South African e-Science CA Certificate Policy and Certification Practice Statement

Version 0.0.3

Document Object Identifier:1.2.840.113612.5.4.2.8.0.1

List of changes

VERSION	DATE	CHANGES
draft_bb8	26 June 2009	Minor edits to overall document. Clarification of certain technical details and posture of certain technical issues. Moved List of changes to the front. Still need to check all cross-references in the document.
Draft-0.2	29 November 2013	Changes made in the light of the ei4Africa project results
Draft-0.3	22 April 2014	Implementing changes requested by reviewer Roberto Cecchini

Table of Contents

1 Introduction

This document is a draft. It describes the set of rules and procedures adhered to by the South African e-Science project (SAGrid) Certificate Authority. The legal entity which is represented in the document is the South African Council for Scientific and Industrial Research (CSIR). The following terms are used in this document:

Activation data
Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

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 life-time.

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.

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.

Certification Practice Statement (CPS)
A statement of the practices, which a certification authority employs in issuing certificates.

Issuing Certification Authority (Issuing CA)
In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Policy Management Authority (PMA)
The Authority responsible for the maintenance of the CP and CPS.

Policy Qualifier
Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Registration Authority (RA)
An entity that is responsible for identification and authentication of certificate subjects, 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.

Robot
A personal credential which can perform automated tasks on behalf of the user.

SAGrid
The South African National Compute Grid project (http://www.sagrid.ac.za)

SANREN
The South African National Research Network (http://www.sanren.ac.za)

Set of provisions
A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS and employing the approach described in this framework.

1.1 Overview

This document is structured according to RFC 5280 [2]
This document is the CP/CPS for the *South African e-Science CA.* It describes the set of rules and procedures followed by the *South African e-Science CA* herewith abbreviated as the SAGrid CA, (SAGrid, http://www.sagrid.ac.za/).

1.2 Identification

Document title: **SAGrid CA Certificate Policy and Certification Practice Statement**
Document version: **0.0.3**
Document date: **April 22 2014**
The following ASN.1 Object Identifier has been assigned to this CP/CPS: **1.2.840.113612.5.4.2.8 .0.1**
This document is available from: **http://security.sanren.ac.za/CA/CPS**

1.3 Community and Applicability

1.3.1 Certification Authorities

The South African e-Science CA is a self-signed root certification authority. It does not issue certificates to subordinate CAs.

1.3.2 Registration Authorities

The South CA delegates identification and authorization of certificate subjects to trusted individuals (Registration Authorities). These intermediaries are formally appointed by the CA manager of the Structure in which they operate. Their identities are published in an online repository.
RAs must perform their tasks in accordance with this CP/CPS.

1.3.3 End Entities

The South African e-Science CA issues certificates for:

- bona fide members of the South African research and tertiary education community, including students, employees and fellows of South African universities, public research facilities and science councils.

- digital processing entities, capable of performing cryptographic operations, owned by SAGrid member institutes or used for activities in which SAGrid member institutes are involved;

- services on digital processing entities, owned by SAGrid member institutes or used for activities in which SAGrid member institutes are involved;

- parties not affiliated with the South African research and tertiary education community, when they have a bona fide need to possess a certificate issued by the South African e-Science CA, as established by the PMA.

1.3.4 Applicability

Certificates issued can be used for:

- e-mail signing and encryption (S/MIME);

- client authentication (SSL/TSL and GSI);

- server authentication and encryption of communications (SSL/TSL and GSI)

- generation of proxy certificates, as specified in RFC3820 [10];

- object-signing.

1.4 Contact Details

1.4.1 Specification Administration Organization

The South African e-Science CA is managed by the Meraka Institute
This document is managed by the South African e-Science CA manager (see Section 1.4.2).

