DutchGrid CA

DutchGrid and NIKHEF Medium-Security X.509 Certification Authority

Certification Policy and Practice Statement

Version 3.4

Document Revision Information

Document Identifier	1.3.6.1.4.1.10434.4.2.2.1.3.4
Document Version	3.4 (FINAL)
Last Modified	2020-04-09
Last Edited By	DLG

Table of Contents

Document Revision History

Version	Date	Comments
1.0	*February 2001*	*Initial Version*
1.5	*May 15, 2001*	
2.0α	*September 24, 2001*	
2.1	*November 2001*	
2.2	*November 4, 2004*	*Resynchronized compliance with minimum requirements v3.2*
3.0	*May 14, 2007*	*Resynchronized compliance with Classic AP v4.1, and removed all references to optional procedures and operations that were unused. Added automatic client (robot) certificate applications*
3.1	*November 30, 2007*	*Implemented changes for compliance with the Grid Certificate Profile draft 0.25 and results of the QuickScan Audit feedback*
3.2	*January 2012,* *April 2012*	*Implemented changes as recommended in the audit 2011 and peer reviews thereof. Increased minimum key length to 2048 bits as of September 1st, 2012.*
3.3	*July 2012*	*Allowed for additional hash algorithms and key lengths*
3.4	*April 2020*	*Allow for voucher-based electronic document submission in addition to facsimile and postal mail; and add tele-meeting vetting of applicants with which the RA has an existing business relationship, subject to compensatory controls.*

1 INTRODUCTION

This Certification Policy and Practice Statement (CP/CPS) is written according to the framework laid out by RFC 2527. It describes the set of rules and procedures adhered to by the DutchGrid and Nikhef medium-security Certification Authority, operated by the Computer Technology Group and the Physics Data Processing Group of the Dutch National institute for sub-atomic physics (Nikhef), supported by the Virtual Laboratory for e-Science project and the BIG GRID project, as a courtesy service to the DutchGrid community.

This document is currently at version 3.3. The document is to be formally referred to as the "*DutchGrid and Nikhef medium-security X.509 certification authority certification policy and practice statement, version 3.3*", but is abbreviated to "*the DutchGrid CP/CPS*" when referred to herein.

1.1 Overview

The DutchGrid and Nikhef Medium-Security X.509 Certification Authority offers identity certification services for science and research in the Netherlands, for the purpose of cross-organisational distributed resource access, solely in the context of academic and research and similar, not-commercially competitive, applications.

The DutchGrid CP/CPS is a statement of practices, which the DutchGrid medium-security CA employs in issuing public-key certificates.

A public-key certificate (hereinafter ”certificate”) binds a public-key value to a set of information that identifies the entity (such as person, organisation, account, or site) associated with use of the corresponding private key (this entity is known as the ”subject” of the certificate). A certificate is used by a ”certificate user” or ”relying party” that needs to use, and rely upon the accuracy of, the public key distributed via that certificate. A certificate user is typically an entity that is verifying a digital signature from the certificate's subject or an entity sending encrypted data to the subject.

The degree to which a certificate user can trust the binding embodied in a certificate depends on several factors. These factors include the practices followed by the certification authority (CA) in authenticating the subject; the CAs operating policy, procedures, and security controls; the subject's obligations (for example, in protecting the private key); and the stated undertakings and legal obligations of the CA (for example, warranties and limitations on liability).

1.2 Identification

This document is named the "*DutchGrid and Nikhef medium-security X.509 certification authority certification policy and practice statement, version 3.3*". The currently valid version of the text is available from:

```
http://ca.dutchgrid.nl/medium/policy/
```

The following ASN.1 object identifier has been assigned to this CP/CPS:

```
1.3.6.1.4.1.10434.4.2.2.1.3.3
```

This current version is version 3.3, issued in July, 2012. It supersedes any previous version of this CP/CPS as of this date.

1.3 Community and Applicability

1.3.1 Certification authorities

The DutchGrid Medium-Security X.509 CA ("DutchGrid MS CA") is a self-signed root certification authority. It is not a subordinate authority, and does not issue certificates to subordinate CAs.

The DutchGrid MS CA is managed by the Nikhef PDP group in close consultation with the DutchGrid Platform community members and the participating grid and e-Science projects in the Netherlands.

Certificates of the DutchGrid MS CA are issued by people of the CA Operations Staff: no automated issuing is allowed. The CA operating personnel is designated by the DutchGrid CA Manager, and the manager and operators are responsible for the operational service of the DutchGrid MS CA. The current list of operational staff is published in the on-line Repository (the location thereof is documented in section 1.4).

The CA functions are managed and operated on a best-effort basis. The operating organisations, the Nikhef collaboration, and/or the foundation FOM cannot be held liable for any damages resulting from the operation or non-operation of the DutchGrid MS CA.

1.3.2 Registration authorities

Registration Authorities (RAs) are individual people recognised and designated as such by the DutchGrid MS CA to act as trusted intermediaries in the identity verification process between subscriber and certification authority. The RAs are formally assigned by the CA and their identities and contact details are published in an on-line accessible repository, the location of which is stated in section 1.4.

The RAs are required to declare their understanding of and adherence to this CP/CPS, and are required to perform their functions in accordance with this CP/CPS and the current best practices as defined by the DutchGrid medium-security Certification Authority management.

The DutchGrid CA Operations Staff also fulfils the role of a Registration Authority.

1.3.3 End entities

Certificates can be issued to natural persons and to computer entities (hosts, networked services and automated clients).

The entities that are eligible for certification by the DutchGrid MS CA are:

- all those entities related to organisations, formally based in and/or having offices inside the Netherlands, that are involved in research on or deployment of multi-domain distributed computing infrastructures, intended for cross-organisational sharing of resources. Only research and educational organisations, and organisational units of other organisations involved in research or education for non competitive purposes, qualify under this policy;
- all those entities associated to the DutchGrid Platform;
- all organisations or organisational units located in the Science Park Amsterdam that are run on a non-for-profit basis.

All services provided by the DutchGrid MS CA are non-discriminatory, and are provided to all qualified entities under the same conditions and at the same service level.

Consumers – being natural persons not acting in a professional capacity or in the context of business – are not permissible end-entities of the DutchGrid MS CA and are not allowed to use any of the DutchGrid MS CA services or to apply for or rely on certificates.

1.3.4 Applicability

Certificates issued are suitable for the

- Client authentication in TLS and GSI transactions;
- Server and service identification in TLS and GSI transactions;
- The generation of ‘proxy’ certificates, such as specified in RFC3820.

The use of the certificates for email signing is permitted, and appropriate certificate extensions will be included on request. The use of certificates for long-term encryption of data is not supported. The certificates issued by the DutchGrid medium-security Certification Authority may not be used for financial transactions.

Notwithstanding the above, using certificates for purposes contrary to applicable law is explicitly prohibited.

1.4 Contact Details

1.4.1 Specification administration organization

The DutchGrid medium-security Certification Authority is administered by the Dutch ”Nationaal instituut voor sub-atomaire fysica (Nikhef)” as part of its continuing commitment to Grid computing in the Netherlands. It is managed by the Nikhef Physics Data Processing (PDP) group, and is operated by the Nikhef Computer Technology (CT) Group. The DutchGrid MS CA management is responsible for ensuring that the CA is operated in accordance with this CP/CPS.

1.4.2 Contact person

The DutchGrid MS CA Manager is:

David Groep, Nikhef Physics Data Processing group,
P.O. Box 41882, NL-1009 DB Amsterdam, The Netherlands
phone: +31 20 592 2179, telefax: +31 20 592 5155
e-mail: ca@dutchgrid.nl.

CA Operation Staff are listed in the DutchGrid online Repository (web site).

1.4.3 Person determining CPS suitability for the policy

The Policy and the Practice statement are the same document. This section is therefore not applicable.

2 GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The DutchGrid MS CA must maintain this CP/CPS document to reflect all practices and procedures by which the CA will operate. The DutchGrid MS CA ensures that all aspects of the service, operations, and infrastructure related to the certificates issued under this policy are performed in accordance with the requirements of this policy.

The DutchGrid MS CA will generate and suitably protect the private key used for signing certificates under this policy.

The DutchGrid MS CA will accept requests for certification by all entities eligible for certification under this policy, as detailed in section 1.1.3. The CA will authenticate these entities according to the procedures outlined in this document, and only issue signed certificates based on these requests if the policy requirements are satisfied.

The DutchGrid MS CA will notify the applicant of the issuing of the certificate by an electronic mail message sent to the address provided at the time of application, or alternatively the address where the request originated.

The certificates issued by the DutchGrid medium-security Certification Authority under this policy will contain a reference to this CP/CPS document in the policy object identifier in the ”certificatePolicies” extension. The URI of the on-line repository containing the CP/CPS will be provided in the comments-extension of the issued certificates.

All certificates issued by the DutchGrid medium-security Certification Authority will be available from a publicly-accessible on-line repository. This repository will contain no data about the subscriber, except for such data as contained within the certificate. In particular, no sensitive private data, no data concerning the identification procedure and no specific address information will be maintained in this repository. Professional affiliation is not to be considered sensitive private data. The CA will provide an interface to retrieve any issued and valid certificates in the on-line repository, but it will not publish a full list or index of all certificates.

The DutchGrid medium-security Certification Authority will accept revocation requests according to the procedures outlined in this document. Entities requesting revocation will be authenticated by the CA or its assigned RA.

The DutchGrid medium-security Certification Authority will issue a Certificate Revocation List. This CRL will be published in a publicly-available on-line repository.

By issuing a certificate that references this policy, the CA certifies to the subscriber and to all qualified relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period that the CA has issued and will manage the certificate in accordance with this policy, as stated in the certificate extensions. Also, the CA certifies that there are no misrepresentations of fact in the certificate as known to the CA, and the CA has taken reasonable steps to verify any additional information in the certificate. Also, the certificate meets all material requirements of this CP/CPS.

