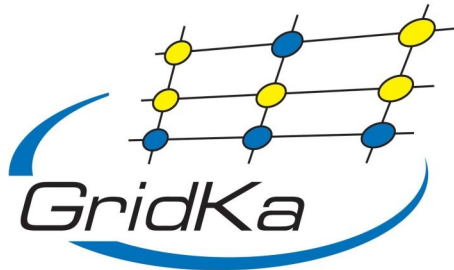




Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft



GridKa-CA

Certificate Policy
and
Certification Practice Statement

Version 1.3

June 2006

Inhaltsverzeichnis

1 Introduction	5
1.1 Overview.....	5
1.1.1 General Definitions.....	5
1.2 Identification.....	6
1.3 Community and Applicability	6
1.3.1 Certification Authorities	6
1.3.2 Registration Authorities (RA).....	6
1.3.3 End entities	6
1.3.4 Applicability	6
1.3.5 User Restrictions	6
1.4 Contact Details	7
2 General Provisions	7
2.1 Obligations	7
2.1.1 CA Obligations.....	7
2.1.2 RA Obligations.....	7
2.1.3 Subscriber Obligations	7
2.1.4 Relying Party Obligations	8
2.1.5 Repository Obligations	8
2.2 Liability	8
2.3 Financial responsibility	8
2.4 Interpretation and Enforcement	8
2.5 Fees	8
2.6 Publication and Repositories	8
2.6.1 Publication of CA Information	8
2.6.2 Frequency of Publication	8
2.6.3 Access Controls	8
2.6.4 Repositories	9
2.7 Compliance Audit	9
2.8 Confidentiality	9
2.8.1 Types of information to be kept confidential.....	9
2.8.2 Types of information not considered to be confidential.....	9
2.8.3 Disclosure of certificate revocation/suspension information.....	9
2.8.4 Release to law enforcement officials.....	9
2.8.5 Release as part of civil discovery.....	9
2.8.6 Disclosure upon owner's request.....	9
2.8.7 Other information release circumstances.....	9
2.9 Intellectual Property Rights	10
3 Identification and Authentication	10
3.1 Initial Registration	10
3.1.1 Types of Names	10
3.1.1.1 Country.....	10
3.1.1.2 Organization.....	10
3.1.1.3 Organizational Unit.....	10
3.1.1.4 Name (Common Name).....	10
3.1.2 Need for names to be meaningful.....	11
3.1.3 Rules for interpreting various name forms.....	11
3.1.4 Uniqueness of Names	11
3.1.5 Name claim dispute resolution procedure.....	11
3.1.6 Recognition, authentication and role of trademarks.....	11
3.1.7 Method to Prove Possession of Private Key.....	11
3.1.8 Authentication of Organization Identity	11

3.1.9 Authentication of Individual Identity	11
3.2 Routine Rekey	12
3.3 Rekey After Revocation	12
3.4 Revocation Request	12
4 Operational Requirements	12
4.1 Certification Application	12
4.2 Certificate Issuance.....	12
4.3 Certificate Acceptance	12
4.4 Certificate Suspension and Revocation	12
4.4.1 Circumstances for Revocation	12
4.4.2 Who can request revocation	13
4.4.3 Procedure for Revocation Request	13
4.4.4 Circumstances for Suspension	13
4.4.5 Who can request suspension	13
4.4.6 Procedure for suspension request	13
4.4.7 Limits on Suspension Period	13
4.4.8 CRL Issuance Frequency	13
4.4.9 CRL Checking Requirements for Relying Parties	13
4.4.10 Online Revocation/status Checking Availability	13
4.4.11 Online Revocation Checking Requirements	13
4.4.12 Other Forms of Revocation Advertisement	13
4.4.13 Requirements for Relying Parties on Other Forms of Revocation Advertisement	14
4.4.14 Variations of the Above in Case of Private Key Compromise	14
4.5 Security Audit Procedures	14
4.5.1 Types of Events Audited	14
4.5.2 Processing Frequency of Audit Logs	14
4.5.3 Retention Period for Audit Logs	14
4.5.4 Protection of Audit Logs	14
4.5.5 Backup Procedures	14
4.5.6 Accumulation System	14
4.5.7 Vulnerability Assessments	14
4.6 Records Archival	14
4.6.1 Types of Events Recorded.....	14
4.6.2 Retention Period for Archives	14
4.6.3 Protection of Archive	14
4.6.4 Archive Backup Procedures	15
4.6.5 Time-stamping Requirements	15
4.6.6 Archive Collection System	15
4.6.7 Procedures to Obtain and Verify Archive Information	15
4.7 Key Changeover	15
4.8 Compromise and Disaster Recovery	15
4.9 CA Termination	15
5 Physical, Procedural, and Personnel Security Controls	15
5.1 Physical Security Controls	15
5.1.1 Site Location	15
5.1.2 Physical Access	15
5.1.3 Power and Air Conditioning	15
5.1.4 Water Exposures	16
5.1.5 Fire Prevention and Protection	16
5.1.6 Media Storage	16
5.1.7 Waste Disposal	16
5.1.8 Off-site Backup	16
5.2 Procedural Controls.....	16
5.3 Personnel Security Controls	16