1.4.2 Main Contact Person

The primary contact for the CA is the SAGrid Coordinator :

Dr. Bruce Becker
Meraka Institute
Council for Scientific and Industrial Research (CSIR)
Building 43 CSIR Campus

P.O Box 395
Pretoria 0001
South Africa
Phone: +27 12 841 3746
Cell: +27 84 989 6169
e-mail: bbecker@csir.co.za

1.4.3 CA Managers

The CA managers and responsible sfor CA day-to-day operations of the CA are :

Dr. Bruce Becker, Simeon Miteff
Meraka Institute
Council for Scientific and Industrial Research (CSIR)
Building 43 CSIR Campus

P.O Box 395
Pretoria 0001
South Africa
Phone: +27 12 841 3746
Cell: +27 84 989 6169
e-mail: bbecker@csir.co.za

1.4.4 Person Determining CPS Suitability for the Policy

See Section 1.4.2

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

The **South African e-Science CA** will operate a Certification Authority service in accordance with all provisions of this CP and associated CPS.

In particular it will:

- issue certificates based on the requests from entitled subscribers, validated by a Registration Authority;
- notify the subscriber of the issuing of the certificate;

- publish the issued certificates on the online CA repository;
- accept revocation requests according to the procedures outlined in this document (see section 3.4);
- generate and publish Certificate Revocation Lists (CRLs) as described in this CP/CPS document
- Identify and publish a list of services for the robots for which service robot certificates are issued.(cf. Sections 3.1.2 and 7.1.1)

2.1.2 RA Obligations

The SAGrid CA delegates the tasks of identification and authorization of certificate subjects to **Registration Authorities**.

A **Registration Authority** must:
- authenticate the entity which makes the certification request in accordance to the procedures outlined in this document;
- verify that the information provided in the certificate request is correct and that the requester has the characteristics specified in Section 1.3.3;
- for host or service certificate verify that the requester is the system administrator of the resource or has been authorized by him;
- for robots certificates verify that the requester has satisfied the requirements as stated in section 3.1.9
- accept revocation requests, according to the procedures outlined in this document (see section 3.4), and immediately notify the South African e-Science CA manager;
- provide information to the subscriber on how to properly maintain a certificate and the corresponding private key in accordance to “Protection of private key data for end-users in local and remote systems” [8]. A copy of this document should also be supplied to the subscriber for referencing purposes;
- record and archive all certificate requests, all revocation requests and notifications of certificate issuance.

2.1.3 Subscriber Obligations

Subscribers must:
- adhere to the procedures published in this document;
- use the certificates for the permitted purposes only;
- generate a key pair using a trustworthy method;
- for host or service certificates apply only if they are the system administrators or have been authorized by the relevant person;
- for robot certificates, use a secure key token to protect the private key;
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, in particular, for natural person certificates:
- selecting a suitable pass phrase of at least 12 characters;
- not store it in a network shared file system (e.g. in an AFS or NFS directory);
- notify immediately the CA manager or the relevant RA in case of loss or compromise of the private key.

Failure to comply to these obligations is sufficient cause for the revocation of the certificate.

2.1.4 Relying Party Obligations

We refer to any entity that accepts certificates issued by the CA generically as a "Relying Party." Relying parties must:

- understand and accept this CP and associated CPS;
- verify the CRL before validating a certificate (see Section 2.6.4);
- use the certificates for the permitted purposes only (see Section 1.3.4)

2.1.5 Repository Obligations

The CA will make available on its web server the certificates and CRLs, as soon as issued.

2.2 Liability

The CA only guarantees to issue and to revoke certificates according to the practices described in this document. No other liability, implicit or explicit, is accepted.

2.2.1 CA Liability

The CA:

- will not give any guarantees about the security or suitability of the service: the certification service is run with a reasonable level of security, but it is provided on a *best effort only* basis;
- doesn't warrant its procedures and will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides;
- denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

2.2.2 RA Liability

It is the RA's responsibility to authenticate subscribers according to the procedure described in this document and to inform the CA if circumstances for revocation are satisfied.

2.3 Financial Responsibility

The CA assumes no financial responsibility with respect to use or management of any issued certificate.

2.3.1 Indemnification by Relying Parties

No stipulation

2.3.2 Fiduciary Relationships

No stipulation

2.3.3 Administrative Processes

Administrative processes pertaining to this CP/CPS shall be determined by the PMA[1] and the sponsoring organization[2] pursuant to the agreement between the two entities.