No other liability, either expressed or implied, is accepted with regard to the certificates issued by the DutchGrid medium-security Certification Authority.

2.1.2 RA obligations

A Registration Authority (RA) is a person that verifies and validates certification applications in accordance with all provisions specified in this CP/CPS. To this end, the RA must agree to follow this CP/CPS and all operational procedure derived therefrom, specifically including those related to the use of personal data provided to the RA.

The RA must validate the relationship between the public key data contained in the request and the key data held by the requester, or ensure that this connection between the public key and the identity vetting trail can be verified by the CA based on information attested to by the RA at the time of identity verification.

The RA must verify to a reasonable extent that the private key pertaining to the key pair submitted for certification is in possession of the requesting entity or person responsible for the entity. This verification can be based a hand-written digest of the key information on the application form, in the handwriting of the signatory of the application, or may be based on out-of-band or non-technical means.

The RA must verify to a reasonable extent that the information submitted for assertion in the certificate is correct at the time of validation.

- For personal ("users") certificates, that the subject name bears a reasonable resemblance to the name of the person as shown on the official identity piece presented, or be the colloquial name used by this person in every and all day-to-day communications, if such a colloquial name can be positively attested to by the RA. If alternative names are included in the certificate request, the RA shall verify to a reasonable extent that these names are correct at the time of verification;
- For any certificates containing DNS names, either in the subject name or subject alternative names ("hosts", i.e. hosts and services, or "servers"), the RA must ensure that the requestor is entitled to the use of these names, either by being the responsible system administrator of the host system concerned, by being either the registrant, administrative contact or operational contact for the domain name or of the first higher-level domain name in the domain name system that is registered in an ICANN designated registry, or by being appropriately authorised by such an administrator, registrant, administrative or operational contact;
- For certificates issued to automated clients ("robots"), verify that the documented subject name and alternative subject names are related to the human person or group of persons responsible for this automaton, and that all requirements imposed on robot certificates are met.

The RA shall confirm any validation to the CA via a reliable and trusted mechanism. This is usually done by countersigning an application form containing the verified identity information and the key-pair digest, with the handwritten signature of the RA. The RA may only countersign an application form if all verifications are completed successfully, the key-pair digest has been written on the form, and enough information on the identity verification is written on the form that allows matching of the request to any previous requests for the same subject name.

The certificate application form counter-signed by the RA must be sent to the CA via postal mail or facsimile message, in which case this form may be sent either by the RA directly, or by the applicant. In special cases of urgency, the RA may contact the CA operations staff by telephone (after positive voice identification of the RA) or signed email, and attest to the correctness of the certificate application request to the CA, who may, at its own discretion, decide to issue the certificate for the request thus identified. The RA must communicate the subject name and key-pair digest to the CA, and send the countersigned application form immediately and directly to the CA – the form must not be returned to the applicant in this case.

The certificate application form may be submitted electronically through the SURFfilesender service, provided that:

- the address of record of the applicant is verified by initiating the transfer by the CA operator and sending an 'upload voucher' to the applicant. The validity period of the voucher shall not exceed 8 days,
- the applicant uploads the document(s) using the voucher URL provided
- if initial identity vetting of the applicant was via tele-meeting only, the CA – at its own discretion – may demand that the uploaded documents be encrypted with a secret that is communicated to the applicant by telephone or text message using the number provided on the vetting record (Section 9 application form), thereby verifying the phone number

- Otherwise, the applicant may opt to encrypt the transfer and send the secret to the CA by other means, to allow the CA operator to decrypt the submitted documentation

After receipt, the document(s) will be printed by the CA operator and removed from all electronic storage. The document(s) will be removed from SURFfilesender following the period set by the applicant, but at most after 21 days.

In case the RA temporarily retains any application forms or accompanying documents, it must treat all these documents as confidential. All documents must be stored in a safe and trusted location at all times, until they can be sent to the CA.

The RA must forward requests for revocation by subscribers to the CA with priority, as soon as a request is recognised as such. The RA must give an assessment as to the validity of the revocation request.

The RA must instruct the applicant on the proper care and protection of the private key data associated with the request.

Entities that act as RA for the DutchGrid MS CA have no notification obligations when certificates have been issued, revoked or suspended.

2.1.3 Subscriber obligations

Subscribers must adhere to the procedures and policies specified in this document, or derived thereof, as published by the CA.

Subscribers to the DutchGrid MS CA have the obligation to ensure that the data presented in the certification request is accurate. For requests for host, server and automated client and robot certificates, they may only apply for certificates for entities for which they are responsible.

The subscriber must generate a key pair in a trustworthy manner, using allowed versions of the key-pair generation software, and has the obligation to protect the private key against all disclosure or unintended usage. For personal (“users”) certificates, the pass phrase protecting the private key should be strong and at least 12 characters in length. Keys used by hosts, servers, and services, may be stored in an unencrypted form, in which case they private key should be accessible only by those applications, services or systems and be protected by appropriate operating system file permissions. Keys used by automated clients or robots must be protected in a way compliant with the robot requirements (c.f. section 4.1 and 3.1.9).

Storage of any (encrypted) private key on any publicly accessible medium is strongly discouraged: storage on a medium that is customarily deemed secure and which is properly administrated is admissible.

The certificate must only be used by the subscriber for purposes consistent with this policy.

The subscriber must instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure or other compromise of the subscribers’ private key.

By making a certificate request to the DutchGrid MS CA, the subscriber or potential subscriber accepts the registration of such data in all the repositories described in section 2.1.1. The subscriber is allowed to correct or complete the data retained in these repositories by contacting the CA operator stated in section 1.4, in accordance with the Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens 2000). A request to remove data from this repository will result in immediate and irreversible revocation of the certificate(s) pertaining to the subscriber and will cause the subject names involved to be blocked permanently thereafter. In case of removal of subscriber data from the repository, an audit trail pertaining to this removal will be retained by the CA.

2.1.4 Relying party obligations

Qualified relying parties are expected to rely on certificates that reference this Policy and Practice Statement as appropriate authentication of the subscriber if

- The relying party is familiar with this CP/CPS before drawing any conclusion on trust of a certificate issued by the DutchGrid MS CA;

- The reliance is reasonable and in good faith, in light of all the circumstances known to the relying party at the time of the reliance;
- The purpose for which the certificate was used was appropriate under this CP/CPS;
- Use for any authorisation decision either *(i)* the full subject distinguished name, *(ii)* only the common prefixes "/O=dutchgrid/O=users/…", "/O=dutchgrid/O=hosts/…", "/O=dutchgrid/O=servers/…", or "/O=dutchgrid/O=robots/…", where the subject name is in the OpenSSL one-line string representation), *(iii)* for host, service, or server certificates only the CN or parts of the CN.

  In particular, the apparent affiliation of the user (the additional *organization* and *organizationalUnit* attributes "O" and "OU"), should not be given any meaning, as they are solely used to reflect the initial RAs selected for the acts of verification.
- The relying party accepts all limitations on the liability of the DutchGrid MS CA, as detailed in section 2.2;
- The relying party checked the status of the certificate to their own satisfaction prior to any reliance. Specifically, they have to check whether the validity period has expired and if the certificate has been included in the most recent Certificate Revocation List issues by the DutchGrid MS CA;
- The relying party has checked the authenticity of the DutchGrid MS CA root certificate before using it.

2.1.5 Repository obligations

The DutchGrid MS CA maintains four types of repository

1. An on-line public repository containing the CA root certificate, the most current Certificate Revocation List (CRL), and all issued and valid certificates.
2. An on-line protected repository, only accessible to CA management and operations staff, containing the certificate status and request audit trail, basic identifying information for each pending request and issued certificate (including the document type and number used for identity vetting, and the renewal confirmation tokens)
3. An off-line paper document archive, containing the completed application forms received from applicants and RAs, as well as documentation on all revoked certificates.
4. An off-line paper archive containing the letters of designation of all Registration Authorities confirmed or reconfirmed after June 1st, 2006.

These repositories shall be maintained and secured as follows.

On-line Public Repository

The on-line repository is located at

```
http://ca.dutchgrid.nl/medium/
```

The repository is hosted on a machine in a protected systems environment, where the physical machine is managed by CA staff. The repository is operated at a best-effort basis, where the intended availability is continuous. This repository does not contain personal data apart from those data published in the issued certificates.

The issued certificates are published within one hour after issuing. Revocations are published within one hour after the revocation by including them in a Certificate Revocation List and publishing this List in the repository.

On-line Protected Repository

The on-line protected repository is hosted on a dedicated physical system that is exclusively designated to the handling of requests for certificate application. The system contains a management interface that is accessible only by CA staff via an authenticated and secure link.

This Protected Repository contains information pertaining to all requests for certification and to all certificates issued. This repository is intended to:

- establish an authentication binding between the series of request for a specific subject name and the identity of the subscriber and applicants;
- provide a means a contact the subscriber about expiration or revocation of the subscriber's certificate;
- provide an index to the audit trail of the certification and identity verification procedures for auditing of the CA operations with respect to this CP/CPS;
- store sufficient identifying data (identity piece type and serial numbers thereon) to allow unique binding of the requested subject name to a single entity.

Off-line paper archive

This repository is not available to any party except the CA management and operational staff, and to assigned internal or external auditors of the CA. This archive will not hold more information than:

- name of subscriber;
- affiliation of subscriber to the level of detail as stated in the certificate;
- electronic mail addresses of subscriber;
- telephone numbers and logs related to the authentication verification procedure;
- postal and street addresses, as declared by the subscriber, needed to ensure that the subscriber can be contacted in person;
- types and serial numbers on identity cards shown during the verification process and/or additional personal numbers to ensure that the subscriber can re-authenticated successfully and uniquely identified on renewal;
- Name of the RA or RAs involved in the verification process, time and place of the verification meeting.

