



GridKa-CA

Certificate Policy  
and  
Certification Practice Statement

Document Identifier 1.3.6.1.4.1.2614.5548.1.1.1.6

Document Version 1.6

September 2011

Ursula Epting

## Table of Contents

1 INTRODUCTION .....	6
1.1 Overview.....	6
1.1.1 General Definitions.....	6
1.2 Identification.....	8
1.3 Community and Applicability .....	8
1.3.1 Certification authorities .....	8
1.3.2 Registration authorities .....	8
1.3.3 End entities .....	8
1.3.4 Applicability .....	8
1.4 Contact Details.....	8
1.4.1 Specification administration organization.....	8
1.4.2 Contact person.....	9
1.4.3 Person determining CPS suitability for the policy.....	9
2 GENERAL PROVISIONS .....	9
2.1 Obligations .....	9
2.1.1 CA obligations.....	9
2.1.2 RA obligations.....	9
2.1.3 Subscriber obligations .....	9
2.1.4 Relying party obligations .....	10
2.1.5 Repository obligations .....	10
2.2 Liability .....	10
2.2.1 CA liability.....	10
2.2.2 RA liability.....	10
2.3 Financial Responsibility .....	10
2.3.1 Indemnification by relying parties.....	10
2.3.2 Fiduciary relationships.....	10
2.3.3 Administrative processes.....	10
2.4 Interpretation and Enforcement.....	11
2.4.1 Governing law.....	11
2.4.2 Severability, survival, merger, notice.....	11
2.4.3 Dispute resolution procedures.....	11
2.5 Fees .....	11
2.5.1 Certificate issuance or renewal fees.....	11
2.5.2 Certificate access fees.....	11
2.5.3 Revocation or status information access fees.....	11
2.5.4 Fees for other services such as policy information.....	11
2.5.5 Refund policy.....	11
2.6 Publication and Repository.....	11
2.6.1 Publication of CA information .....	11
2.6.2 Frequency of publication .....	11
2.6.3 Access controls .....	12
2.6.4 Repositories .....	12
2.7 Compliance audit.....	12
2.7.1 Frequency of entity compliance audit.....	12
2.7.2 Identity/qualifications of auditor.....	12
2.7.3 Auditor's relationship to audited party.....	12

## GridKa-CA Certification Policy and Certification Practice Statement Version 1.6

2.7.4 Topics covered by audit.....	12
2.7.5 Actions taken as a result of deficiency.....	13
2.7.6 Communication of results.....	13
2.8 Confidentiality .....	13
2.8.1 Types of information to be kept confidential.....	13
2.8.2 Types of information not considered to be confidential.....	13
2.8.3 Disclosure of certificate revocation/suspension information.....	13
2.8.4 Release to law enforcement officials.....	13
2.8.5 Release as part of civil discovery.....	13
2.8.6 Disclosure upon owner's request.....	13
2.8.7 Other information release circumstances.....	13
2.9 Intellectual Property Rights .....	13
3 IDENTIFICATION AND AUTHENTICATION .....	14
3.1 Initial Registration.....	14
3.1.1 Types of names .....	14
3.1.2 Need for names to be meaningful.....	14
3.1.3 Rules for interpreting various name forms.....	15
3.1.4 Uniqueness of names .....	15
3.1.5 Name claim dispute resolution procedure.....	15
3.1.6 Recognition, authentication and role of trademarks.....	15
3.1.7 Method to prove possession of private key.....	15
3.1.8 Authentication of organization identity .....	15
3.1.9 Authentication of individual identity .....	15
3.2 Routine Rekey .....	15
3.3 Rekey after Revocation .....	15
3.4 Revocation Request .....	16
4 OPERATIONAL REQUIREMENTS .....	16
4.1 Certificate Application .....	16
4.2 Certificate Issuance.....	16
4.3 Certificate Acceptance .....	16
4.4 Certificate Suspension and Revocation .....	16
4.4.1 Circumstances for revocation .....	16
4.4.2 Who can request revocation.....	16
4.4.3 Procedure for revocation request .....	17
4.4.4 Revocation request grace period.....	17
4.4.5 Circumstances for suspension .....	17
4.4.6 Who can request suspension .....	17
4.4.7 Procedure for suspension request .....	17
4.4.8 Limits on suspension period .....	17
4.4.9 CRL issuance frequency .....	17
4.4.10 CRL checking requirements.....	17
4.4.11 On-line revocation/status checking availability .....	17
4.4.12 On-line revocation checking requirements .....	17
4.4.13 Other forms of revocation advertisements available .....	17
4.4.14 Checking requirements for other forms of revocation advertisements .....	17
4.4.15 Special requirements of key compromise .....	17
4.5 Security Audit Procedures .....	17
4.5.1 Types of event recorded.....	17
4.5.2 Frequency of processing log.....	18
4.5.3 Retention period for audit logs .....	18