[1]In this document, PMA refers implicitly to the EUGridPMA.
[2]The sponsoring organisation is the South African Council for Scientific and Industrial Research, in particular the Meraka Institute Operating Unit – http://www.csir.co.za/meraka

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Interpretation of this CP and CPS is according to the laws of the Republic of South African.

2.4.2 Severability, Survival, Merger, Notice

Should it be determined that one section of this document is incorrect or invalid, its other sections shall remain in effect until the document is amended.
Before termination of its operations, the SAGrid CA will notify its subscribers and Registration Authorities. All issued certificates will be revoked before the time of termination.

2.4.3 Dispute Resolution Procedures

The PMA shall resolve any disputes associated with the use of the certificates issued by this CA.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

No fees are charged.

2.5.2 Certificate Access Fees

No fees are charged

2.5.3 Revocation or Status Information Access Fees

No fees are charged.

2.5.4 Fees for Other Services such as Policy Information

No fees are charged.

2.5.5 Refund Policy

No refund will be given at any time.

2.6 Publication and Repositories

2.6.1 Publication of CA Information

The CA operates an online repository at the address specified below (section 2.6.4) that contains:

- the CA's certificate;
- the certificates issued by the CA;
- the Certificate Revocation List;
- a copy of this document and all previous versions;
- other information relevant to the CA

2.6.2 Frequency of Publication

- Certificates will be published as soon as issued.
- CRLs will be published as soon as issued and at least every week.
- Changes to this CP and CPS will be published as soon as they are approved.
- Previous versions will remain available online.

2.6.3 Access Controls

The online repository is maintained on a best effort basis, available on 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance.
The CA doesn't impose any access control on its Policy, its certificate, issued certificates and CRLs.

2.6.4 Repositories

Repository of certificates and CRLs is at **http://security.sanren.ac.za/CA/**

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

The CA management will perform, once per year, a self-assessment to verify the compliance of its operating procedures to this CP/CPS.
The CA will accept no more than one external compliance audit per year and its entire cost must be borne by the requester.

2.7.2 Identity/Qualifications of Auditor

No stipulation.

2.7.3 Auditor's Relationship to Audited Party

The audit can be requested by qualified relying parties, e.g. by a policy management authority which the CA recognizes. The CA may require evidence of the chosen auditor qualifications. The CA may impose confidentiality restrictions upon the auditor.

2.7.4 Topics Covered by Audit

The audit will verify the compliance of the CA operating procedures with the current CP/CPS.

2.7.5 Actions Taken as a Result of Deficiency

The CA manager will announce the steps, with a timetable, that will be taken to remedy the deficiencies found.

2.7.6 Communication of Results

The CA manager will publish the results and the proposed remedies. The quantity of details will be decided according to security and confidentiality reasons.

2.8 Confidentiality

The CA collects subscribers' full name, organization, e-mail address, details of the document presented for identification (type, number, date of issuance) in accordance with the applicable South African law
Under no circumstances will the CA have access to the private keys of any subscriber to whom it issues a certificate.

2.8.1 Types of Information to Be Kept Confidential

Data collected during the authorization process and not published in the certificate is considered confidential.
The Meraka Institute of the South African CSIR, as host and sponsor of the CA, has the responsibility of to protect private data stated here.

2.8.2 Types of Information Not Considered Confidential

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

2.8.3 Disclosure of Certificate Revocation/Suspension Information

When a certificate is revoked, a reason code may be included in the CRL entry for the action. This reason code is not considered confidential.
Other details concerning the revocation will not be disclosed unless required by a legal authority of competent jurisdiction.

2.8.4 Release to Law Enforcement Officials

See Section 2.4.1

2.8.5 Release as Part of Civil Discovery

See Section 2.4.1

2.8.6 Disclosure Upon Owner's Request

Disclosure upon owner's request will be done according to the applicable South African law

2.8.7 Other Information Release Circumstances

No other circumstances for release of personal information apart from those in the above paragraphs.