5.3.1	Background Checks and Clearance Procedures for CA Personnel.....	16
5.3.2	Background Checks and Security Procedures for other Personnel.....	16
5.3.3	Training Requirements and Procedures	16
5.3.4	Training Period and Retraining Procedures	16
5.3.5	Frequency and Sequence of Job Rotation	16
5.3.6	Sanctions Against Personnel	16
5.3.7	Controls on Contracting Personnel	16
5.3.8	Documentation Supplied to Personnel	16
6	Technical Security Controls	17
6.1	Key Pair Generation and Installation	17
6.1.1	Key Pair Generation	17
6.1.2	Private Key Delivery to Entity	17
6.1.3	Public Key Delivery to Certificate Issuer	17
6.1.4	CA Public Key Delivery to Users	17
6.1.5	Key Sizes	17
6.1.6	Public Key Parameters Generation	17
6.1.7	Parameter Quality Checking	17
6.1.8	Hardware/software key generation	17
6.1.9	Key Usage Purposes	17
6.2	Private Key Protection	17
6.2.1	Private Key (n out of m) Multi-person Control	17
6.2.2	Private Key Escrow	17
6.2.3	Private Key Archival and Backup	17
6.3	Other Aspects of Key Pair Management	18
6.4	Activation Data	18
6.5	Computer Security Controls	18
6.5.1	Specific Security Technical Requirements	18
6.5.2	Computer Security Rating.....	18
6.6	Life Cycle Security Controls	18
6.7	Network Security Controls	18
6.8	Cryptographic Module Engineering Controls	18
7	Certificate and CRL Profile	18
7.1	Certificate Profile	18
7.1.1	Version Number	18
7.1.2	Certificate Extensions	18
7.1.3	Algorithm Object Identifiers	19
7.1.4	Name Forms	19
7.1.5	Name Constraints.....	19
7.1.6	Certificate Policy Object Identifier	19
7.1.7	Usage of Policy Constraints Extensions.....	19
7.1.8	Policy Qualifier Syntax and Semantics	19
7.2	CRL Profile	20
7.2.1	Version	20
7.2.2	CRL and CRL Entry Extensions	20
8	Specification Administration.....	20
8.1	Specification Change Procedures	20
8.2	Publication and Notification Procedures	20
8.3	CPS Approval Procedures	20
9	Bibliographie.....	20

1 Introduction

1.1 Overview

This document describes the set of rules and operational practices used by GridKa-CA, the Certification Authority for the Forschungszentrum Karlsruhe in der Helmholtz-Gemeinschaft [1] for all purposes of Grid-Computing, for issuing certificates. This document is based on the structure suggested by the RFC 2527 [2].

1.1.1 General Definitions

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)

CA - Certification Authority

An authority trusted by one or more users to create and assign public key certificates.

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.

CP - Certificate Policy

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 for the trading of goods within a given price range.

CPS - Certification Practice Statement

A statement of the practices which a certification authority employs in issuing certificates.

CRL - Certificate Revocation Lists

A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

PKI - Public Key Infrastructure

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 certificate policy identifier in an X.509 certificate.

RA - Registration Authority

An entity that is responsible for identification and authentication of certificate subjects, but does not sign or issue certificates.

Relying Party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

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 [3].

1.2 Identification

Title: GridKa-CA Certificate Policy (CP) and Certification Practice Statement (CPS).

Version: 1.3

Date: 09.06.2006

OID assigned: 1.3.6.1.4.1.2614.5548.1.1.1.3

Expiration: This document is valid until further notice.