## GridKa-CA Certification Policy and Certification Practice Statement Version 1.6

4.5.4 Protection of audit log .....	18
4.5.5 Audit log backup procedures .....	18
4.5.6 Audit collection system (internal vs external).....	18
4.5.7 Notification to event-causing subject.....	18
4.5.8 Vulnerability assessments .....	18
4.6 Records Archival .....	18
4.6.1 Types of event recorded.....	18
4.6.2 Retention period for archive .....	18
4.6.3 Protection of archive .....	18
4.6.4 Archive backup procedures .....	18
4.6.5 Requirements for time-stamping of records .....	19
4.6.6 Archive collection system (internal or external).....	19
4.6.7 Procedures to obtain and verify archive information .....	19
4.7 Key changeover .....	19
4.8 Compromise and Disaster Recovery .....	19
4.8.1 Computing resources, software, and/or data are corrupted.....	19
4.8.2 Entity public key is revoked.....	19
4.8.3 Entity key is compromised.....	19
4.8.4 Secure facility after a natural or other type of disaster.....	19
4.9 CA Termination .....	19
5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS .....	19
5.1 Physical Controls .....	19
5.1.1 Site location and construction.....	20
5.1.2 Physical access .....	20
5.1.3 Power and air conditioning .....	20
5.1.4 Water exposures .....	20
5.1.5 Fire prevention and protection .....	20
5.1.6 Media storage .....	20
5.1.7 Waste disposal .....	20
5.1.8 Off-site backup .....	20
5.2 Procedural Controls.....	20
5.2.1 Trusted roles.....	20
5.2.2 Number of persons required per task.....	20
5.2.3 Identification and authentication for each role.....	20
5.3 Personnel Controls .....	21
5.3.1 Background, qualifications, experience, and clearance requirements.....	21
5.3.2 Background check procedures .....	21
5.3.3 Training requirements .....	21
5.3.4 Retraining frequency and requirements.....	21
5.3.5 Job rotation frequency and sequence.....	21
5.3.6 Sanctions for unauthorized actions.....	21
5.3.7 Contracting personnel requirements.....	21
5.3.8 Documentation supplied to personnel .....	21
6 TECHNICAL SECURITY CONTROLS .....	21
6.1 Key Pair Generation and Installation .....	21
6.1.1 Key pair generation .....	21
6.1.2 Private key delivery to entity .....	21
6.1.3 Public key delivery to certificate issuer .....	21
6.1.4 CA public key delivery to users .....	21
6.1.5 Key sizes .....	22

## GridKa-CA Certification Policy and Certification Practice Statement Version 1.6

6.1.6 Public key parameters generation .....	22
6.1.7 Parameter quality checking .....	22
6.1.8 Hardware/software key generation .....	22
6.1.9 Key usage purposes (as per X.509 v3 key usage field).....	22
6.2 Private Key Protection.....	22
6.2.1 Standards for cryptographic module.....	22
6.2.2 Private key (n out of m) multi-person control .....	22
6.2.3 Private key escrow .....	22
6.2.4 Private key backup .....	22
6.2.5 Private key archival.....	23
6.2.6 Private key entry into cryptographic module.....	23
6.2.7 Method of activating private key.....	23
6.2.8 Method of deactivating private key.....	23
6.2.9 Method of destroying private key.....	23
6.3 Other Aspects of Key Pair Management .....	23
6.3.1 Public key archival.....	23
6.3.2 Usage periods for the public and private keys.....	23
6.4 Activation Data .....	23
6.4.1 Activation data generation and installation.....	23
6.4.2 Activation data protection.....	23
6.4.3 Other aspects of activation data.....	23
6.5 Computer Security Controls .....	23
6.5.1 Specific computer security technical requirements .....	23
6.5.2 Computer security rating.....	23
6.6 Life Cycle Technical Controls .....	24
6.6.1 System development controls.....	24
6.6.2 Security management controls.....	24
6.6.3 Life cycle security ratings.....	24
6.7 Network Security Controls .....	24
6.8 Cryptographic Module Engineering Controls .....	24
7 CERTIFICATE AND CRL PROFILES .....	24
7.1 Certificate Profile .....	24
7.1.1 Version number(s) .....	24
7.1.2 Certificate extensions .....	24
7.1.3 Algorithm object identifiers .....	25
7.1.4 Name forms .....	25
7.1.5 Name constraints.....	25
7.1.6 Certificate policy Object Identifier .....	26
7.1.7 Usage of Policy Constraints extensions.....	26
7.1.8 Policy qualifier syntax and semantics .....	26
7.1.9 Processing semantics for critical certificate policy extension.....	26
7.2 CRL Profile .....	26
7.2.1 Version number(s).....	26
7.2.2 CRL and CRL entry extensions .....	26
8 SPECIFICATION ADMINISTRATION.....	26
8.1 Specification change procedures.....	26
8.2 Publication and notification policies.....	26
8.3 CPS approval procedures.....	26
9 BIBLIOGRAPHIE.....	27

## 1 INTRODUCTION

The Certification Policy and Certification Practice Statement (CP/CPS) describes the set of rules and operational practices used by GridKa-CA, the Certification Authority (CA) for the Karlsruhe Institute of Technology (KIT) [1] operated by the Department of Distributed Systems and Grids at the Steinbuch Centre for Computing (SCC) [2] for all purposes of Grid-Computing, for issuing certificates. This document is based on the structure suggested by the RFC 2527 [3]

### 1.1 Overview

The GridKa-CA offers identity certification services for science and research in Germany, for the purpose of cross-organisational distributed resource access.

#### 1.1.1 General Definitions

The document makes use of the following terms:

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 )
Authentication	The process of establishing that individuals, organisations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. This process corresponds to the second process involved with identification, as shown in the definition of „identification“ below. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organisation, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.
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.
Certificates - or Public Key Certificates	A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.
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.