The information contained in this repository will not be made available to any party but the CA management, operations staff, and the internal or external auditors as part of their assigned duty. Additional information may be obtained during the verification process to support the identity vetting by the RA and the CA, but will not be permanently stored by the CA.

Off-line paper archive of RA designation letters

This archive contains all signed letters of designation for the RAs of the DutchGrid MS CA.

Publishing of Repository Policies

An abstract of this policy as a privacy statement is published in the on-line public repository.

2.2 Liability

2.2.1 CA liability

The DutchGrid MS CA will not give any guarantees about the security or suitability of the service; it is provided on a best-effort basis only. The operator, Nikhef, the FOM foundation, the DutchGrid Platform, the supporting projects, its personnel or partners are not to be held liable for any damages, including but not limited to lost profit, lost savings and incidental or consequential damages. The DutchGrid MS CA is not to be held legally responsible for problems arise out of its operation, or for problems relating to the use or misuse of the certificates it issues.

It is explicitly prohibited to use the certificates issued by the DutchGrid MS CA under this policy for any kind of financial transactions or for any kind of trade.

2.2.2 RA liability

It is the RA's responsibility to authenticate the identity of subscribers requesting certificates, according to the practices described in this document. It is the RA's responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied.

The RAs of the DutchGrid MS CA 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 by the DutchGrid MS CA.

2.3.1 Indemnification by relying parties

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

Nikhef and the supporting projects finance the operations of the DutchGrid MS CA with regard to equipment and personnel cost. No other costs are or will be covered by Nikhef, its partners, the foundation FOM, the DutchGrid platform or the supporting projects. The contribution by Nikhef and the supporting projects is voluntary and may be withdrawn at any time, but Nikhef will ensure that the archiving and retention requirements as described in this CP/CPS are met.

Costs related to auditing are not covered by Nikhef, its partners, the foundation FOM, the supporting projects, or by any institution charged with the operation of the DutchGrid MS CA.

2.4 Interpretation and Enforcement

2.4.1 Governing law

Interpretation of this policy is according to the Law of The Netherlands.

2.4.2 Severability, survival, merger, notice

If any part or any provision of this document shall to any extent prove invalid or unenforceable in law, including the laws of the European Union, the remainder of such provision and all other provisions of this document shall remain valid and enforceable to the fullest extent permissible by law, and such provision shall be deemed to be omitted from this document to the extent of such invalidity or unenforceability. The remainder of this document shall continue in full force and effect and the DutchGrid MS CA, Subscribers, and Relying Parties shall negotiate in good faith to replace the invalid or unenforceable provision with a valid, legal and enforceable provision which has an effect as close as possible to the provision or terms being replaced.

Nikhef intends to continue operations of the DutchGrid MS CA for a period of at least 6 month after the validity period of the last certificate has ended. This intention does not constitute a legally binding guarantee to continue the activities of the DutchGrid MS CA for this period.

Before termination of the CA, the CA will notify all its subscribers, all cross-certifying CAs, and any relying parties known to the CA to be currently and actively relying on the certificate issues by the CA.

2.4.3 Dispute resolution procedures

In case of a dispute based on the contents of this CPS, the Director of Nikhef will be the sole person responsible for resolution of the problem. The complainer cannot take legal action against Nikhef, any of the Nikhef partners, the foundation FOM, the DutchGrid platform, the supporting projects, or the DutchGrid MS CA operating body.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

No fees are charged for the certification service, for any and all certificates issued as soft tokens. When certificates are issued on secure hardware tokens (as defined in section 6.2.1) the applicant is responsible for acquiring an appropriate secure hardware token, compliant with all current policies and operating procedures of the DutchGrid CA. The CA may mediate in the acquisition and initialization of appropriate secure hardware tokens. The DutchGrid MS CA cannot a priori be forced to issue certificates other than via soft tokens.

2.5.2 Certificate access fees

No fees are charged for certificate access.

2.5.3 Revocation or status information access fees

No fees are charged for revocation or status information access.

2.5.4 Fees for other services such as policy information

A reasonable fee may be charged, at the discretion of the CA, for obtaining information from the private repositories at the owner's request. The cost of any secure hardware tokens made available to a subscriber may be recouped by the CA. No fees are charged for any other service.

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

The DutchGrid MS CA operates an on-line repository, that contains:

- the self-signed CA certificate and the public part of the CA signing key;
- all certificates issued under this CP/CPS;
- the most recent Certificate Revocation List (CRL), signed by the CA;
- all past and current versions of the CP/CPS;
- contact information for the CA
- other relevant information

The information in these repositories regarding issued and revoked certificates is updated as soon as possible, but at least within one hour of the issuing or revocation.

2.6.2 Frequency of publication

The information in the public repositories defined in section 2.6.1 is available permanently, on a best-effort basis.

There is no automatic periodic renewal of the DutchGrid MS CA Certificate Revocation List: updates are done manually. A new CRL will be issued within one hour after every revocation, and at least 7 days before expiration of the previously issued CRL.

2.6.3 Access controls

The DutchGrid MS CA imposes no access control on this CP/CPS and on the CRL. There is no access control on the publication of issued certificates, although the DutchGrid MS CA reserves the right to impose such access controls when needed for reasons of proper system maintenance or to prevent abuse of the data contained in the certificates.

For the on-line protected repository, which contains the CA operations interface and certificate request processing system, the CA operators must authenticate using valid certificates to be able to use the interface.

2.6.4 Repositories

The on-line Public Repository with information specified in 2.6.1 is located at the URL

```
http://ca.dutchgrid.nl/medium/
```

2.7 Compliance audit

2.7.1 Frequency of entity compliance audit

The DutchGrid MS CA will cooperate with a compliance audit at least once every year. Such an audit may be requested by authorities, with whom cross-certification relations exist, by CAs with which the DutchGrid MS CA has entered into a common policy management authority, by a policy management authority in which the DutchGrid MS CA has entered or by qualified relying parties. Any costs associated to such compliance audit are to be born by the requesting party.

The DutchGrid MS CA management will internally self-assess compliance of the operating procedures to this CP/CPS at least once a year.

2.7.2 Identity/qualifications of auditor

No stipulation.

2.7.3 Auditor's relationship to audited party

An external audit can be requested by authorities, with whom cross-certification relations exist, by CAs with which the DutchGrid MS CA has entered into a common policy management authority, by a policy management authority in which the DutchGrid MS CA has entered or by qualified relying parties. The auditor can be chosen by the requestor but the CA may require evidence of auditor's qualifications. The CA reserves the right to impose confidentiality restrictions upon the auditor, for both security and data protection reasons.

2.7.4 Topics covered by audit

The audit will verify that the current operating procedures of the CA comply with the latest approved version of the CP/CPS, and that all issuance of currently valid certificates complies with the CP/CPS valid at the time of issuance.

2.7.5 Actions taken as a result of deficiency

In case of a deficiency, the CA Manager will announce the steps that will be taken to remedy the deficiency. This announcement will include a timetable.

2.7.6 Communication of results

The CA manager will make the result publicly available with as many details of any deficiency as (s)he considers necessary.

2.8 Confidentiality

The DutchGrid MS CA collects personal data about subscribers. This data collection is subject to the Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens) 2000). The subscriber acknowledges that such data is being collected by the CA and permits storage of any such data in the secure repository intended in section 2.1.2 according to the stipulations made therein.

2.8.1 Types of information to be kept confidential

Any data part of the verification audit trail, and any data collected during the validation process is considered confidential, except for those data asserted in the issued certificate.

2.8.2 Types of information not considered confidential

Any data contained in the subscribers certificate and any data contained in CRL's is not considered confidential. Contact information for the CA operational staff and for the RAs is not considered confidential.

Statistics regarding certificates issuance and revocation contain no Personal Information and is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

No details about the revocation are currently disclosed in a public repository. Qualified relying parties may inquire about the reason for revocation, and will be notified of such reason to the level of detail specified in the CRL reason field as defined in OID 2.5.29.21.

A reason field compliant with OID 2.5.29.21 may be included in the CRL at any time by the DutchGrid MS CA.

No other details concerning the revocation are disclosed.

2.8.4 Release to law enforcement officials

The DutchGrid MS CA will not disclose certificate or certificate related information to any third party, above that what is part of the certificate, except when required by law, or by authentic request of the subscriber.

The DutchGrid MS CA will take care that no information will be available except for what is required for authentication validation purposes under this CP/CPS and documented therein. All other information collected must be securely destroyed.

2.8.5 Release as part of civil discovery

See section 2.8.4.

2.8.6 Disclosure upon owner's request

No information will be disclosed unless requested by the subscriber in an authenticated request and upon presentation of proper proof of identity. The owner may request this information as stipulated in the WBP2000 at any time. The CA reserved the right to charge a reasonable fee for the service.

2.8.7 Other information release circumstances

An auditor doing a formal compliance audit may have access to all confidential data contained in the secure repository specified in section 2.1.1. The auditor will not have access to cryptographic keys that are part of the CA infrastructure. The repository does not contain private keys of subscribers.

Any auditor will be required in writing to agree keeping all confidential data secret and not to publish it in any reports.

There are no other circumstances for the release of private or personal information.

2.9 Intellectual Property Rights

This document is formatted according to RFC 2527 by Chokhani and Ford (1999), and loosely inspired by the Gridforum CP draft as of September 2001 by Butler and Genovese (GGF 2001), by the SURFnet PCA CPS version 1.1 by Teun Nijssen (SURFnet 2001), and by the INFN CA draft version 0.3 by Roberto Cecchini (INFN 2001).

Version 3.0 of this CP/CPS owes significantly to the UK e-Science CP/CPS document version 1.3 by Jens Jensen of RAL/CCLRC. We are grateful for that very thorough document and in particular for the significant contribution on robot certificates, their protection and use.

