time provided the official providers of time signals.
The hardware clock of the offline system for the certificate and CRL signing, which determines the time stamping of the certificates and the CRLs, will be synchronized manually by the operator whenever the host starts.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All certificates issued by the SSSCA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280.

7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by the SSSCA.

7.1.2 Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in the SSSCA certificates are in the following table.

For natural person certificates:	
Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
Extended Key Usage	clientAuth, emailProtection, codeSigning timeStamping
CRL Distribution Points	URI
Certificate Policies	OID
For server/services certificates:	
Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
Extended Key Usage	clientAuth, emailProtection, codeSigning timeStamping
CRL Distribution Points	URI
Certificate Policies	OID
For CA certificates:	
Basic Constraints	critical, ca: true
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
Extended Key Usage	clientAuth, emailProtection, codeSigning timeStamping
CRL Distribution Points	URI
Certificate Policies	OID

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by the SSSCA are according to:

a)	hash function:	id-sha	1 1.3.14.3.2.26
b)	encryption:	rsaEncryption	1.2.840.113549.1.1.1
c)	signature:	sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4 Name forms

Each entity has a unique and unambiguous Distinguished Name (DN) in all the certificates issued to the same entity by the SSSCA. The DN shall be

structured as defined in ITU-T Standards Recommendation X.501. CNRST prefers that organizations use domain component naming.
Issuer:
C=MN, O=SSSCA, CN=Grid Team
Subject:
C=MN, O=SSSCA, OU=string, CN=name surname
C=MN, O=SSSCA, OU=string, CN=FQDN
The subject field contains the Distinguished Name of the entity with the following
attributes:

MN	Top-level domain (Mongolia)
SSSCA	SSSCA domain
[string]	[Organization string]
name [surname]	CommonName
[service ” /”] FQDN	

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

7.1.6 Certificate policy object identifier
SSS 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)
The SSSCA creates and publish X.509 v2 CRLs.

7.2.2 CRL and CRL entry extensions
The SSSCA shall issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation shall not be included in the individual CRL entries.
The CRL shall include the date by which the next CRL shall be issued. A new CRL shall be issued before this date if new revocations are issued.
The CRL extensions that shall be included are:

- The Authority Key Identifier
- The CRL Number

The CRL entry extensions that will be included are:

- CRL Reason Code
- Invalidity Date

7.3 OCSP profile

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 SSSCA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.
The SSSCA shall at least once a year assess the compliance of the procedures of RA with the CP/CPS document in effect.

8.2 Identity/qualifications of assessor

Not defined.

8.3 Assessor's relationship to assessed entity

Compliance Audits performed by third-party audit firms shall be conducted by firms independent of the audited entity. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services.

8.4 Topics covered by assessment

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

8.5 Actions taken as a result of deficiency

The SSSCA shall take immediate action if the assessment reveals a conflict between the provisions of the CP/CPS document and the actual practice.

8.6 Communication of results

The results of the assessment shall be summed up in a protocol agreed by the assessor and the SSSCA. If no agreement can be reached each party may compile its own version; any communication of results must then provide both versions.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

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

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

The subscriber’s information will be kept confidential unless the subscriber decides to make it public. The information provided by the subscriber to verify his/her identity will be kept confidential.

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information
All participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and consent to use private information
If the SSSCA or any of its accredited RAs wants to use private information, it must ask the subscriber for a written consent. No subscriber shall be under the impression that he/she has an obligation to agree.

9.4.6 Disclosure pursuant to judicial or administrative process
Persuant to a judicial or administrative process private in formation shall only be released upon presentation of a regular warrant issued according to the Mongolian law.

9.4.7 Other information disclosure circumstances
No stipulation.

9.5 Intellectual property rights
The SSSCA does not claim any IPR on certificates which it has issued.

9.6 Representations and warranties

9.6.1 CA representations and warranties
The information published in the certificates, CRLs and OCSP responses are accurate to the best of SSSCA's knowledge. No other warranties are accepted.