## GridKa-CA Certification Policy and Certification Practice Statement Version 1.6

Certificate Revocation Lists (CRL)	A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.
GSI	Grid Security Infrastructure formerly called the Globus Security Infrastructure, is a specification for secret, tamper-proof, delegatable communication between software in a grid computing environment. Secure, authenticatable communication is enabled using asymmetric encryption [4].
Identification	The process of establishing the identity of an individual or organisation, i.e., to show that an individual or organisation is a specific individual or organisation. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organisation corresponds to a real-world identity of an individual or organisation, and (2) establishing that an individual or organisation applying for or seeking access to something under that name is, in fact, the named individual or organisation. A person seeking identification may be a certificate applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.
Personal Information	For the purpose of this document, Personal Information refers to data which is sufficient for the identification of a subscriber according to section 3.1.9. Personal Information will always contain a photo of the individual sufficient for validation of the subscriber, and the subscriber's name sufficient to establish reasonable link to the CN according to section 3.1.2.
Public Key Infrastructure (PKI)	A term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. All of this implies a set of standards for applications that use encryption.
Policy Qualifier	Policy-dependent information that accompanies a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS.
Registration Authority (RA)	An individual or group of people appointed by an organisation that is responsible for identification and authentication of certificate subscribers, but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party (RP)	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Repository	A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.
Subscriber	For certificates issued to individuals, same as certificate subject. In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource.

Within this document the words „MUST“, „MUST NOT“, „REQUIRED“, „SHALL“, „SHALL NOT“, „SHOULD“, „SHOULD NOT“, „RECOMMENDED“, „MAY“, „OPTIONAL“ are to be interpreted as in RFC 2119 [5].

## **1.2 Identification**

Title: GridKa-CA Certificate Policy and Certification Practice Statement

Version: 1.6

Date: 13.08.2011

OID assigned: 1.3.6.1.4.1.2614.5548.1.1.1.6

Expiration: This document is valid until further notice.

## **1.3 Community and Applicability**

GridKa-CA provides PKI services for members of Karlsruhe Institute of Technology and for the German scientific community such as:

- High energy physics experiments: Alice, Atlas, BaBar, CDF, CMS, COMPASS, D0, LHCb
- Further institutions of the Helmholtz-Gemeinschaft: DESY, Gesellschaft für Schwerionenforschung (GSI)
- German institutes and universities engaged in national and international Grid-projects, a current list can be obtained under <http://grid.fzk.de/ca/RA.html>.

### **1.3.1 Certification authorities**

GridKa-CA does not issue certificates to subordinate Certification Authorities at this time.

### **1.3.2 Registration authorities**

The GridKa-CA also performs the role of a RA.

Further RA's are operating at different sites of the German scientific community. The current list of further RA's may be obtained from the following URL: <http://grid.fzk.de/ca/RA.html>.

### **1.3.3 End entities**

The GridKa-CA issues certificates for people, robots, hosts and services involved in the experiments and projects listed in 1.3.

### **1.3.4 Applicability**

The issued certificates are suitable for:

- Client authentication in SSL/TLS and GSI transactions and communication encryption.
- Server authentication SSL/TLS and GSI transactions
- Generating GSI proxies such as specified in RFC3820

The use of the certificates for email signing and encryption is permitted at one's own risk. Certificates issued by the GridKa-CA are only valid in the context of the Grid research activities of the Karlsruhe Institute of Technology and other German Research Institutes involved in the projects listed in 1.3. Any other usage including financial transactions is strictly forbidden.

The ownership of a GridKa-certificate does not imply automatic access to any kind of

computing resources.

## **1.4 Contact Details**

### **1.4.1 Specification administration organization**

The GridKa-CA is managed by the Karlsruhe Institute of Technology in Germany.

### **1.4.2 Contact person**

The CA-manager (contact person for questions related to this policy document or the GridKa-CA in general) is:

Ursula Epting

Karlsruhe Institute of Technology

Steinbuch Centre for Computing

Postfach 3640

76021 Karlsruhe

Germany

Phone: (+ 49) 721/608-26786

Fax: (+ 49) 721/608-926786

E-Mail: [Gridka-CA@kit.edu](mailto:Gridka-CA@kit.edu)

### **1.4.3 Person determining CPS suitability for the policy**

The CA-manager.

## **2 GENERAL PROVISIONS**

### **2.1 Obligations**

#### **2.1.1 CA obligations**

GridKa-CA will:

- maintain and publish this CP/CPS document
- guarantee that operations and infrastructure conform to this CP/CPS
- accept certification requests validated by the RA and issue certificates
- deliver the certificate to end entity
- notify end entities several times in advance that the certificate is going to expire
- accept revocation requests from RA's or end entities
- validate revocation requests
- issue and publish Certificate Revocation Lists (CRLs) according to the rules described in this document
- authorize RA's

#### **2.1.2 RA obligations**

Authorized RA's will:

- authenticate entities requesting a certificate according to the procedures described in this document
- determine if the person has the right to have a GridKa-CA certificate
- approve certificate requests after successful authentication or send validated, signed certificate requests to GridKa-CA
- create and send validated revocation requests to the GridKa-CA

- follow the policies and procedures described in this document

### **2.1.3 Subscriber obligations**

- Read and accept the policies and procedures published in this document
- Generate a key pair using a trustworthy method
- Keep the private key safe and protected
- Use a strong passphrase with a minimum of 12 characters to protect the private key
- Notify the GridKa-CA/RA:
  - in case of possible private key compromise, key destruction or loss
  - when the certificate is no longer required
  - when the information in the certificate becomes wrong or inaccurate

### **2.1.4 Relying party obligations**

- Be familiar with the policies and procedures published in this document
- Check the authenticity of the GridKa-CA root certificate
- Use the certificates for permitted purposes only
- Accept all limitations on the liability of the GridKa-CA as described in section 2.2
- Check the status of the validity of a certificate and check if it has been included in the most recent Certificate Revocation List (CRL) issued by GridKa-CA

### **2.1.5 Repository obligations**

GridKa-CA maintains different online/offline repositories and publishes general information, root certificate, CP/CPS, CRL's, issued certificates there. The repositories shall be protected like described in the sections 2.6.3 and 2.6.4.