This text may be used by others without prior approval; acknowledgements are welcomed but not required, except where parts of the text have been taken from other documents, in which case the original author(s) must be acknowledged. Unmodified copies of this CP/CPS may be redistributed without explicit permission.

No intellectual property rights are claimed on issued certificates or certificate revocation lists. The DutchGrid MS CA reserves all other rights related to this document.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

Each entity in the PKI has a subject Distinguished Name (DN) structured according to X.501. When represented in an ASN.1 formatted X.509 certificate, attributes values in this DN are encoded as *PrintableString*s.

All entities in the PKI will have subject names such that the first attribute-value pair in the ASN.1 encoded will be “O=dutchgrid”, except for the subject name of the CA root certificate, which will start with the two RDN distinct relative DN sets “C=NL” and “O=Nikhef”, each being sets of length 1.

There are four different name forms for subject names associated with subscribers. These subscriber classes are indicated in the subject DN of the certificate by means of an “organization” attribute, immediately following the “O=dutchgrid” in the sequence.

- The "users" class shall contain only certificates for subscribers that are natural persons. The private key must only ever be held by the applicant, and must be stored in a properly encrypted form under the control of the user.

  The common name in the subject DN must bear a reasonable resemblance to the name of the person as shown on the official identity piece presented including at least one given name in full and the full surname, or be the full colloquial name used by this person in every and all day-to-day communications and include the full surname as documented on the official identity piece, if such a colloquial name can be positively attested to by the RA.

  Users may request a descriptive string of up to 16 characters to be appended to the full name in the CN. This descriptive string will be appended to the name, surrounded by round brackets, where the name proper and the bracketed string are separated by a single space characters (“ “).

  The common name must consist entirely of characters in the set

  ```
  ’ ’, ’0’ - ’9’, ’a’ - ’z’, ’A’ - ’Z’, ’(’, ’)’, ’-’, ’.’
  ```

- The "hosts" class shall contain only certificates for entities that are networked systems, applications or services. This certificate should be used solely to identify the network endpoints of the system, application or service in communications. The private key for such entities may be stored in an unencrypted form, and must be protected by operating system mechanisms limiting the use to authorized administrators of the host, application or services. As more than one administrator may have access to the private key, authentication with this certificate does not necessarily represent a non-reputable action by an individual.

  The common name in the subject DN must contain a valid sub-domain name in the Internet domain name system as operated by ICANN. The sub-domain name may be prefixed with a service name, in which case the service name and the sub-domain name must be separated with a single forward slash (“/”) in the common name of the DN.

  The common name must consist entirely of characters in the set

  ```
  ’0’ - ’9’, ’a’ - ’z’, ’A’ - ’Z’, ’-’, ’.’, ’/’
  ```

- The "servers" class shall contain only certificates for subscribers that are networked systems. These certificates must only be used to identify secured web servers or secured LDAP servers, and are only available at the discretion of the CA manager. In particular, these certificates are issued to systems associated with the CAs own operation. The private key for such entities may be stored in an unencrypted form, and must be protected by operating system mechanisms limiting the use to authorized administrators of the system.

The common name in the subject DN must contain a valid sub-domain name in the Internet domain name system as operated by ICANN.

The common name must consist entirely of characters in the set

```
’0’ - ’9’, ’a’ - ’z’, ’A’ - ’Z’, ’-’, ’.’
```

- The "robots" class shall contain only certificates for agents that perform automatic functions on behalf of a natural person. They must not be used to identify network end-points. The common name in the robot certificates shall identify both the intended use of the robot as well as the natural person responsible for the agent. The private key for such entities must be stored in a secure hardware token or on a hardware security module, compliant with the requirements specified in section 6.2.1.

  The common name in the subject DN must start with the string “Robot:”, contain an comprehensible and brief description of the usage type of the robot, and shall bear a reasonable resemblance to the name of the person as shown on the official identity piece presented, including at least one given name in full and the full surname, or be the full colloquial name used by this person in every and all day-to-day communications and include the full surname as documented on the official identity piece, if such a colloquial name can be positively attested to by the RA.

  The common name must consist entirely of characters in the set

  ```
  ’ ’, ’0’ - ’9’, ’a’ - ’z’, ’A’ - ’Z’, ’(’, ’)’, ’-’, ’.’, ’:’
  ```

  and must be formed like

  ’…/CN=Robot: *robot function - Responsible Person*’

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 organisation may be a commonly recognised colloquial name, is assigned by the DutchGrid MS CA, and must be in the permitted character set.

Personal and Robot Certificates

The name used for a subscriber must relate on the full name of such person given at birth or be the full colloquial name used by this person in every and all day-to-day communications and include the full surname as documented on the official identity piece, if such a colloquial name can be positively attested to by the RA.. Names associated with an assumed identity, pseudonym, re-assigned identity, role, or alias must not be used.

The CN of a personal certificate may contain additional text other than the subscriber’s authenticated name, in order to disambiguate between different users with the same name, or to allow the same user to have more than one certificate. The additional text must be formatted in such a way that it cannot be confused with the subscriber’s name. For disambiguation between different users, the disambiguating characters are preferably numerals, are separated from the name with a single space, and are not enclosed in parentheses. For additional names issued to the same user, it is recommended that disambiguating text follows the subscriber’s name, with a space as separator, and be enclosed in parentheses. The CA does not otherwise enforce or validate the content of this text.

Host and Service Certificates

The common name in host and service certificates must be the fully qualified domain name (FQDN) of the host on which the certificate will be installed. It must be formatted as a sub-domain name according to the rules defined for the corresponding top-level domain name, as defined by the ICANN designated operator for the top-level domain name, notwithstanding the limitations on the permitted characters specified in section 3.1.1.

The FQDN may be preceded by a service name, which must be separated from the FQDN by a single forward-slash ("/") character. This will classify it as a *service* certificate.

3.1.3 Rules for interpreting various name forms

No stipulation.

3.1.4 Uniqueness of names

The DutchGrid MS CA will assert to a reasonable level that the subject name is unique and never assigned to more than one entity within the ensemble of all certificates issued by the DutchGrid CAs. At least, any subject name shall be linked to a unique entity within the ensemble of certificates issued by the DutchGrid MS CA. If the name presented by the applicant is not unique, the CA will ask the applicant to resubmit the request with a variant of the common name to ensure uniqueness. Punctuation, case and whitespace are not discriminatory elements of a subject name and must not be used to distinguish names under this policy.

The DutchGrid MS CA will ensure that a subject name is not re-used. If an applicant request a certificate with the same subject name as an existing certificate (regardless of the status of this latter certificate), and the request is not an authenticated rekeying or renewal, the CA will consult the original identifying personal information to ensure the subscriber is the same person who was identified in the original certificate. Otherwise, the subject name will not be re-used.

For host and service certificates, the RA must verify to a reasonable extent that the applicant is, at the time of the application, entitled to the use of the FQDN presented in the subject names, according to the RA requirements specified in section 2.1.2. It is recommended that the applicant is the same individual that requested the preceding certificate issued to that host or service, or has been designated as the successor of that individual. Otherwise, the RA shall have the discretionary right to re-assert the binding between the responsible person and the FQDN, according to the requirements of initial registration for host and service certificates.

3.1.5 Name claim dispute resolution procedure

Name claim disputes are settled at the sole discretion of the CA administrators, mentioned in section 1.4.

3.1.6 Recognition, authentication and role of trademarks

As stipulated in section 3.1.5.

3.1.7 Method to prove possession of private key

The DutchGrid MS CA verifies the possession of the private key relating to certificate requests

- by accepting only certificate requests signed with the associated private key, and
- simultaneously by out-of-band means at the time of identity verification by the RA. Such verification is based on a digest of public material of original key pair, written down on the verification form, and presented to the RA by the applicant during the verification meeting.

The CA will verify, before approving the request, that the digest on the form matches the electronically submitted certificate signing request.

3.1.8 Authentication of organization identity

The DutchGrid MS CA or the RA on its behalf uses the specification of organisations for checking eligibility only. It checks the eligibility by checking that the organisation is known to its peers to be part of the distributed and grid computing effort in the Netherlands, or that the organisation is based on the Science Park Amsterdam, and that the organisation is involved in not-for-profit research or education, by personal attestation of the RA or its peer organisations in the Netherlands.

The organisation name mentioned in the subject name is an approximation of the name of the organisation at which the applicant is based at the time of the initial application. The organisation name is solely intended to serve as a referral indicator to the most appropriate local RA for the applicant, and as such the organisation name mentioned in the certificate is not authenticated and must not be relied on for any purpose.

3.1.9 Authentication of individual identity

Certificates issued by the CA bind a subject name to an identified entity that is in possession of the private key pertaining to that certificate. This binding will be authenticated by the CA or its assigned RA's.

Information exchanged between the RAs and the CA shall be either by strong cryptographic means, or by means that constitute valid legal evidence, or shall be verified by out-of-band methods with firm positive identification by both parties involved.

Personal Certificates

In case the entity is a natural person, the initial authentication will be based on suitable photo-identity documents as specified in section 9.1, and

- an in-person appearance of the applicant before the RA, roving RA or Central RA Service of the DutchGrid MS CA during which this document is presented by the applicant; or
- a video-supported tele-meeting in which the applicant meets with the RA, during which the photo-ID document is presented and verified for authenticity. In addition, all of the following checks must be made and conditions met:
    - the RA and the applicant must have a pre-existing business relationship,
    - the RA must initiate the tele-meeting, and the tele-meeting shall have at least a resolution and quality sufficient to verify the authenticity details of documents and read documents shown in front of the camera, and be over secure channels when traversing the public internet,
    - the RA shall only authenticate documents of which the RA is familiar with their physical form and authenticity properties, and verify such properties, including holographic and transparency elements,
    - unless deemed infeasible by the RA, the applicant shall demonstrate authenticity of photo-ID documents by showing – on video during the meeting - their real-time read-out via NFC, e.g. using the ReadID app, and show the serial number thus read-out to the RA over video,
    - the vetting record (Section 9 application form), including the digest of the public key pair information, shall be completely filled by the applicant and shown legibly to the RA during the tele-meeting,
    - the RA shall, to the extent possible, confirm the liveness of the applicant and the likeness with the image on the presented photo-ID,
    - the applicant shall sign the application form during the tele-meeting,
    - the RA shall generate (invent) a one-time unique code of at least 8 digits, and communicate this to the applicant during the tele-meeting by calling or sending a text message to the phone number written on the vetting record, and verify that the applicant writes this code in lieu of the signature of the RA on the vetting record.