1.3 Community and Applicability

GridKa-CA provides PKI services for members of Forschungszentrum Karlsruhe in general and for the German scientific community such as:

- High energy physics experiments: Alice, Atlas, BaBar, CDF, CMS, COMPASS, D0, LHCb
- International projects: CrossGrid, DataGrid, LHC Computing Grid Project, GridLab, EGEE
- Further institutions of the Helmholtz-Gemeinschaft: DESY, GSI
- German institutes and universities engaged in Grid-projects, a current list can be obtained under <http://grid.fzk.de/ca/orga.html>

1.3.1 Certification Authorities

GridKa-CA doesn't issue certificates to subordinate Certification Authorities at this time.

1.3.2 Registration Authorities (RA)

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 registration authorities may be obtained from the following URL: <http://grid.fzk.de/ca/ra-list.html>.

1.3.3 End entities

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

1.3.4 Applicability

The issued certificate types and suitability are as follows:

Personnel, Server and Application certificates: authentication and communication encryption.

1.3.5 User Restrictions

Certificates issued by the GridKa-CA are only valid in the context of the Grid research activities of the Forschungszentrum Karlsruhe 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

The GridKa-CA is managed by the Forschungszentrum Karlsruhe in Germany.
The contact person for questions related to this document or GridKa-CA in general is:

Ursula Epting
Forschungszentrum Karlsruhe in der Helmholtz-Gemeinschaft
Institut fuer Wissenschaftliches Rechnen (IWR)
Postfach 3640
76021 Karlsruhe
Germany
Phone: (+ 49) 7247/82-6786
Fax: (+ 49) 7247/82-7768
E-Mail: GridKa-CA@iwr.fzk.de

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

GridKa-CA will:

- issue certificates based on validated requests
- accept certification requests validated by the RA
- deliver the certificate to end entity
- notify end entities three and one week in advance that the certificate is going to expire
- accept revocation requests from RA's or end entities
- issue and publish Certificate Revocation Lists (CRLs) according to the rules described in this document

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
- 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

- Read and accept the policies and procedures published in this document
- See paragraph 4.4.9 on CRL checking requirements for relying parties
- Use the certificates for permitted purposes only

2.1.5 Repository Obligations

GridKa-CA will publish all information described in section 2.6.1 on its web server <http://grid.fzk.de/ca/>.

2.2 Liability

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

2.3 Financial responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

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.

2.5 Fees

No fees are charged.

2.6 Publication and Repositories

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 as soon as issued and at least every month.

2.6.3 Access Controls

GridKa-CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS.

The GridKa-CA web site is 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.

GridKa-CA may impose a more restricted access control policy to the repository at its discretion.

2.6.4 Repositories

The GridKa-CA online repository is available at <http://grid.fzk.de/ca>.

2.7 Compliance Audit

The GridKa-CA may be audited by other trusted CA's 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.

2.8 Confidentiality

GridKa-CA collects personal information about the subscribers (e.g. full name, organization, a copy of the identity card, telephone number, e-mail-address and in case of a RA a copy of the handwritten signature). These data will be protected according to the German Law.

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 [2]

EuGridPMA Minimum Requirement [4]

INFN Certificate Policy and Certificate Practice Statement [5]

LIP Certificate Policy and Certificate Practice Statement [6]

Cern Certificate Policy and Certificate Practice Statement [7]

CNRS Certificate Policy and Certificate Practice Statement [8]

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.

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

3.1.1.1 Country

Necessity: Optional

Comment: For personal certificates, this is the country of residence of the subscriber. For server/application certificates, it is the country where the server/application is located.

3.1.1.2 Organization

Necessity: Mandatory

Comment: For personal certificates and server/application certificates the name of the Organization is "GermanGrid".

3.1.1.3 Organizational Unit

Necessity: Mandatory

Comment: For personal certificates, this is a shortform of the official name of the institution or organizational unit or department employing the subscriber. For server/application certificates, it is a shortform of the official name of the organizational unit or department running the server/application.

3.1.1.4 Name (Common Name)

Necessity: Mandatory

Comment: For personal certificates it is the first name followed by the surname as presented in the identity card issued by the government or the organization the person belongs to. For server certificates it is the fully qualified domain name of the server maybe with the prefix „host/“. For application certificates it is the fully qualified hostname where the application is running prefixed with the name of the application „service/“.

3.1.2 Need for names to be meaningful

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber.