## **2.2 Liability**

### **2.2.1 CA liability**

The GridKa-CA:

- guarantees only to control the identity of the subjects requesting a certificate or revocation request according to the procedures described in this document; no other liability, neither implicit nor explicit is accepted
- is run on a best effort basis and does not give any guarantees about the service security or suitability
- will not be held liable for any problems arising from its operation or use made of certificates it issues
- 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 responsibility of the RA's to authenticate the identity of the subscribers requesting certificates according to the practices described in this document and to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied. RA's are not to be held liable or legally responsible for problems that arise out of their operation, or for problems relating to the use or misuse of the certificate requests they verified.

## **2.3 Financial Responsibility**

No financial responsibility is accepted.

### **2.3.1 Indemnification by relying parties**

No stipulation.

### **2.3.2 Fiduciary relationships**

No stipulation.

### **2.3.3 Administrative processes**

KIT finances the operations of the GridKa-CA. Further costs are and will not be covered. The service is voluntary and may be withdrawn at any time, but KIT ensures that archiving and retention requirements as described in this document are met.

## **2.4 Interpretation and Enforcement**

### **2.4.1 Governing law**

This document must be treated according to German law. Legal disputes arising from the operation of the GridKa-CA will be treated according to German Law.

### **2.4.2 Severability, survival, merger, notice**

No stipulation.

### **2.4.3 Dispute resolution procedures**

No stipulation.

## **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 refunds will be given at any time.

## **2.6 Publication and Repository**

### **2.6.1 Publication of CA information**

GridKa-CA publishes the following information through its online repository:

- The GridKa-CA certificate
- The latest CRL
- A copy of this document and copies of all previous documents
- Other relevant information

### **2.6.2 Frequency of publication**

New information will be published as soon as available.

CRLs will be published within one hour after every revocation and at least 7 days before expiration of the previously issued CRL. Certificates will be published within one hour after issuance.

### **2.6.3 Access controls**

GridKa-CA does not impose any access control restrictions to the information available at its public web site (<http://grid.fzk.de/ca>), which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS and other general information.

For the user webinterface (<https://gridka-ca-sec.fzk.de>) access is free to apply for the first user certificate. All other areas are only accessible with a valid certificate. Especially the access to the RA-admin area is secured and only accessible with a registered RA-admin certificate.

The internal webinterface is only accessible by Gridka-CA admins with a valid and registered CA-admin certificate.

The GridKa-CA web sites are maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available on a 24 hours per day, 7 days per week basis.

Paper repositories are protected in a secured cabinet with access only to GridKa-CA personnel. Email repository is only accessible by GridKa-CA personnel.

### **2.6.4 Repositories**

The public GridKa-CA online repository is available at <http://grid.fzk.de/ca> it contains general information, CP/CPS, CRL's, root certificate, a list of RA's

The secured external webinterface for subscribers and RA's is available at <https://gridka-ca-sec.fzk.de>. It contains all issued certificates which are not publicly accessible. Users can only view and download their own certificates, RA's can view only the certificates/requests of the subscribers of their own organisation.

The secured internal CA interface for CA-administrators for the management of everything contains all information about issued certificates or revocation requests, information about users, organisations, RA's.

Paper repositories containing all paper based information.

Email repository contains all e-mails sent to and from GridKa-CA

These repositories shall be protected as described in section 2.6.3

## **2.7 Compliance audit**

### **2.7.1 Frequency of entity compliance audit**

The GridKa-CA may be audited by other CA's or relying parties which are member of one of the PMA's of IGTF to verify its compliance with the rules and procedures specified in this document. Any costs associated to such an audit must be covered by the requesting party.

### **2.7.2 Identity/qualifications of auditor**

No stipulation

### **2.7.3 Auditor's relationship to audited party**

No stipulation

### **2.7.4 Topics covered by audit**

No stipulation

### **2.7.5 Actions taken as a result of deficiency**

No stipulation

### **2.7.6 Communication of results**

No stipulation

## **2.8 Confidentiality**

GridKa-CA collects personal data about the subscribers. These data will be protected according to the German Law. The subscriber acknowledges that such data is being collected by the CA and permits storage of any such data in secured online or paper based repositories.

### **2.8.1 Types of information to be kept confidential**

All information about subscribers that is not present in the certificate and CRL is considered confidential and will not be released outside.

### **2.8.2 Types of information not considered to be confidential**

Information included in issued certificates and CRLs (Full Name, email-address, shortform of the organization) issued by the GridKa-CA is not considered confidential.

### **2.8.3 Disclosure of certificate revocation/suspension information**

If a certificate has to be revoked because of private-key-compromise GridKa-CA may notify:

- The person holding the certificate (personnel or host or service)
- Known relying parties

### **2.8.4 Release to law enforcement officials**

In case of law enforcement, officials will be allowed to inspect the collected personal information after exhibition of regular warrant.

### 2.8.5 Release as part of civil discovery

In case of civil discovery, personal information will not be revealed.

### 2.8.6 Disclosure upon owner's request

Personal information will be revealed upon owner's request.

### 2.8.7 Other information release circumstances

Information about the holder of a certificate may be released to site-managers of relying parties under certain circumstances. In each case the holder of the certificate has to give his/her accordance.

## 2.9 Intellectual Property Rights

This document is based on the following sources:

RFC 2527 by Chokani and Ford [3]

EuGridPMA Minimum Requirements [6]

EuGridPMA Guidelines and Authentication Profiles, Classic X.509 CAs with secured infrastructure [7]

Many parts of the text were taken from:

DutchGrid and NIKHEF Medium-Security X.509 Certification Authority CP/CPS v3.1 [8]

UK e-Science Certification Authority Certificate Policy and Certification Practices Statement Version 1.4 [9]

Thanks to the two authors David Groep (NIKHEF) and Jens Jensen (STFC) for the permission to do so.