      The RA shall itself record:
        - the phone number used
        - the unique code conveyed
        - the date and time of the meeting

- the organisational affiliation of the applicant based as per the existing business relationship

The unique code will be checked by the CA contacting the RA, or vice versa, using independent means before issuance. The digest of the public key pair information (POP challenge) will be checked against the electronically submitted CSR following the standard procedure. When the application form is submitted electronically using Filesender as per section 2.1.2, the CA shall in addition validate the email address as provided on the application form via this method.

The CA shall ensure that the applicant's identity is verified in accordance with the stipulations in this CP/CPS. In addition, the RA shall record the process followed for issuance of each certificate and submit this in the form of signed documentary evidence to the CA for archival. This record shall include data provided by both the applicant and the RA.

The applicant shall provide as documentary information:

- The name, date and place of birth of the applicant
- The type and unique number of the identity piece presented by the applicant
- The contact address, phone number, and electronic mail address of the applicant
- The digest of the public key pair information pertaining to the request, as specified by the CA in the appropriate technical documentation.
- The signature of the applicant, indicating acceptance of all conditions in the CP/CPS
- The place and date of signing by the applicant

The RA will verify the correctness of the data on the identity piece, and make sure to a reasonable extent that the other information provided is correct. The RA will then

- Declare his or her name
- Note the time and date of successful verification
- Note the physical meeting place
- Sign the form, indicating the RA has verified the identity according to the requirements for RAs
- Provide further information for the CA as needed

Personal certificates may optionally have *Object Signing* asserted in the *netscapeCertificateType* extension and *codeSigning* asserted in the *extendedKeyUsage* extension. For certificates that contain an object signing extension, the CA does not check, and makes no assertion, that the user is trustworthy as a software developer or deployer. Relying parties must check the authenticated identity and decide independently whether to run the signed software.

Robot Certificates

In case the entity to be certified is a robot, as defined in section 3.1.1, all provisions specified above for personal certificates must be met. In addition, the applicant must provide to the satisfaction of both the CA and the RA that the private key pertaining to the certificate request is adequately protected by being generated and solely stored on a secure hardware token as defined in section 6.2.1, out of which is cannot be extracted in plain-text.

The subject name of the robot certificate must contain a reasonable representation of the full name of the applicant, as specified for personal certificates.

Host and Service Certificates

In case the entity to be certified is a host or service, the requester (a natural person) shall prove to the satisfaction of the RA that the certificate application pertains to the networked system defined in the subject and is bound thereto, and that the requester is adequately authorised to act as a responsible person for the host and service, either by being the responsible system administrator of the host system concerned, by being either the registrant, administrative contact or operational contact for the first higher-level domain name in the domain name system that is registered in an

ICANN designated registry, or by being authorised by such an administrator, registrant, administrative or operational contact. In a service certificate, the name of the services is not otherwise validated.

The requestor shall be authenticated according to the procedure for Personal Certificates.

The CA shall ensure that the applicant's identity is verified in accordance with the stipulations in this CP/CPS. In addition, the RA shall record the process followed for issuance of each certificate and submit this in the form of signed documentary evidence to the CA for archival. This record shall include data provided by both the applicant and the RA.

The applicant shall provide as documentary information:

- The name, date and place of birth of the applicant
- The type and unique number of the identity piece presented by the applicant
- The contact address, phone number, and electronic mail address of the applicant
- The digest of the public key pair information pertaining to the request, as specified by the CA in the appropriate technical documentation.
- The host name and qualifications of the applicant as being the responsible person
- The signature of the applicant, indicating acceptance of all conditions in the CP/CPS
- The place and date of signing by the applicant

The RA will verify the correctness of the data on the identity piece, and make sure to a reasonable extent that the other information provided is correct. The RA will then

- Declare his or her name
- Note the time and date of successful verification
- Note the physical meeting place
- Sign the form, indicating the RA has verified the identity according to the requirements for RAs

Other stipulations

Other than the authentication described above, the CA does not check, and makes no assertion, about the subscriber's data in the certificate. In particular, the CA does not check and makes assertion that the subscriber is trustworthy, is acting in good faith at any particular time, or is a capable user, system responsible or software developer.

3.2 Routine Re-key

The CA will allow routine re-keying before expiration of the subscribers current certificate. The re-key request must be accompanied by a request based on a new key pair. Recertification of a public key certified at any previous time is not allowed except for secure hardware tokens as detailed below.

Re-key authentication may be by the procedure detailed in section 3.1.9, in which case the original identity documentation is used, or by signing the re-key request with a current, valid private key pertaining to the same subscriber, provided that the last verification by an RA is not longer ago than 5 years. In case the request is signed by the subscribers existing certificate, the CA shall assign a RA local to the subscriber to re-verify the subscriber data, the subscriber affiliation, and the right of the subscriber to a certificate. The RA must answer positively to this query.

For certificates issued based on key material exclusively held on a secure hardware token, in particular for Robot certs so held, the certificate may be renewed for a period up to 5 years for keypairs of at least 2048 bits RSA length.

3.3 Re-key after Revocation

A revoked key will not be re-certified. The authentication of a new certificate request follows the rules specified in section 3.1.

3.4 Revocation Request

Anyone can make certificate revocation requests to the CA, by email or by phone. A revocation request must be authenticated, unless the DutchGrid MS CA can independently verify that a key compromise has happened. This authentication can be via the procedure described in section 3.1 or via a digitally singed message with a non-expired and not previously revoked certificate issued under this policy to the subscriber or an RA, regardless of the CP/CPS version.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The DutchGrid MS CA will reject certificate applications that are not legitimate; in case a valid electronic mail address is supplied as part of the request, the DutchGrid MS CA may notify such applicant of this rejection. Obviously nonsensical requests will be discarded without notification. Requests that are not complete with documentation within 30 days may be discarded.

Applicants must generate their own key pair; the DutchGrid MS CA will never itself generate a key pair for an applicant. The DutchGrid MS CA does not accept secret key escrow responsibilities. Personal and robot certificates must not be shared; host and service certificates must be linked to a single network entity.

The minimum key length for all applications made before September 1st, 2012 is at least 1024 bits. The minimum key length for all applications made on or after September 1st, 2012 is at least 2048 bits.

The validity period is at most 365 days.

Certificate application is by submitting a PEM-formatted certificate request by electronic mail to <ca@dutchgrid.nl>, or by an on-line procedure on the web site as provided by the DutchGrid MS CA.

On initial application, and subsequently every 5 years, a hand-signed application form must be filled by the applicant and provided to the CA via the RA. The RA, after validating the subscriber's identity and validating the data on the form, counter-signs the form. The applicant or the RA sends it - by means that constitute traceable legal evidence - to the CA. The CA will verify the correctness of the form, validate the proof of possession challenge, and will check the relationship between the electronic certificate signing request and the paper-form-based identity validation.

In case the requester is a natural person requesting his or her own certificate or a robot certificate, the requirements detailed in section 3.1 apply. In case the entity is a machine or object, the administrator or responsible person will be authenticated based on the requirements detailed in section 3.1.

In case a re-key is requested, the certificate signing request must be submitted in an S/MIME signed document, by electronic mail or by uploading to the web site, according to the procedures defined by the CA, and the request must be signed with a valid certificate with the same subject name as that in the request.

For robot certificates, the applicant must prove to the RA that a secure hardware token was used to generate the private key and is used to hold the private key.

4.2 Certificate Issuance

On receipt of a certificate request that qualified according to this CP/CPS, the CA or RA will carefully check the compliance, and validity of any documents presented by the subscribers. Only after successful authentication, the DutchGrid MS CA will issue a certificate. Such issuance will be notified to the subscriber at the electronic mail address specified as part of the request. On request of the subscriber, another means of communication may be selected. If the communication fails permanently, the certificate may be revoked without further notice. No confirmation of receipt of electronic mail notification is done.

For each re-key request, an RA is contacted by the CA to re-affirm the eligibility and data correctness in the application, before a new certificate is issued.

A request for certification is normally handled within three working days after both the electronic certificate signing request and the completed and correct paper validation form have been received; however, during the period around New Year the response period may be up to 7 working days.

The CA will wait for at most two weeks, if either of the electronic submission or the paper-based form is missing. Following that period the request may be discarded.

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 when the secret key pertaining to the certificate is compromised or suspected to be compromised. This includes situation where:

- the subscribers data as represented in the certificate have changed (name changed, machine or object decommissioned, organisation dissolved or no longer eligible under the criteria detailed in section 1.1.3);
- the subscribers data is suspected to be inaccurate;
- the associated private key has been compromised or misused;
- the associated private key is suspected to have been compromised or misused; or
- the subscriber is known to have violated his obligations with regard to the DutchGrid MS CA.

4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate or by the CA or RA that issued or was part of the issuance of the certificate. Also, any person currently responsible for a certified machine or object can request revocation.

Other entities may request revocation, presenting event proof of knowledge of the private key compromise or change of subscriber's data.

4.4.3 Procedure for revocation request

The DutchGrid MS CA will handle request for revocation that reach it by any means, authenticated or unauthenticated. If the DutchGrid MS CA can independently verify that a certificate has been compromised or misused, DutchGrid MS CA will revoke the certificate immediately. In all other cases, the request for revocation will be authenticated as detailed in section 3.1.