9.6.2 RA representations and warranties
All accredited RAs shall perform their task of identification of the requesting parties as described in 3.2.3 and 3.2.2 to the best of their knowledge. No other warranties are accepted.

9.6.3 Subscriber representations and warranties
By requesting an SSSCA certificate a subscriber commits itself to use and protect the certificate and the certified keys according to the stipulations of the CP/CPS document in effect at the date of issuance of the said certificate. (S)he may however apply more stringent observances.
Subscribers must:

- Read and adhere to the procedures published in this document
- Use the certificate for the permitted purposes only
- Authorize the processing and conservation of personal data (as required under the
- Data Protection Law)
- Take every precaution to prevent any loss, disclosure or unauthorized access to or
- use of the private key associated with the certificate, including:
    - (Personal certificates) selecting a Strong Passphrase;
    - (Personal certificates) protecting the passphrase from others;
    - Notifying immediately the SSSCA and any relying parties if the private key is lost or compromised;

- Requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.

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

9.6.4 Relying party representations and warranties

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

- The relying party is familiar with the CA' s CP and the CPS that generated the certificate before drawing any conclusion on trust of the subscriber' s certificate; and
- The reliance is reasonable and in good faith in light of all circumstances known to the relying party at the time of reliance; and
- The certificate is used for permitted purposes only; and
- The relying party checked the status of the certificate to their own satisfaction prior to reliance.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

The SSSCA 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

Also the SSSCA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.

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

9.8 Limitations of liability

Except if explicitly dictated otherwise by the Mongolian law the SSSCA 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.

It 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 appropriate RA acting in conformance with this CP/CPS.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This document becomes effective after its publication on the Web site of the SSSCA starting at the date announced there. There is no term set for its expiration.

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
Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

9.11 Individual notices and communications with participants
All e-mail communications between the CA and its accredited RAs must be signed with a certified key.
All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

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 SSSCA Web pages at least 2 weeks before becoming effective.
The SSSCA will inform its subscribers and all relying parties it knows of by means of an e-mail.

9.12.3 Circumstances under which OID must be changed
Substantial changes shall cause the OID to be changed. The decision is made by the general manager of the SSSCA and submitted to the SSS GRID PMA for approval.

9.13 Dispute resolution provisions
Disputes arising out of the CP/CPS shall be resolved by the general manager of the SSSCA.

9.14 Governing law
The SSSCA and its operation are subject to the Mongolian law. All legal disputes arising from the content of this CP/CPS document, the operation of the SSSCA and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by SSSCA shall be treated according to Mongolian law.

9.15 Compliance with applicable law
All activities relating to the request, issuance, use or acceptance of a SSSCA certificate have to comply with the Mongolian law.
Activities initiated from or destined for another country than Mongolia must also comply with that country's law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement
Not applicable.

9.16.2 Assignment
Not applicable.

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)
Not applicable.

9.16.5 Force Majeure
Events that are outside the control of the SSSCA will be dealt with immediately by the SSS GRID PMA.

9.17 Other provisions
No stipulation

10. RFERENCES

- S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, " Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC 3647, November 2003 [replaces RFC 2527]
  http://www.ietf.org/rfc/rfc3647.txt
- S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework" , RFC 2527, March 1999
  http://www.ietf.org/rfc/rfc2527.txt
- R. Housley, W. Polk, W. Ford and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" , RFC 3280, April 2002
  http://www.ietf.org/rfc/rfc3280.txt
- R. Housley, W. Ford, W. Polk and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and CRL Profile" , RFC 2459,January 1999
  http://www.ietf.org/rfc/rfc2459.txt
- Moroccan Magrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.0, January 2007
  http://www.magird.ma
- Certification Authority Austrian Grid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.2.0, May 2007
  http://ca.austriangridca.at
- Pakistan Grid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.2.0, December 2007
  http://www.ncp.edu.pk/pk-grid-ca/