The GridKa-CA claims no intellectual property rights on issued certificates, practice/policy specifications, names or keys.

## 3 IDENTIFICATION AND AUTHENTICATION

### 3.1 Initial Registration

#### 3.1.1 Types of names

To each entity the GridKa-CA assigns a Distinguished Name (DN, X.500) that identifies each entity uniquely. The DN is inserted in the subject field of the issued certificate to bind the entity to the certificate. The DN must be a non-empty printable string and must consist only of characters from the set: '0' – '9', 'a' – 'z', 'A' – 'Z', '-', '!', ':', '/', ''.

Following naming attributes may be used in entities' DN. See also 7.1.4

Attribute	Presence	Value	Comment
„countryName“ (C)	Optional	„C=DE“	For all certificates
„organizationName“ (O)	Mandatory	„O=GermanGrid“	For all certificates
„organizationalUnitName“ (OU)	Mandatory	„OU=...“	For all certificates, this is a shortform of the official name of the institution or organizational unit or department employing the subscriber or running the server/service.

„commonName“ (CN)	Mandatory	„CN=...“	See description below
-------------------	-----------	----------	-----------------------

For personal certificates the CN must contain at least one first name followed by the surname as presented in the identity card issued by the government or the organization the person belongs to.

For robot certificates the CN must start with the string „Robot: grid function“ followed by “ – first name surname“ of the subscriber.

For server certificates the CN must contain the fully qualified domain name (FQDN) of the server, maybe with the prefix „host/“.

For service certificates the CN must contain the fully qualified hostname where the service is running, prefixed with the name of the service „service-name/“.

### 3.1.2 Need for names to be meaningful

The Subject Name in a certificate must be meaningful and must bear a reasonable association with the authenticated name or names of the subscriber. The subscriber must choose a representation of their name in the permitted character set as specified in section 3.1.1.

The name used for the „OrganizationalUnitName“ may be the full name of the organisation the subscriber belongs to or an abbreviation of it. The chosen name must be in the permitted character set and will be mediated between the RA and the CA before certification service to the institution will be started.

### 3.1.3 Rules for interpreting various name forms

See Section 3.1.1 and 3.1.2

### 3.1.4 Uniqueness of names

The DN for each certificate must be unique with the exception of certificate rekeying. In case of real subject name duplication, additional numbers and/or letters will be appended to the DN to guarantee uniqueness.

### 3.1.5 Name claim dispute resolution procedure

Name claim disputes will be solved by the GridKa-CA

### 3.1.6 Recognition, authentication and role of trademarks

No stipulation

### 3.1.7 Method to prove possession of private key

GridKa-CA is currently not proving the possession of the private key relating to certificate requests.

### 3.1.8 Authentication of organization identity

GridKa-CA/RA verifies the identity of organizations by checking:

- that the organization is known to be part of the grid-computing projects or related experiments (mentioned in 1.3) by checking with the Institute Manager or the Grid-Department-Manager of the Karlsruhe Institute of Technology.
- that the organization is operating in Germany, by checking official contact information.

### **3.1.9 Authentication of individual identity**

Authorized RA's are verifying the identity of a natural person by

- Personal contact, comparing the information in the identity card (names, date of birth, place of birth of the subscriber, nationality, the type and last 5 numbers of the identity piece, contact information) with the information presented in the registration form and compares the photograph in the identity card with the real appearance of the person.
- The RA keeps the registration form in a secure place or sends it to the GridKa-CA via signed e-mail, mail or fax for archival.

In case the entity to be certified is a machine or a service the person in charge has to fulfil the process defined in the section above and give prove that he/she is adequately authorized. Furthermore it will be checked if the IP-adress corresponding to the FQDN is within the range of the requesting organization.

### **3.2 Routine Rekey**

Rekey before expiration can be accomplished by sending a rekey request based on a new public key after successful authentication with current certificate at our web interface. RA's check if the requestor has still the right to receive a certificate before they approve the request. Rekey after expiration follows the same authentication procedure as for initial registration.

### **3.3 Rekey after Revocation**

Rekey after revocation follows the same rules as an initial registration.

### **3.4 Revocation Request**

Certificate revocation requests can be submitted by anyone via the user webinterface or by written form signed manually or E-mail sent to GridKa-CA@kit.edu signed with a valid GridKa-CA certificate or by telephone. The CA verifies the request using electronic or other appropriate means.

## **4 OPERATIONAL REQUIREMENTS**

### **4.1 Certificate Application**

The minimum key length for all certificates is 1024 bits. The default validity period is 1 year and one month. Each applicant must generate its own key pair using either Globus grid-cert-request, OpenSSL [10] (or similar software) or a secure Online-Procedure provided by GridKa-CA.

Certificate requests in PEM-format are uploaded to the webinterface or sent by e-mail to GridKa-CA@kit.edu. Depending on if the requester is a person or a machine or a service the procedures outlined in 3.1.9 are applied.

Help on the configuration of Globus/OpenSSL files is available from the repository (see 2.6.4). Non-conforming requests will not be accepted.

### **4.2 Certificate Issuance**

GridKa-CA issues the certificate if, and only if, the authentication of the subject is successful according to 3.1.9. The certificate will be provided at the user webinterface for

download or sent to the applicant by (signed) e-mail or the applicant will be informed about the reason why the certificate could not be issued.

#### **4.3 Certificate Acceptance**

No stipulation.