2.9 Intellectual Property Rights

This document follows the template specified by RFC 3647 [1].
Parts of this document are inspired by other CP and CPS: INFN[6] , UK e-Science Grid[4], AustrianGrid[9], CNRS GRID2- FR[7] , DutchGrid[5] and BYGCA [8]

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name is of the X.500 name type, all its parts are encoded as *PrintableString*s.
The *CommonName* has one of the following forms:

- **Natural Person:** name and surname of the subscriber;
- **Digital Processing Entity:**the entity fully qualified domain name;
- **Service:**the service name, a '**/**' and the server fully qualified domain (e.g. '**gridftp/server.domain.name**');
- **Robot:**the string '**Robot:** ', a brief description of its function, a '-' and the full name of the subscriber (e.g.: '**Robot: function - subscriber name**')

3.1.2 Need for Names To Be Meaningful

The *CommonName* must represent the subscriber in a way that is easily understandable for humans and must have a reasonable association with the authenticated name of the subscriber. It may contain additional text to disambiguate between different users or to allow the same user to have more than one certificate.

3.1.3 Rules for Interpreting Various Name Forms

See Section 3.1.1

3.1.4 Uniqueness of Names

The Distinguished Name must be unique for each subject certified by the CA. If the name presented by the subscriber is not unique, the CA Manager will ask the subscriber to resubmit the request with some variation. Additional numbers or letters can be appended to the common name to ensure uniqueness (see Section 3.1.2). Two names are considered identical if they only differ in case or punctuation or white space. These can therefore, not be used to distinguish names
The CA will ensure that each issued DN is unique and that it will never be assigned to more than one entity for the whole life of the CA.
Certificates must apply to unique individuals or resources. Users may not share certificates.

3.1.5 Name Claim Dispute Resolution Procedure

The CA manager will resolve this kind of disputes. The CA manager is the final arbiter of these disputes.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

The possession of the private key by the requester is considered proven when the signature of the certificate signing request (CSR) is verified using the public key present in the request.

3.1.8 Authentication of Organization Identity

Authentication of Organization Identity is part of the procedure for the appointment of an RA (see Section 1.3.2), and only the Organizations for which an RA has been appointed appear the certificates.

3.1.9 Authentication of Individual Identity

- **Natural Person**: the subscriber is authenticated by meeting the the RA face to face and producing the following documents:
  - a valid national Identity booklet or a valid passport of a legal resident in South Africa
  - a valid official letter conforming the affiliation with the indicated organization

  The RA carefully validates the documents and confirms the photo image and then makes photocopies and scanned images of the documents. The original letter of affiliation is retained by the RA. The RA will communicate to the CA in a secure on-line transaction or in person the following: name and surname of the requester and the details of his ID document. Another set of photocopies of the subscribers documents is securely sent to the CA. No such photocopies will be accepted from the subscriber.

- **Digital Processing Entity** and **Service:** the requester must send the request to the RA by a signed e-mail. The RA verifies the correctness of the request and sends it – including the requester's signature – to the CA by a signed e-mail.

- **Robot**: as for a Natural Person. In addition the certificate request must be generated in the RA's presence using a secure hardware token, as described in Section 6.2.1.

3.2 Routine Re-key

Re-key of certificates of natural persons and Robots before the expiration, *and providing that the last identification in accordance to Section 3.1.9 is not older than 5 years*, can be requested by an on-line procedure, which checks the validity of the subject's certificate. In case the request is signed by the subscriber's valid existing certificate, the CA shall assign an RA local to the subscriber to re- verify the subscriber's data, the subscriber affiliation, and the right of the subscriber to a certificate. The certificate is issued after the approval by the relevant RA.
In all the other cases re-keying follows the same rules as an initial registration.

3.3 Re-key After Revocation

There is no re-keying after revocation. Re-key after revocation follows the same rules as an initial registration (Section 3.1).

3.4 Revocation Request

Certificate revocation requests must be sent by **signed** e-mail by the owner of the certificate, by the appropriate Registration Authority or by any other entity presenting proof of knowledge of a circumstance for revocation.