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 distinguished name for each certificate must be unique. In case of real subject name duplication, additional numbers and/or letters will be appended to the distinguished name 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 Forschungszentrum Karlsruhe.
- 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 person by

- Personal contact checking the identity card, comparing photograph and registering the number of the identity piece or keeping a copy of the identity card.
- If the RA is located at a distant organization there are two different options:
 - the RA keeps a copy of the identity card and sends the request per email to GridKa-CA/RA signed with his/her personal certificate
 - or
 - the RA sends the copy of the identity card, manually signed per post to the GridKa-CA/RA. If any doubts exist that the copy couldn't be correct the GridKa-RA can contact the RA of the organization to get some further proof. The GridKa-RA then calls the requestor, using the indicated telephone number (it must belong to the range of the assigned organization and must not be a private number of the individual). During the call digital fingerprints or content data can be compared.

For natural persons the subject name must be conforming to the name in the identity card.

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 IP-adress corresponding to the full qualified domain name is within the range of the requesting organization.

The GridKa-RA shall record the issuance of each certificate, containing

- the identity of the person performing the identification
- the number and type of the identity card or the number of the copy of the identity card which corresponds to the serial number of the certificate.
- whether the contact was personal or by post and phone
- the date and time of the verification or in case any reasons why the verification failed
- the name of the RA which signed the copy of the identity card or the electronic request.

3.2 Routine Rekey

Rekey before expiration can be accomplished by sending a rekey request based on a new public key. It will be checked with the distant RA if the requestor has still the right to receive a certificate. Rekey after expiration follows the same authentication procedure as for a new certificate.

3.3 Rekey After Revocation

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

3.4 Revocation Request

Certificate revocation requests should be submitted by written form signed manually or E-mail sent to GridKa-CA@iwr.fzk.de signed with a valid GridKa-CA certificate. The CA inspects the signature electronically or based on the declaration of identity mentioned in 3.1.9

4 Operational Requirements

4.1 Certification 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 [9] (or similar software) or a secure Online-Procedure provided by GridKa-CA.

Certificate requests in PEM-format are sent by e-mail to GridKa-CA@iwr.fzk.de. 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 are available from Website of the Forschungszentrum Karlsruhe. Non-conforming requests won't 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 sent to the applicant by (signed) e-mail or the applicant will be informed about the reason why the certificate couldn't be issued.

4.3 Certificate Acceptance

Not defined.

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 subject has failed to comply with the rules in this policy
- The subscriber no longer needs the certificate to access relying parties' resources
- The system 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/application 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
- GridKa-CA/RA

4.4.3 Procedure for Revocation Request

The entity requesting the certificate must send the revocation request by signed e-mail to the GridKa-CA/RA. 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 Circumstances for Suspension

Not defined.

4.4.5 Who can request suspension

Not defined.

4.4.6 Procedure for suspension request

Not defined.

4.4.7 Limits on Suspension Period

Not specified.

4.4.8 CRL Issuance Frequency

CRLs are issued after every certificate revocation or at least every 30 days.

4.4.9 CRL Checking Requirements for Relying Parties

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

4.4.10 Online Revocation/status Checking Availability

Not Implemented.

4.4.11 Online Revocation Checking Requirements

Not Implemented.

4.4.12 Other Forms of Revocation Advertisement

None.

4.4.13 Requirements for Relying Parties on Other Forms of Revocation Advertisement

None.

4.4.14 Variations of the Above in Case of Private Key Compromise

Not defined.

4.5 Security Audit Procedures

4.5.1 Types of Events Audited

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

4.5.2 Processing Frequency of Audit Logs

The log files are analysed at least once a month.

4.5.3 Retention Period for Audit Logs

The minimum retention period is 3 years.

4.5.4 Protection of Audit Logs

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

4.5.5 Backup Procedures

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

4.5.6 Accumulation System

The audit log accumulation system is internal to the GridKa-CA.

4.5.7 Vulnerability Assessments

Not defined.

4.6 Records Archival

4.6.1 Types of Events 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 Archives

Logs will be kept for a minimum of 3 years.

4.6.3 Protection of Archive

Records are backed up on removable media, which are stored in a room with restricted access.

4.6.4 Archive Backup Procedures

See Section 4.6.3

4.6.5 Time-stamping Requirements

Not defined.

4.6.6 Archive Collection System

The archive system is internal to the GridKa-CA.

4.6.7 Procedures to Obtain and Verify Archive Information

Not defined.