#### **4.4 Certificate Suspension and Revocation**

##### **4.4.1 Circumstances for revocation**

A certificate will be revoked in the following circumstances:

- The subscriber's private key has been lost or is suspected to be compromised
- The information in the certificate is wrong or inaccurate
- The subscriber has failed to comply with the rules in this policy
- The subscriber no longer needs the certificate to access relying parties' resources
- The host/service to which the certificate has been issued has been retired

##### **4.4.2 Who can request revocation**

The revocation of the certificate can be requested by:

- The certificate subscriber or in case of host/service certificates each person which is responsible for the host/service.
- Any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data or relation with GridKa-CA
- GridKa-CA/RA

##### **4.4.3 Procedure for revocation request**

The entity requesting revocation of a certificate must send the revocation request by signed e-mail to the GridKa-CA/RA or submit the request via the webinterface. If this is not possible the CA/RA must be contacted directly. Authentication can be performed as described in 3.1.9.

##### **4.4.4 Revocation request grace period**

No stipulation.

##### **4.4.5 Circumstances for suspension**

No stipulation.

##### **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 after every certificate revocation or at least once every 30 days and at least 7 days before the stated next update time in the latest-issued CRL.

#### **4.4.10 CRL checking requirements**

No stipulation.

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

No stipulation.

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

No stipulation.

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

No stipulation.

#### **4.4.14 Checking requirements for other forms of revocation advertisements**

No stipulation.

#### **4.4.15 Special requirements of key compromise**

No stipulation.

### **4.5 Security Audit Procedures**

#### **4.5.1 Types of event recorded**

- opening and closing of the cabinet which protects the ca-machine
- boots of the ca-machine
- interactive logins on the ca-machine

#### **4.5.2 Frequency of processing log**

No stipulation.

#### **4.5.3 Retention period for audit logs**

The minimum retention period is 3 years.

#### **4.5.4 Protection of audit log**

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

#### **4.5.5 Audit log backup procedures**

Audit log files are copied to an off-line medium, which is saved in safe storage.

#### **4.5.6 Audit collection system (internal vs external)**

No stipulation.

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

No stipulation.

#### **4.5.8 Vulnerability assessments**

No stipulation.

### ***4.6 Records Archival***

#### **4.6.1 Types of event recorded**

The following events are recorded in either digital or paper-based archives:

- Certification requests
- Revocation requests
- Identity verification procedures
- Issued certificates
- Issued CRLs
- E-mail messages sent and received by the GridKa-CA/RA

#### **4.6.2 Retention period for archive**

All electronic data and logs will be kept for a minimum of 3 years.

#### **4.6.3 Protection of archive**

Records of the offline CA machine are backed up on removable media, which are stored in a room with restricted access.

#### **4.6.4 Archive backup procedures**

Records of the offline CA machine are backed up on removable media, which are stored in a room with restricted access.

For external and internal web interfaces the stored information is backed up automatically daily to tape storage. Once a month additionally all data is archived in the tape storage.

#### **4.6.5 Requirements for time-stamping of records**

Not defined.

#### **4.6.6 Archive collection system (internal or external)**

The archive system is internal to the GridKa-CA for the offline CA machine and internal to Steinbuch Centre for Computing for the external and internal web interfaces.

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

Archive information can be obtained by CA personnel, using the archiving software's commands.

### ***4.7 Key changeover***

CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA-key should be generated one year before the old one loses validity. From that point on new certificates are signed by the new CA-key. The new CA-key is posted in the on-line repository.

#### **4.8 Compromise and Disaster Recovery**

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

These issues will be solved according to internal procedures.

##### **4.8.2 Entity public key is revoked**

No stipulation.

##### **4.8.3 Entity key is compromised**

If the CA private key is compromised - or suspected to be - the CA will:

- Inform subscribers, RAs and other relying parties.
- Terminate the issuance and distribution of certificates and CRLs
- Notify relevant security contacts

##### **4.8.4 Secure facility after a natural or other type of disaster**

Recovery after natural or other disasters will be done following internal procedures.

#### **4.9 CA Termination**

Upon termination the GridKa-CA will:

- Notify subscribers, RAs and relying parties one and a half year in advance of the planned termination.
- Terminate the issuance and distribution of certificates and CRLs.
- Notify relevant security contacts.
- Notify widely as possible the end of the service.
- Keep all archived data for 3 years after termination and destroy all data securely afterwards.

### **5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**

#### **5.1 Physical Controls**

The CA operates in a controlled environment, where access is restricted to authorized people. The CA-machine is additionally protected by a secure cabinet where access is restricted to CA-personnel.

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

The GridKa-CA is located at the Steinbuch Centre for Computing (SCC) of the Karlsruhe Institute of Technology (KIT). Access to KIT is restricted to authorized people. Access to the room which the ca-machine is additionally restricted to authorized personnel of SCC and access to the cabinet holding the ca-machine is restricted to authorized CA-personnel.

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

Physical access to the Hardware is restricted to authorized CA-personnel. All removable media is stored in a secure cabinet.

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

The building has an air conditioning system and the CA machines are connected to an

UPS system.

#### **5.1.4 Water exposures**

No stipulation.

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

The building has a fire alarm system.

#### **5.1.6 Media storage**

The GridKa-CA key and Backup copies of CA related information is kept in several removable storage media in secure cabinets .

#### **5.1.7 Waste disposal**

If personal information is concerned waste paper will be shredded, waste harddisks will be shredded using appropriate tools.

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

No stipulation.

### ***5.2 Procedural Controls***

#### **5.2.1 Trusted roles**

No stipulation.

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

No stipulation.

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

No stipulation.

### ***5.3 Personnel Controls***

#### **5.3.1 Background, qualifications, experience, and clearance requirements**

CA personnel is recruited from the department of Distributed Systems and Grid.

#### **5.3.2 Background check procedures**

No other personnel are authorized to access offline CA facilities without the physical presence of CA personnel.