4 Operational Requirements

4.1 Certificate Application

Procedures are different if the subject is a natural person or a digital processing entity. In every case the subject has to generate his own key pair.

Minimum key length is 1024 bits.

- **Natural person**. Before submitting the request the user must be authenticated by an RA. During the authentication a random authorization number is generated, communicated to the user and sent to the CA, together with the user's data (see Section 3.1.9). Before 48 hours from the authentication, the user must submit a certificate request via an online procedure, specifying the above authorization number. The request is considered valid if the information supplied by the user coincides with that received during the authentication.

- **Digital Processing Entity** and **Services**. Certificate requests are sent by e-mail to the appropriate RA and must be signed by a valid CA certificate belonging to a natural person. The RA verifies the right of the requester to obtain the certificate and then forwards the request to the CA by a signed e-mail. An e-mail with a request of confirmation is sent to the address specified by the requestor to check its validity. The certificate request is not valid until reception of the confirmation. A configuration file for OpenSSL is available from the CA web server.

- **Robot. The procedure here is the same** as for a natural person, with the difference that the user must generate the certificate request in presence of the RA, using a secure hardware token (see Section 6.2.1).

4.2 Certificate Issuance

The CA issues the certificate if, and only if, the authentication of the subject is successful.
If the subject is a natural person, a message is sent to their e-mail address with the download instructions. In the other cases, the certificate is sent *to the address specified in the request*.
If the authentication is unsuccessful, the certificate is not issued and an e-mail with the reason is sent to the subject.
A copy of all correspondence is always sent to the RA.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- the subscriber's private key is lost or suspected to be compromised;
- the information in the subscriber's certificate is suspected to be inaccurate;
- the subscriber violated his obligations.

In addition, a subscriber may always request the revocation of his certificate.

4.4.2 Who Can Request Revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of a circumstance for revocation (see Section 3.4).

4.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself properly. SAGrid CA Operators will then decide on the matter.

4.4.4 Revocation Request Grace Period

The revocation for a compromise of the private key must be requested immediately, within one working day for the other circumstances.

4.4.5 Circumstances for Suspension

The CA does not offer suspension services.

4.4.6 Who Can Request Suspension

No stipulation.

4.4.7 Procedure for Suspension Request

No stipulation.

4.4.8 Limits on Suspension Period

No stipulation.

4.4.9 CRL Issuance Frequency

CRLs are issued immediately after every certificate revocation or at least every week.

4.4.10 CRL Checking Requirements

A relying party must verify a certificate against the most recent CRL issued, in order to validate the use of the certificate (see Section).

4.4.11 Online Revocation/Status Checking Availability

OCSP is not supported.

4.4.12 Online Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisement Available

No stipulation

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Re-Key Compromise

No stipulation

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

The following events are recorded:

- authentications of natural person;
- certification requests;
- issued certificates;
- revocation requests;
- issued CRLs;
- all correspondence sent and received by the CA;
- reboot, login and logout on the signing machine.

Comment [Bruce Bec1]: We should define the procedure for recording : 1) where are these events recorded to ? 2) who is notified of the recordings ? 3) how are they to be recorded ?

4.5.2 Frequency of Processing Log

No stipulation.

4.5.3 Retention Period for Audit Logs

The minimum retention period is three years.

Comment [Bruce Bec2]: What is the maximum retention period ? 10 years (duration of the certificate validity ?)

4.5.4 Protection of Audit Log

Only authorized persons have access to the logs.

Comment [Bruce Bec3]: Define "authorized person" - these are people authorized by the CA Manager ?

4.5.5 Audit Log Backup Procedures

Records shall be backed up on removable media, which shall be stored in a secure physical location with restricted access.

4.5.6 Audit Collection System (Internal vs. External)

The audit record collection process is done under the control of the CA operators.

4.5.7 Notification to Event-causing Subject

The subject who caused an audit event to occur is not notified of the audit action.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of Records Archived

See Section .