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

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

4.9 CA Termination

Upon termination the GridKa-CA will:

- Notify subscribers, RAs and relying parties
- Terminate the issuance and distribution of certificates and CRLs
- Notify relevant security contacts
- Notify widely as possible the end of the service

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. The CA-machine is additionally protected by a secure cabinet where access is restricted to CA-personnel.

5.1.1 Site Location

The GridKa-CA is located at the Institut fuer Wissenschaftliches Rechnen (IWR) of the Forschungszentrum Karlsruhe.

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.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

Not defined.

5.3 Personnel Security Controls

5.3.1 Background Checks and Clearance Procedures for CA Personnel

CA personnel is recruited from the Grid Infrastructure and Services team.

5.3.2 Background Checks and Security Procedures for other Personnel

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

5.3.3 Training Requirements and Procedures

Not defined.

5.3.4 Training Period and Retraining Procedures

Not defined.

5.3.5 Frequency and Sequence of Job Rotation

Job rotation is not performed.

5.3.6 Sanctions Against Personnel

Not defined.

5.3.7 Controls on Contracting Personnel

Not defined.

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 doesn't generate any keys for entities.

6.1.2 Private Key Delivery to Entity

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered by E-mail, SSL over http or/and floppy.

6.1.4 CA Public Key Delivery to Users

The CA certificate can be downloaded from the GridKa-CA web site (<http://grid.fzk.de/ca/>).

6.1.5 Key Sizes

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

6.1.6 Public Key Parameters Generation

Not defined.

6.1.7 Parameter Quality Checking

Not defined.

6.1.8 Hardware/software key generation

Key generation is performed by software.

6.1.9 Key Usage Purposes

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

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

Not defined.

6.2.2 Private Key Escrow

Not defined.

6.2.3 Private Key Archival and 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.

6.3 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.

6.4 Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Security Technical Requirements

- CA operating systems are maintained at a high level of security by applying all the relevant patches
- Monitoring is performed to detect unauthorized software changes
- CA systems configuration is reduced to the base minimum

6.5.2 Computer Security Rating

Not defined.

6.6 Life Cycle Security Controls

Not defined.

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.

6.8 Cryptographic Module Engineering Controls

Not defined.

7 Certificate and CRL Profile

7.1 Certificate Profile

7.1.1 Version Number

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
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: URL:<http://grid.fzk.de/ca/>

Certificate Policies: The OID of the CP/CPS

Netscape Cert Type: SSL Client 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.pem>

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

7.1.3 Algorithm Object Identifiers

Not defined.

7.1.4 Name Forms

Issuer: C=DE, O=GermanGrid, CN=GridKa-CA

Subject: [C=DE], O=GermanGrid, OU=XXX, CN=Subject-Name

Where XXX 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/globus/orga.html>

7.1.5 Name Constraints

see 7.1.4

7.1.6 Certificate Policy Object Identifier

The certificate policy object identifier (OID) for this document is:

1.3.6.1.4.1.2614.5548.1.1.1.3

Version 1.3

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	3

7.1.7 Usage of Policy Constraints Extensions

No stipulation

7.1.8 Policy Qualifier Syntax and Semantics

No stipulation

7.2 CRL Profile

7.2.1 Version

X.509 v1

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.

8.2 Publication and Notification Procedures

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

Not defined.

9 Bibliographie

- [1] Forschungszentrum Karlsruhe in der Helmholtz-Gemeinschaft, <http://www.fzk.de>
- [2] 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>
- [3] S. Bradner, „Key words for use in RFCs to Indicate Requirement Levels“, RFC 2119, March 1997 – <http://www.ietf.org/rfc/rfc2119.txt>
- [4] EuGridPMA - <http://eugridpma.org/guidelines/EUGridPMA-minreq-classic-20040402-3-1.pdf>
- [5] INFN Certificate Policy and Certificate Practice Statement - <http://security.fi.infn.it/CA/CPS/>
- [6] LIP Certificate Policy and Certificate Practice Statement - <http://www.lip.pt/ca/ca-policy.html>
- [7] Cern Certificate Policy and Certificate Practice Statement - https://edms.cern.ch/file/431705/LAST_RELEASED/CP-CPS.pdf
- [8] CNRS Certificate Policy and Certificate Practice Statement - <http://www.urec.cnrs.fr/igc/Doc/Datagrid-fr.policy.pdf>
- [9] The OpenSSL Project – <http://openssl.org>