#### **5.3.3 Training requirements**

No stipulation.

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

No stipulation.

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

Job rotation is not performed.

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

No stipulation.

### **5.3.7 Contracting personnel requirements**

No stipulation.

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

- Copies of this document
- GridKa-CA Operation Manual

## **6 TECHNICAL SECURITY CONTROLS**

### ***6.1 Key Pair Generation and Installation***

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

Keys for the GridKa-CA are generated by CA staff on a dedicated machine not connected to any kind of network. The software package is OpenSSL (0.9.6.b) or higher. Each subscriber must generate her/his own key pair. The GridKa-CA does not generate any keys for entities.

#### **6.1.2 Private key delivery to entity**

No private keys are delivered to entities

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

Public keys are delivered by e-mail, SSL over http or/and floppy or other removable media.

#### **6.1.4 CA public key delivery to users**

The CA certificate can be downloaded from the GridKa-CA web sites (<http://grid.fzk.de/ca/> or <https://gridka-ca-sec.fzk.de> ) or Terena Tacar (<https://www.tacar.org/cert/list> ).

#### **6.1.5 Key sizes**

- The minimum key length for a personnel or server/service certificate is 1024 bit, but a key length of 2048 bits is recommended.
- The CA key length is 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**

Key generation is performed by software.

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

Keys may be used for authentication, non-repudiation, data encipherment, message integrity, session establishment and signing of proxy certificates.

The GridKa-CA private key can only sign certificates and CRLs.

## **6.2 Private Key Protection**

Subscribers must adequately protect the private key associated with the certificate issued to them. The level of protection considered adequate depends on the type of certificate:

- Personal certificates issued to human individuals must be stored in encrypted form only, and be protected by activation data (a passphrase) that is strong and has a minimum of 12 characters length. It is up to the user to ensure that the private key is not unduly copied around or stored on shared file systems. The user shall protect the encrypted private key via appropriate file-system-level protections.
- Robot, host and service certificates may be stored in unencrypted form. The responsible person shall protect the private key via appropriate file-system-level protection, such that only the person or group of persons responsible for the service or host has access to this key. The subscriber is and must be responsible for the host in which the credentials are installed, and must be responsible for granting and revoking privileged access to the file system by others.

### **6.2.1 Standards for cryptographic module**

### **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 GridKa-CA private key is kept encrypted in multiple copies in floppy disks or CD-ROMs in safe places. The passphrase is, for emergencies in a sealed envelope kept in a secure cabinet. It's controlled from time to time if the envelope is unopened.

### **6.2.5 Private key archival**

No stipulation.

### **6.2.6 Private key entry into cryptographic module**

No stipulation.

### **6.2.7 Method of activating private key**

GridKa-CA private key is protected by a passphrase of at least 15 characters.

### **6.2.8 Method of deactivating private key**

Logging off the machine will deactivate private key.

### **6.2.9 Method of destroying private key**

After termination of the GridKa-CA service and expiration of archival period for archives, the private key will be destroyed using current best practices.

## **6.3 Other Aspects of Key Pair Management**

The GridKa-CA certificate has currently a validity of 11 years and will expire on Tuesday, 10th June 2014.

### **6.3.1 Public key archival**

### **6.3.2 Usage periods for the public and private keys**

## **6.4 Activation Data**

The GridKa-CA private key is protected by a passphrase of at least 15 characters length.

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

No stipulation.

### **6.4.2 Activation data protection**

No stipulation.

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

No stipulation.

## **6.5 Computer Security Controls**

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

- The external and internal web interfaces and offline CA machine are under the administration of the GridKa-CA. They are maintained at a high level of security by applying all the relevant patches, the configuration is reduced to the base minimum.
- The external and internal web interfaces are additionally monitored using a host-based intrusion detection system to detect unauthorized software changes. Strict firewall rules are applied.

### **6.5.2 Computer security rating**

No stipulation.

## **6.6 Life Cycle Technical Controls**

### **6.6.1 System development controls**

No stipulation.

### **6.6.2 Security management controls**

No stipulation.

### **6.6.3 Life cycle security ratings**

No stipulation.

### **6.7 Network Security Controls**

- The CA signing machine is kept off-line.
- CA machines other than the signing machine are protected by a firewall and host-based intrusion detection system.

### **6.8 Cryptographic Module Engineering Controls**

No stipulation.

## **7 CERTIFICATE AND CRL PROFILES**

### **7.1 Certificate Profile**

#### **7.1.1 Version number(s)**

GridKa-CA and subscriber certificates: X.509 v3.

#### **7.1.2 Certificate extensions**

- CA-certificate:

X509v3 Basic Constraints: critical CA:TRUE  
X509v3 Subject Key Identifier:  
C6:75:C9:28:AC:D1:0B:FC:3C:FF:B9:B5:1E:D3:5F:3B:80:62:12:34  
X509v3 Authority Key Identifier:  
keyid:C6:75:C9:28:AC:D1:0B:FC:3C:FF:B9:B5:1E:D3:5F:3B:80:62:12:34  
DirName:/C=DE/O=GermanGrid/CN=GridKa-CA serial:00  
X509v3 Key Usage: critical Certificate Sign, CRL Sign  
X509v3 Issuer Alternative Name: email:[gridka-ca@iwr.fzk.de](mailto:gridka-ca@iwr.fzk.de)  
X509v3 CRL Distribution Points: URI:<http://grid.fzk.de/ca/gridka-crl.pem>  
Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA  
Netscape CA Revocation Url: <http://grid.fzk.de/ca/gridka-crl.pem>  
Netscape Base Url: <http://grid.fzk.de/ca>  
Netscape CA Policy Url: <http://grid.fzk.de/ca/gridka-cps.pdf>