4.6.2 Retention Period for Archives

See Section 4.5.3.

4.6.3 Protection of Archive

See Section 4.5.4

4.6.4 Archive Backup Procedures

See Section 4.5.5.

4.6.5 Requirements for Time-stamping of Records

No stipulation.

4.6.6 Archive Collection System (Internal or External)

See Section 4.5.6.

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover

A new CA self-signed certificate is generated at least one year before the expiry of the old one. From that time on, only the new key will be used for certificate signing purposes. The new public key is available on the online repository,and new certificates can be issued.
The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed by the associated private key have also expired.

The CA certificate will have a validity period of ten years.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and/or Data Are Corrupted

If CA equipment is damaged or rendered inoperative it will be replaced as soon as possible using the backup copies available on-site or off-site.

4.8.2 Entity Public Key is Revoked

See Section 4.8.3.

4.8.3 Entity Key is Compromised

If the CA's private key is — or suspected to be compromised, the CA will:

- inform subscribers (by electronic message) and cross-certifying CA's;
- terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key;
- generate a new CA certificate (with a new key pair) and make it immediately available on the public repository;
- all subjects will have to re-certify, following the initial identification procedures defined in Section 4.1

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.

4.8.4 Secure Facility After a Natural or Other Type of Disaster

In case of a natural disaster, disaster recovery procedures should start as soon as is humanly possible. Backup copies kept in an off-site location are to be used to restart CA operations.

4.9 CA Termination

At least 60 days before the CA terminates its services, it will:

1. inform cross-certifying CAs, Registration Authorities, subscribers and relying parties ;
2. make widely available information of its termination;
3. stop issuing certificates and CRLs;
4. Annihilate all copies of private keys.

The CA manager will be responsible for the archival of records as per Section 4.6.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

The CA operates in a controlled environment, where access is restricted to authorized people only

5.1.1 Site Location and Construction

The CA is housed in the Data Center of Building 9 at the CSIR Campus.

5.1.2 Physical Access

The signing machine and all removable media are kept in the CSIR server room. The CSIR Pretoria campus is a national key point of South Africa and is a highly-secure location. Access to the CA signing machine and the online repository are authorised to CA and Computing Services personnel only.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the online repository is connected to a UPS system in order to maximise availability.

5.1.4 Water Exposures

The room in which the CA will be housed is reasonably waterproofed. However floods are not expected in the region.

5.1.5 Fire Prevention and Protection

The building has a fire alarm system and fire extinguishers in place. CSIR follows the South African laws regarding fire prevention and safety.

5.1.6 Waste Disposal

Removable storage media a physically destroyed to avoid any re-use before they are disposed of in waste bins.

5.1.7 Off-site Backup

Critical files are backed up at an off-site location.

5.2 Procedural Controls

5.2.1 Trusted Roles

- No stipulation.

5.2.2 Number of Persons Required per Task

No stipulations.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.3 Personnel Security Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

CA management is done by trained persons, well aware of the necessary security requirements.
RAs must be familiar with their tasks and be aware of the security implications of their activities. A guide is maintained online at http://security.sanren.ac.za/CA and RA's much certify that they have read it. Periodical instruction seminars are kept by CA manager.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training Requirements

No stipulation.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

In case of unauthorized actions by a CA or RA operator, the CA manager may revoke the privileges concerned.

5.3.7 Contracting Personnel Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

The CA manager will supply the CA and RA operators with a copy of this document.
The CA manager will supply the CA and RA operators with a copy of the document 'Protection of private key data for end-users in local and remote systems" [8].
The CA operator has access to the online documentation of the CA procedures primarily via the CA public-facing website.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keys for the SAGrid CA are generated by CA staff on a dedicated machine, not connected to any type of network. The software package is OpenSSL. Each entity must generate its own key pair.

6.1.2 Private Key Delivery to Entity

No delivery of private keys is allowed. SAGrid CA does not generate private keys for its subjects. Each requesting party must generate its own key pair.

6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to the CA in a secure and trustworthy manner: by online SSL transaction for personal and robot certificates, by signed e-mail for server and service certificates.