4.4.4 Revocation request grace period

If the subscriber discovers that a private key is compromised, the subscriber must request revocation immediately, i.e., as soon as reasonably possible compatible with the urgency of the compromise.

The DutchGrid MS CA has a maximum response time of one working day for validated revocation requests; it will handle revocation requests with priority as soon as the request is recognised as such.

After validation and processing of a revocation request, the CRL will be updated as soon as possible but within 1 hour, and the new CRL published in the on-line repository.

4.4.5 Circumstances for suspension

The DutchGrid MS 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 updated, re-issued and published within one hour after every approved certificate revocation, but at least once every thirty (30) days and at least seven (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 re key compromise

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

The following events are recorded electronically on the off-line CA signing system:

- initialisations of the CA software on the off-line system;
- certificate signing requests, including their configuration and profile
- issued CRLs
- issued certificates

The following events are recorded using paper forms held in the off-line archive:

- the CA operator processing the certificate requests
- identity validation data, as stored in the on-line protected repository
- issued certificate serial numbers and validity periods
- all data documented on the paper form by the applicant and the RA
- validated requests for revocation

4.5.2 Frequency of processing log

No stipulation.

4.5.3 Retention period for audit log

The minimum retention period is three years.

4.5.4 Protection of audit log

Electronic audit logs from the off-line CA signing system are copied periodically, but at least once every month, to alternative removable media in encrypted archives. Such encrypted archives are protected with a pass phrase of at least 15 characters. The archives are stored in a PIN-protected safe, where the PIN is known only to CA operators. The paper forms are stored in binders.

Both the safe and the binders are stored in a room with electronic access control, where access is restricted to CA operators and designated systems maintenance personnel of the Nikhef Computer Technology group.

4.5.5 Audit log backup procedures

As stipulated in section 4.5.4.

4.5.6 Audit collection system (internal vs external)

Authorized external auditors will have access to archival information, inasfar as allowed by applicable data protection guidelines.

4.5.7 Notification to event-causing subject

Subjects are notified on request acceptance, certificate issuance, and certificate revocation. RAs are notified of rekeying requests and revocations for end-entities validated by them.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of event recorded

The following events are recorded and archived by the CA:

- certification requests
- issued certificates, including
  - a paper based form related to each certificate signing session, detailing the ca operator, the list of certificates issued, and the serial numbers and the validity periods thereof
  - a paper-based audit trail pertaining to all initial identity verifications, with all data as specified in section 3.1.9
  - an on-line protected record including identity document type and serial numbers, or renewal RA confirmation linkage token
- requests for revocation
- issued CRLs
- all mail sent to the DutchGrid MS CA
- all mail received by the DutchGrid MS CA
- all signed agreements with other parties
- all signed RA compliance letters

On the off-line system, boot, initialisation, logout, and all system commands entered, and all actions that affect the status of certificates, are printed in near-real-time to a line printer, including a date and time stamp. This line printer has no memory and does not keep persistent state. The output of the line printer is kept in the locked cabinet containing the CA systems.

4.6.2 Retention period for archive

The minimum retention period is three years. Materials pertaining to the identity vetting are kept for at least three years post the validity of any certificates based on this validation.

4.6.3 Protection of archive

The electronic data on media related to the off-line CA signing system is kept on electronic flash media, and is stored in a PIN protected safe when not in use. The PIN is known only to CA managers and operators. Backup copies thereof are solely stored in this safe.

The on-line protected archive, except for the electronic mail exchange, is copied daily to another on-line system and from there to two physically separated tape storage locations. Access to this archive is protected with unix permissions, where only designated CA staff can login to the master instance of this archive; other system adminstrators of Nikhef and SARA have access to archival copies of the on-line protected archive as part of their system administration duties.

Access to the protected electronic mail archive is controlled by Unix-style permissions. The mail archive is stored on a central mail service system, protected by Unix-style permissions, where CA operators are configured to have access. System administration staff will also have access to these archives as part of their system-administration duties. The archive is copied daily to two physically separate tape storage locations.

The paper-based verification trail is stored on paper in a locked and access-controlled room at Nikhef.

4.6.4 Archive backup procedures

As stipulated in section 4.6.5.

4.6.5 Requirements for time-stamping of records

All on-line archives are time-stamped using an NTP-synchronised host clock. The archives collected on the CA signing system are time-stamped using a clock that is periodically synchronized against external wall clocks. Off-line archives are time-stamped using un-synchronized time sources, periodically verified against an absolute time source.

4.6.6 Archive collection system (internal or external)

The electronic on-line archives are stored in at least two physically different locations off-site.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key changeover

A new public key of the DutchGrid MS CA is generated and posted in the on-line repository mentioned in section 1.4. In addition, signed electronic mail is sent to relevant relying parties, and to the mailing lists of the peer coordinating bodies in which the DutchGrid MS CA participates.

At least 13 months before the public root certificate of the DutchGrid CA expired, the CA shall decide to either extend the validity period (following a risk assessment and taking into account the then-current best practice regarding life time), or to generate a new keypair and transition all signing services to this new key pair.

In no case shall end-entity certificates be valid for a period that extends beyond the validity of the issuing CA.

The CA shall issue CRLs for a given issuing CA and key pair for at least as long as there are valid end-entity certificates, and it shall issue at least one CRL after the last end-entity certificate for that CA and key pair has expired.

4.8 Compromise and Disaster Recovery

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

The DutchGrid MS CA off-line signing system is a computer without any fixed disk drives, and operates using an read-only operating system stored on CD-ROM. This machine, where the private key is activated, is not accessible via any network.

If the machine is corrupted or defective, it will be replaced by another, similar, system where the hard disks similarly have been removed. If the operating system CD-ROM proves defective, another instance of the CD-ROM is obtained from trustworthy sources and the appropriate PGP finger prints verified. Several sources and mirrors will be compared to ensure the operating system is genuine.

The private keys of the DutchGrid MS CA are only available in encrypted form on removable flash media. These media are only temporarily attached to the signing system when signing is being done, and are otherwise stored in a PIN-protected electronic safe located in a restricted-access controlled room.

If CA related data becomes corrupted, the cause will be diagnosed and the data restored from the latest back-up on the same or alternative media. All copies of all media that contain or have contained the private key will be permanently stored in a safe in a restricted-access controlled room, or will be sanitized locally and subsequently destructed securely according to then current best practice.

If any media containing copies of the private key (even in encrypted form) are lost, this is handled as an entity key compromise.

4.8.2 Entity public key is revoked

No stipulation.

4.8.3 Entity key is compromised

If media containing the (encrypted) private key are lost, this is handled as a major incident that will imply generating a new key pair and terminating all services associated with the lost key pair. This will be announced widely to all peer CAs, identified major relying parties, subscribers and any coordinating organisations in which the CA participates.

4.8.4 Secure facility after a natural or other type of disaster

In case of (natural) disaster, the DutchGrid MS CA administrator(s) will as soon as physically possible confirm that all CA activation materials are at the intended locations. Depending on the situation, disaster recovery will start.

4.9 CA Termination

Termination of the DutchGrid MS CA occurs when all services associated with the DutchGrid MS CA are terminated. In this case, the CA will:

- inform all subscribers, registration authorities, cross-certifying CA's, and all relying parties with which the CA has established relations,
- make publicly available information of its termination,
- stop distributing certificates and CRL's.

The CA manager and the host organisations are together responsible for the continued archival of all records as required in section 4.6.2.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The DutchGrid MS CA is housed at Nikhef, located at the Science Park Amsterdam in the Watergraafsmeer. The CA is located in the central computer housing facility of Nikhef, located on the second floor above sea level, in the section dedicated to the housing of Nikhef internal systems. The room is access controlled using electronic proximity keys, and is by construction suitably protected against burglary and break-ins. Access to the building is monitored via closed-circuit TV.

Note that this same building also houses part of the Amsterdam Internet Exchange in a separate section and the CA therefore profits from the civil engineering works related to that facility.

5.1.2 Physical access

Access to the Nikhef internal section of the central computer housing facility is limited to designated individuals related to the DutchGrid MS CA operations and the Computer Technology group system administration staff. Access to the separately locked cabinet housing the CA systems and safe is limited to CA personnel only

The CA infrastructure comprises several systems and locations in this room with different levels of protection

- Off-line CA signing computer system (i.e. the system without hard drive, booted from read-only OS media, to which USB keys are connected only when signing): in a locked cabinet to which only CA staff have access.
- CA signing keys, when not in active use, and all electronic archival and backup media: in a PIN protected electronic safe to which only CA operators and managers have access.

  Note that the private key itself is protected with a pass phrase on the electronic media.
- Paper audit trail archive: in a locked cabinet.
- On-line CA management system (also hosting the on-line protected archive) and the online-CA web hosting system (hosting only public data): in a locked cabinet to which CA staff and administrators have access. This system is linked to the network, but does not contain any key material.

5.1.3 Power and air conditioning

All CA systems and the environmental conditioning systems are connected to a no-break electrical power system with sufficient diesel fuel supply for 48 hours continuous operation.

5.1.4 Water exposures

No water-cooled systems or racks are used, and all systems are located on raised flooring. The systems are located on the first floor and therefore above flood level.

5.1.5 Fire prevention and protection

The room is equipped with smoke alarms and inert-gas fire suppression system. Guards are on duty 24x7 hours.

5.1.6 Media storage

All media related to CA operations are stored in the PIN controlled safe.

5.1.7 Waste disposal

All copies of all media that contain or have contained the private key will be permanently stored in a safe in a restricted-access controlled room, or will be sanitized locally and subsequently destructed securely according to then-current best practice.

5.1.8 Off-site backup

There is one off-site backup of the private key of the CA in a remote location, printed in encrypted form on paper, in a tamper-evident envelope, in a fire-proof safe to which only the CA manager has access. All CA material except for the private key on the off-line system is backed up to removable media on certificate and CRL publication, and those media (not holding key material) are held in locked offices of the CA staff at Nikhef. The on-line and on-line protected archives are backed up to two geographically distant remote locations.