- User/Host/Service-certificates:

Basic Constraints: critical, CA FALSE  
Key Usage: critical, Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment  
Subject Key Identifier: unique identifier of the subject (hash)  
Authority Key Identifier: unique identifier of the issuer  
Subject Alternative Name: subject's e-mail address or FQDN  
Issuer Alternative Name: issuer's e-mail address  
CRL Distribution Points: URI:<http://grid.fzk.de/ca/>

## GridKa-CA Certification Policy and Certification Practice Statement Version 1.6

Certificate Policies: The OID of the CP/CPS (OID 1.3.6.1.4.1.2614.5548.1.1.1.6), OID referring to the IGTF Profile for „Classic X.509 Certification Authorities with secured infrastructure“ (OID 1.2.840.113612.5.2.2.1)

Netscape Cert Type: SSL Client and/or SSL Server, S/MIME

Netscape Comment: CP/CPS version

Netscape Base Url: <http://grid.fzk.de/ca>

Netscape Revocation Url: <http://grid.fzk.de/ca/gridka-crl.der>

Netscape CA Policy Url : <http://grid.fzk.de/ca/gridka-cps.pdf>

- Robot Certificates:

Subject Key Identifier: unique identifier of the subject (hash)

Authority Key Identifier: unique identifier of the issuer

Subject Alternative Name: subject's e-mail address

Issuer Alternative Name: issuer's e-mail address

CRL Distribution Points: URI:<http://grid.fzk.de/ca/>

Certificate Policies: The OID of the CP/CPS (OID 1.3.6.1.4.1.2614.5548.1.1.1.6), OID referring to the IGTF Profile for „Classic X.509 Certification Authorities with secured infrastructure“ (OID 1.2.840.113612.5.2.2.1), OID of the IGTF profile for robot certificates with Private Key protection: Key material held in files (OID 1.2.840.113612.5.2.3.1.2)

Netscape Cert Type: SSL Client, S/MIME

Netscape Comment: CP/CPS version

Netscape Base Url: <http://grid.fzk.de/ca>

Netscape Revocation Url: <http://grid.fzk.de/ca/gridka-crl.der>

Netscape CA Policy Url : <http://grid.fzk.de/ca/gridka-cps.pdf>

### 7.1.3 Algorithm object identifiers

No stipulation.

### 7.1.4 Name forms

The issuer name is: „C=DE/O=GermanGrid/CN=GridKa-CA“

The subscriber subject name may start with „C=DE“ as the first attribute, followed by „O=GermanGrid“ and „OU=...“ and „CN=Subject-Name“

The „OU=...“ is the shortform of the name of the institution, the user or host/service are related to - see 1.3. A current list of all available OU's can be obtained at <http://grid.fzk.de/ca/RA.html>

The permissible form therefore is: „/[C=DE]/O=GermanGrid/OU=.../CN=...“

### 7.1.5 Name constraints

Each certificate must contain „O=GermanGrid“ in its subject

### 7.1.6 Certificate policy Object Identifier

Subscriber certificates contain the certificate policy object identifier (OID) for this document: 1.3.6.1.4.1.2614.5548.1.1.1.6

Version 1.6

The structure is as follows:

IANA	1.3.6.1.4.1.
Forschungszentrum Karlsruhe	2614.
Internal number	5548.
CA	1.
CP/CPS	1.
Version number, major	1.
Version number, minor	6

They also may contain OID's referring to the IGTF-profiles to which they comply.  
Robot certificates include the 1SCP robot OID.

### **7.1.7 Usage of Policy Constraints extensions**

No stipulation

### **7.1.8 Policy qualifier syntax and semantics**

No stipulation

### **7.1.9 Processing semantics for critical certificate policy extension**

No stipulation

## **7.2 CRL Profile**

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

X.509 v2

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

Not defined.

## **8 SPECIFICATION ADMINISTRATION**

### **8.1 Specification change procedures**

Users will not be warned in advance of changes to GridKa-CA 's policy and CPS. Relevant changes will be made as widely available as possible, especially they will be communicated to the PMA's.

### **8.2 Publication and notification policies**

The GridKa-CA policy is available at <http://grid.fzk.de/ca/gridka-cps.pdf>, previous versions can be found at <http://grid.fzk.de/ca/> .

### **8.3 CPS approval procedures**

No stipulation.

## 9 BIBLIOGRAPHIE

- [1] Karlsruhe Institute of Technology (KIT), <http://www.kit.edu>
- [2] Steinbuch Centre for Computing (SCC), <http://www.scc.kit.edu>
- [3] 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>
- [4] GSI Definition, [http://en.wikipedia.org/wiki/Grid\\_Security\\_Infrastructure](http://en.wikipedia.org/wiki/Grid_Security_Infrastructure)
- [5] S. Bradner, „Key words for use in RFCs to Indicate Requirement Levels“, RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>
- [6] EuGridPMA, <http://eugridpma.org/guidelines/EUGridPMA-minreq-classic-20040402-3-1.pdf>
- [7] EuGridPMA, <http://www.eugridpma.org/guidelines/IGTF-AP-classic-4-2.pdf>
- [8] Dutch Grid, Certification Policy and Practice Statement Version 3.1, David Groep, <http://ca.dutchgrid.nl/medium/policy/DutchGridCA-CPCPS-3.1.pdf>
- [9] UK e-Science Certification Authority, Certificate Policy and Certification Practices Statement, Jens Jensen, Version 1.4, [http://www.ngs.ac.uk/sites/default/files/cps-1\\_4.pdf](http://www.ngs.ac.uk/sites/default/files/cps-1_4.pdf)
- [10] The OpenSSL Project, <http://openssl.org>