6.1.4 CA Public Key Delivery to Users

The CA certificate (containing its public key) is delivered to subscribers via the online public web site of the CA.

6.1.5 Key Sizes

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

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

If the key pair is associated with a robot certificate, it must be kept in a secure hardware token, and must be generated in it. In the other cases, key may be generated as software tokens.

6.1.9 Key Usage Purposes

Keys may be used for authentication, data encryption, non-repudiation, message integrity and session key establishment.

The CA private key is the only key that can be used for signing certificates and CRLs.
The Certificate *keyUsage* field is used in accordance with RFC3647 [1].

6.2 Private Key Protection

CA private key is kept on removable media and kept in a safe.
Subscribers must adequately protect the private keys of the certificates issued to them. The required level of protection depends on the type of certificate:

- **personal**: the key must be stored in encrypted form with a sufficiently strong pass phrase, with appropriate file system protections and not in a network shared file system; alternatively the key may be stored in an hardware token as described in Section 6.2.1;

- **host or service**: the key may be stored in unencrypted form, with appropriate file system protections and not in a shared file system; alternatively the key may be stored in a hardware token as described in Section 6.2.1;

- **robot**: the key must be generated and stored in an hardware token as described in Section 6.2.1.

The generation and storage of subscribers' private keys must be in accordance to the document “Protection of private key data for end-users in local and remote systems” [8] issued as a guideline by the EUGridPMA

6.2.1 Standards for Cryptographic Module

A secure hardware token must comply with the requirements of at least FIPS 140-1 level 2, FIPS 140-2 level 2 or equivalent.

6.2.2 Private Key (n out of m) Multi-person Control

Private keys pertaining to personal certificate must not be under multi-person control.
CA private key is not under multi-person control.

6.2.3 Private Key Escrow

Private keys must not be escrowed.

6.2.4 Private Key Backup

The CA private key is kept, encrypted, in multiple copies and in different locations, on removable media.

6.2.5 Private Key Archival

Backup copies can be used as an archival service. Access restrictions are to be set for these backup copies.

6.2.6 Private Key Entry into Cryptographic Module

Apart from robot certificates, private keys may be uploaded into a hardware token.

6.2.7 Method of Activating Private Key

The activation of the CA private key is done by providing the pass phrase.

6.2.8 Method of Deactivating Private Key

The pass phrase of the CA private key is kept only in the memory of the signing machine, which is powered off at the end of each signing session.

6.2.9 Method of Destroying Private Key

Private key backup copies of expired CA certificates will be disposed by secure and permanent physical destruction of the media.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The CA certificate has a validity of ten years. Subscribers' certificates have a validity of at most one year. It may be less depending on the lifetime of the subscriber's affiliation contract.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The length of the pass phrase of the CA private key is of 15 characters at least.

Comment [Bruce Bec4]: What encoding is to be used for these characters ?

6.4.2 Activation Data Protection

If subscriber's private key is protected by a pass phrase, it must be a strong pass phrase; if protected by a hardware token, it must have a PIN known only to the subscriber to activate it. The pass phrase of the CA private key is kept in a sealed envelope kept in an off-site safe.

Comment [Bruce Bec5]: Password security value about 1.3 ?

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA servers include the following functionalities:

- operating systems are maintained at a high level of security by applying all recommended security patches;
- Automated intrusion detection software is employed to alert of unauthorized entry or tampering
- automated monitoring is done in parallel to IDS to detect unauthorized software changes;
- services running on the machine are reduced to the bare minimum;
- machines are protected by a suitably configured firewall.
- The machine used for signing certificates is not connected to any kind of networks.

Comment [Bruce Bec6]: Give a list of the services running on the machine.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

The CA uses open- source software (OpenSSL) that is under continuous scrutiny by the public community. It will not itself be involved in the development of cryptographic software..