5.2 Procedural Controls

5.2.1 Trusted roles

The CA has Managers and Operators. Managers have access to the both the off-line and on-line systems with elevated privileges. Operators may only use canned perform predefined operations on the CA on-line and off-line systems.

5.2.2 Number of persons required per task

There is no requirement for multi-person control for any task.

5.2.3 Identification and authentication for each role

Managers and Operators are given access control material that identifies their role. No additional authentication to assume that role is required.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The role of the CA requires suitably trained persons that are familiar with the importance of a PKI, and who are technically and professionally competent. The CA manager will assign CA operators and verify their suitability. There are no background checks or clearance procedures for CA operators.

An RA can be any person that is familiar with the importance of the PKI and is procedurally and professionally competent. The CA manager will designate RAs after suitable induction and training.

5.3.2 Background check procedures

All CA personnel must be permanent employees of Nikhef.

5.3.3 Training requirements

Each CA Operator must read and demonstrate knowledge of the operating procedures by performing the requisite operations on the on-line and off-line system in the presence of a CA Manager.

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 the event of unauthorised actions, abuse or unauthorised use of systems, powers or capabilities by the CA operators or RAs, the CA manager may revoke the privileges concerned.

5.3.7 Contracting personnel requirements

No contracted personnel will be allowed access to trusted materials.

5.3.8 Documentation supplied to personnel

It is the responsibility of the CA manager to supply the Operators and the RAs with a copy of this CP/CPS and suitable additional documentation to implement the requirements documented therein.

6 TECHNICAL SECURITY CONTROLS

6.1 *Key Pair Generation and Installation*

6.1.1 Key pair generation

Each subscriber and responsible person should take reasonable steps to ensure that the key pair is generated with an reputable algorithms and with a sufficiently high entropy.

Key pairs for the DutchGrid MS CA are generated exclusively by DutchGrid MS CA staff members on a dedicated system not connected to any network and booted from trusted media, using a recent and trustworthy version of the OpenSSL software package.

6.1.2 Private key delivery to entity

Each subscriber must generate his or her own key pair. The CA does not generate key pairs for its subscribers. .

6.1.3 Public key delivery to certificate issuer

The entity must submit an electronic certificate signing request together with the public key according to the procedures detailed in section 4.1. This may be either via e-mail or via a secure and not-secured public web site.

6.1.4 CA public key delivery to users

The CA certificate including its public key is delivered to all entities via the online public web site of the CA. They CA may provide this certificate to other parties for further re-distribution.

6.1.5 Key sizes

Signing requests based on key pairs with a length of less than 1024 bits are not accepted. After September 1st, 2012, requests based on key pairs with a length of less than 2048 bits are not accepted. The CA key length is 2048 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

The public exponent of any key pair must not be three (3).

6.1.8 Hardware/software key generation

If the key pair is associated to a robot certificates, it must be held on a secure hardware token, and the key pair must be generated on said token.

Keys pairs for all other purposes may be generated as soft tokens (files). It is up to the subscriber to ensure that the key pair is generated using trustworthy software on a machine that is free from intrusions.

The DutchGrid MS CA signing key is generated as a soft token using a version of the OpenSSL software.

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

Subscriber keys may be used for authentication, message integrity and session key establishment. The certificate *keyUsage* bits are set such as to support these purposes, but for legacy compatibility the bits corresponding to data encryption and non-repudiation may be asserted in specific subscriber certificates.

The CAs private key is the only key allowed to sign certificates and CRLs. The certificate *keyUsage* bits are set to allow certificate signing, CRL signing and message integrity protection.

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 pass phrase) that is strong. 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.

  Alternatively, the private key may be stored on secure hardware tokens as defined in section 6.2.1, if the hardware token is similarly protected with a strong pass phrase.
- Certificates issued to hosts or services which are used solely for authenticating the host or service run thereon in targeted communications 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 person-group 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.

  Alternatively, the private key may be stored on secure hardware tokens as defined in section 6.2.1, in either protected or unprotected access.
- For robot certificates, the private key must be generated and stored on a secure hardware token as defined below, and be generated and used in accordance with section 3.1.1 and 6.1.8.

6.2.1 Standards for cryptographic module

Secure hardware tokens, whenever referenced in this document, are those hardware security cryptographic devices or hardware security modules that operate on and hold asymmetric cryptographic key pairs in such a way that the private part of the key pair cannot ever be extracted in unencrypted form, can only be unencrypted inside the device, and the encrypted form, if available, uses 128 bit symmetric key encryption or equivalent or stronger., and where the key pair has been generated inside the cryptographic device. Any tampering, any substitution or extraction of keys, and any unauthorized modification of the activation data, must leave evidence on the secure hardware token.

Secure hardware tokens and hardware security modules that comply with the requirements of FIPS 140-1 level 2 or higher, or FIPS 140-2 level 2 or higher, and where the key pair has been generated inside the module, are adequate to meet the requirements set forth above. If not FIPS certified, implementation of an equivalent security level and appropriate mechanisms on the token must be demonstrated: the vendor must have built the device with the intention of obtaining FIPS 140-2 certification at level 2 or higher, and must either intend to submit the device for certification, or have it in process of certification.

The CA private key is kept as a software token on an off-line protected system, which is stored in a PIN-protected electronic safe when not in active use.

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

Private keys pertaining to personal certificates must not be under multi-person control.

Subscriber private keys pertaining to host and service certificates may be under the control of more than one individual working under the control of the responsible person designated in the subscription.

The CA private key is under sole control of the designated CA managers and operators, who can act alone in their capacity.

6.2.3 Private key escrow

Private keys must not be escrowed.

6.2.4 Private key backup

The CAs private key is backed up as part of the backup of the off-line signing system on removable media, kept in a PIN-protected safe.

6.2.5 Private key archival

An additional print-out copy of the encrypted private key is kept in a access-controlled fire safe at an off-site location to which only the CA manager has access.

6.2.6 Private key entry into cryptographic module

The subscriber private key in a hardware token, when so required by sections 3.1.1, 6.1.8, and 6.2, must be generated inside that token. For other purposes, it is permissible to upload the private key into the hardware token.

6.2.7 Method of activating private key

The DutchGrid MS CA private key is protected by symmetric cryptography, derived from a strong pass phrase of at least 15 characters. There is no physical backup of the pass phrase - the passphrase will be learnt by all CA managers and CA operators who require access to this key, as listed in the on-line repository.

6.2.8 Method of deactivating private key

The pass phrase for the CA private key is only kept in memory on the signing machine for the duration of a single operation.

6.2.9 Method of destroying private key

After termination of the CA and after the archival period for archives has expired, all media that contain the private key of the CA will be securely and permanently destroyed, according to then best current practice.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The CA archives all issued certificates and its own public key.

6.3.2 Usage periods for the public and private keys

Subscriber certificates have a validity period of 365 days. The DutchGrid MS CA certificate has a life time of up to 30 years.

6.4 Activation Data

6.4.1 Activation data generation and installation

No stipulation.

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.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The CA protected on-line management server is a dedicated system, on a shielded sub-network with appropriate port-filtering firewall rules, and additionally protected by system-local network access tables. The operating system is maintained with the latest patches, based on signed patch distributions.

Services on the protected on-line management server are reduced to the minimum (ssh, http and https). Access to those services and programs needed for CA management operation is restricted to hosts within the Nikhef network domain, and then only via client-authenticated https. The request submission interface is accessible from outside the Nikhef network (via http and https).

The off-line CA signing system is a dedicated system not connected to any network. It runs a read-only operating system, verified against publicly available and distributed cryptographic digests thereof. The CA signing software is kept on removable media that are stored in a PIN-protected safe when not in active use.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

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

Management interfaces and software related to CA operations are developed on a separate system which does not have production data. Software maintenance may be carried out on the production systems.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

Certificates are generated on a machine that is not connected to any network.

The on-line protected management server is protected by sub-network specific port-filtering firewalls specific to its subnet, and additionally by system-local network access tables. Only ports that are connected to services offered on the specific system are opened, all others are closed.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

Subscriber certificates: X.509 version 3

DutchGrid MS 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 a DER formatted CRL
- *certificatePolicies*

  non-critical, one or more OIDs, with at least one referring to this CP/CPS and one referring to the IGTF Authentication Profile for “Classic X.509 Certification Authorities with Secured Infrastructure”, said OID being 1.2.840.113612.5.2.2.1.
- *authorityKeyIdentifier*

  non-critical, keyid
- *subjectKeyIdentifier*

  non-critical, hash
- *netscape Certificate Type* (not used by default)

  non-critical, SSL Client, S/MIME.

  Note: Object Signing may be added on request for personal certificates, in conjunction with the *extendedKeyUsage codeSigning* attribute.

  Note: SSL Server will be added to host and service certificates
- *extendedKeyUsage*
  non-critical, clientAuth

  Note: codeSigning may be added on request for personal certificates, in conjunction with the assertion of *netscape Certificate Type objectSigning.*

  Note: serverAuth will be added to host and service certificates
- *netscape Certificate Policy URL*

  non-critical, a single HTTP URL referring to the location of this CP/CPS
- *netscape Certificate Comment*

  non-critical, contains a liability waiver, referral to this CP/CPS, and the internal certificate request identifier (“tag id”)
- *subjectAlternativeName*
  - for host and service certifices: 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 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@dutchgrid.nl
- *subjectKeyIdentifier*
  non-critical, hash
- *CRL Distribution Points*
  non-critical, one URI http://ca.dutchgrid.nl/medium/cacrl.pem
- *netscape Certificate Type*
  non-critical, SSL CA, Email CA, Object CA
- *netscape Certificate Authority Revocation URL*
  non-critical, one URL http://ca.dutchgrid.nl/medium/cacrl.pem
- *netscape Authority Policy URL*
  non-critical, one URL http://ca.dutchgrid.nl/medium/policy/
- *netscape Certificate Comment*
  non-critical, "DutchGrid and Nikhef medium-security Certification Authority; policies at http://ca.dutchgrid.nl/medium/policy/"

7.1.3 Algorithm object identifiers

Certificates and certificate revocation lists issued by the CA MUST have the signature based on a digest with the strength of at least SHA-1, and MAY have the signature based on SHA-256, SHA-384 or SHA-512.

7.1.4 Name forms

The issuer name shall be

`"/C=NL/O=Nikhef/CN=Nikhef medium-security certification auth"`

The subscriber subject names shall start with "O=dutchgrid" as the first attribute-value pair in the subjectName sequence. Thereafter, a single organisation attribute shall follow indicating the certificate subject class as specified in section 3.1.1, using one of the following values

- "O=users" for certificates issued in the "users" class
- "O=hosts" for certificates issued in the "hosts" and "service" class
- "O=servers" for certificates issued in the "servers" class
- "O=robots" for certificates issued in the "robots" class

Thereafter shall follow at least one organisation attribute, optionally followed by an organisationalUnit attribute. Thereafter shall come at least one commonName attribute.

Thus, permissible name forms are, in OpenSSL one-line notation:

- `"/O=dutchgrid/O=users/O=…[/OU=…]/CN=…"`
- `"/O=dutchgrid/O=hosts/O=…[/OU=…]/CN=…"`
- `"/O=dutchgrid/O=servers/O=…/CN=…"`
- `"/O=dutchgrid/O=robots/O=…[/OU=…]/CN=Robot:…"`

7.1.5 Name constraints

The CA does not support the name constraints extension.

7.1.6 Certificate policy Object Identifier

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 extension

This extension is not used.

7.1.8 Policy qualifiers 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 version 1 CRLs are issued.

7.2.2 CRL and CRL entry extensions

Certificate revocation lists issued by the CA MUST have the signature based on a digest with the strength of at least SHA-1, and MAY have the signature based on SHA-256, SHA-384 or SHA-512.

8 SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

Minor editorial changes to this document and the procedures implementing it can be made without announcement to subscribers, relying parties of cross-certifying CA's, provided they do not compromise the security level under which the CA operates.

Substantial changes in policy or in the technical security controls will be notified to all relevant relying parties, all cross-certifying CA's and to the public on-line repositories. It will also be announced to the PMAs and other coordinating bodies in which the CA participates.

8.2 Publication and notification policies

This policy and any older versions are available from the on-line repository mentioned in section 1.4.

8.3 CPS approval procedures

New versions of the CP and CPS are approved following a review process in which advise from the PMAs, any other coordinating bodies in which the CA participates is taken, and where the national constituencies are consulted. The CA operates under the authority of the Stichting FOM Nikhef who lends authority to this CP/CPS, and whose representative for the DutchGrid and Nikhef Medium-Security CA approves any changes to the CP, CPS and all derived procedures.

9 Appendices

9.1 List of approved photo-identity document types

The following photo-bearing identity documents are allowed for purposes of identity verification by all RAs, roving RAs, and the Central RA Service:

- A valid passport or similar official document issued by a recognised national government for the purposes of identification or for foreign travel.
- A valid driving license, issued by a recognised body for issuing such licenses that must show an issuer designation and unique document number.
- A European identity card.
- A residence permit issued by the immigration and naturalisation service of a member state of the European Union.

In all cases, it must be possible for the RA to ensure to a reasonable extent that the document presented is authentic and valid, and it should bear the name of the applicant.

9.1.1 Approved photo-identity document types for specific RAs

RAs shall only accept for photo-ID documents during tele-meeting verification if they have previous acquaintance with the physical properties of such document and can check its authenticity properties.

Specially designated Registration Authorities may implement alternative identity vetting mechanisms that are based on an initial in-person identity vetting, and that are at least as strong as the methods described in section 3.1.9 as supplemented by list of allowed photo-identity document types listed above.

A list of such RA is given below:

- At this time, there are no RAs designated that can allow identity vetting based on any alternate procedure.

9.2 Registration form templates

The applicant shall complete and submit to the RA for verification a signed document stating the applicant's registration details and acceptance of the conditions stated in this CP/CPS. The following documents, for persons or robots and hosts or services, respectively, are used for this purpose.

Details and layout of these forms may change.

9.2.1 Personal and robot registration form

http://ca.dutchgrid.nl/request/caregform.pdf

9.2.2 Host, service and server registration form

http://ca.dutchgrid.nl/request/caregformhost.pdf

9.3 List of Changes

9.3.1 Versions 1.0 and 1.5

These versions were not in RFC 2527 format. Version 1.0 was drafted February 2001 and version 1.5 on May 15th, 2001.

9.3.2 Version 2.0

Rewritten the policy according to the RFC2527 template. This version was issued on September 24, 2001.

9.3.3 Version 2.1

The responsible person to attest to the the validity of WTCW-based organizations is now the Nikhef directorate. This version was issued on November 5, 2001.

9.3.4 Version 2.2

This version was issued on November 4, 2004. Changes in this version:

- Telex contact removed
- clarified slightly the constituency
- added non-discriminatory clause for the constituency
- Made the list of RAs dynamic. The RAs are published in the on-line repository
- opened possibility to delegate operation, as long as responsibility remains with the CA managers
- RAs must now be real individuals (no groups)
- RAs must nu also comply with current best practices (not only the literal CP/CPS)
- removed references to the EU DataGrid project, and added those to EUGridPMA in audit section
- allowed alternative naming convention of hosts
- clarified uniqueness (linked to only one *entity*)
- removed option for voice authentication
- added authentication based on existing records
- now really set max lifetime to 1 year for end-entity certificates
- added description of paper-based trail
- tightened revocation grace period
- minor changes on archiving and NTP synchronisation to remove anomalies
- added critical keyUsage extension
- added CA subject name

9.3.5 Version 3.0

This version was issued on May 14th, 2007. This version is a significant rewrite of the policy, introducing new elements such as “robot” certificates, as well as making the written policy more strict and a better fit to the actual procedures. Whereas the previous policy (although not the previous actual practices) we too lenient and not necessarily in correspondence with the relevant guidelines, this policy realigns the written text with the actual operational practices and applicable authentication profiles.

Apart from a large amount of editorial changes, the following major changes have been introduced in version 3.0

- The documented identity vetting process description in this policy is now aligned with the paper-based registration mechanism, and requires the use of a few, designated, photo-identity document types.
- Describe explicitly that an RA is contacted on each re-key request (as is current practice).
- Robot certificates (whose private key is held on a security token, with alternative subject naming, and whose certificate designates it as a robot using appropriate policy identifiers) have been introduced.
- Describe allowed usage of user, host, service, server and robot certificates.

- Details have been added to the certificate profile section to better document the actual certificates issued.
- Rules for allowed name forms have been tightened (version 2.2 allowed too many variants as it was geared towards a changeover that did not materialize).
- Description of the four classes of repositories added.
- Description of the latest security setup.
- Removed references to ZIP disks and replace them with references to the current USB flash memory based system.
- Constraints on the allowed characters in subject names.
- Consumers are no longer eligible as subscribers (since consumers under Dutch law have some inalienable rights that ill fit the operational model of the CA).
- Added the possibility to recoup costs for any hardware security tokens provisioned to a subscriber.
- Allowed other policy OIDs to be included in the issued certificates, indicating compliance with such other policies. In particular, the OID of a robot 1SCP or the OID of the appropriate Authentication profile may be included.

This version 3.0 owes significantly to the work of Jens Jensen and the UK e-Science CP/CPS.

9.3.6 Version 3.1

This version was issued on November 30th, 2007 and includes the following modifications:

- Better wording to reflect that a service name included in the common name of a service certificate merely reflects the applicants statement thereof. The domain name portion thereof is verified by the RA.
- The client certificate profile has been updated to conform to the draft Grid Certificate Profile version 0.25, and now includes key usage *dataEncipherment* and the *extendedkeyUsage* extension.
- Personal and robot certificates no longer assert *SSL Server* or *serverAuth*.
- The policy OIDs included in end-entity certificates include a reference to the OID arc assigned to the IGTF "classic" Authentication Profile.

9.3.7 Version 3.2

This version addresses the changes as a result of the Self-Audit 2011

- In section 8.3, added description of the approval process
- In 6.5.1, added explicitly that the off-line system is dedicated
- In section 5.1, updates the physical controls to reflect move to Room H2.34b and off-site fire-safe backup of encrypted private key (also updated section 6.2.5).
- Knowledge distribution of CA private key pass phrase description added in 6.2.7
- In section 4.6.1, added the log keeping on the off-line system using a line printer
- In section 4.7, added the migration process description for key changeover
- In section 3.2, added procedure to renew (not re-key) certs with key material on hardware tokens for 2048 bit keys/5years
- In section 5.3, added that only permanent staff can hold trusted positions
- In 4.5.7, added notification of event-causing subjects (already operational)
- In 4.5.6, allow external auditors access to relevant information
- In 4.6.2 describe audit retention policy in related to certificate validity and rekeying

9.3.8 Version 3.3

- Allow more (secure) hash algorithms besides SHA-1 in section 7

- Depricate the use of nsCertType (will be dropped by default)
- Institute Nikhef changed to new full-name and capitalisation
- Replaced form examples with web links

9.3.9 Version 3.4

- Allow for voucher-based electronic submission of documents with email-address verification in addition to postal and facsimile submission of forms (section 2.1.2)
- Allow conditional tele-meeting verification by RAs (section 3.1.9) based on pre-existing relationships and additional compensatory controls (verification of phone number instead of physical location and NFC readout of photo-ID documents). The ink-signature of the RA is then replaced by a random unique code that is validated out-of-band by the CA.