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

See Section 6.5.1.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Number:

Subscriber certificates: X.509 version 3
CA certificate: X.509 version 3

7.1.2 Certificate extensions

Subscriber certificates contain the extensions:

basicConstraints
- critical, FALSE

keyUsage
- *critical, Digital Signature, Key Encipherment, Data Encipherment*

CRL Distribution Points
- *non- critical, a single HTTP URL referring to CRL*

certificatePolicies
- *non- critical, one or more OIDs, with at least one referring to this CP/CPS*

authorityKeyIdentifier
- *non- critical, keyid*

subjectKeyIdentifier
- non- critical, hash

subjectAlternativeName
- for host and service certificates: *at least one DNS FQDN*
- for server certificates: *at least one FQDN*
- for personal certificates: *optionally an email address*
- for robot certificates: *at least one valid email address*

The CA certificate contains the extensions:

basicConstraints
- *critical, TRUE*

keyUsage
- *critical, Digital Signature, Certificate Signing, CRL Signing*

subjectAlternativeName
- *non- critical, email address: ca-manager@security.sanren.ac.za*

subjectKeyIdentifier
- *non- critical, hash*

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name forms

Subject certificates:

Issuer: **C=RSA,O=CSIR,CN=South African e-Science CA**

The **Subject** field contains a distinguished name of the entity with the following attributes:

countryName: RSA

organizationName: CSIR

An additional organization attribute shall follow indicating the certificate subject class as specified in section 3.1.1, using one of the following values
Natural Person: Personal Certificate
object-signing: Objsign
digital processing entity: Host
service: Service
robot: Robot

organizationalUnitName: Name of physical organization hosting the RA approving the Subject's request

localityName: Location within which the RA is appointed;

commonName:
Natural Person: requester's full name;
object-signing: requester's full name;
digital processing entity: a Fully Qualified Domain Name
service: the service name, '/', a Fully Qualified Domain Name
robot: 'Robot: ', robot's function, '-', requester's full name

CA certificate:

Issuer: **C=RSA,O=CSIR,CN=South African e-Science CA**
Subject: C=RSA,O=CSIR,CN=South African e-Science CA

Comment [Bruce Bec7]: Should this be CSIR or Meraka ?

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates contain in the Certificate Policy extension one or more OID's, one of them referring to this document (see Section 1.2). Subscriber certificates contain in the certificatePolicies extension the OID of the CP/CPS document under which they were issued. The certificates may contain additional OIDs indicating additional policies with which they comply.
Robot certificates will contain a 1SCP robot OID.

7.1.7 Usage of Policy Constraints Extensions

No stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

The qualifier is a pointer to this document, in the form of an URL.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version

X.509 v1

7.2.2 CRL and CRL Entry Extensions

No stipulation

8 Specification Administration

8.1 Specification Change Procedures

Relevant CPS changes will be announced to the RA, published on the CA web site and submitted to the EuGridPMA.
Minor changes will only be announced on the CA web site, the EUGridPMA mailing list and the relevant announcement mailing list.

8.2 Publication and Notification Procedures

The policy and all previous versions are available at http://security.sanren.ac.za/CA/CPS.

8.3 CPS Approval Procedures

No Stipulation..

9 References

1. S. Chokani and W. Ford, *Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework*, RFC 3647
2. Chokhani, et al. , *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 5280.
3. *UK eScience Certification Authority Certificate Policy and Certification Practices Statement*, Version 1.4, November 2007.
4. *DutchGrid and NIKHEF mediumsecurity X.509 Certification Authority Certification Policy and Practice Statement*, Version 3.1, November 2007.
5. INFN CA Certificate Policy and Certification Practice Statement, Version 2.3.1, February 2008
6. Certificate Policy and Certification Practice Statement CNRS GRID2-FR, Version 1.1, February 2009
7. Belarusian Grid Certification Authority, Certificate Policy and Certification Practice Statement, Version 1.3, April 2009
8. Protection of private key data for end-users in local and remote systems, Version 1.0, 2 May 2009
9. Austrian Grid CP/CPS https://ca.austriangridca.at/CP_CPS/
10. Tuecke, et al., *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile*, RFC 3820

Comment [bruce bec8]: 5280 states that it obsoletes 3280