DutchGrid CA

DutchGrid and Nikhef Certification Authorities Service

DutchGrid Root CP/CPS

version v0.03-20160416

Document Revision Information

Document Identifier	1.3.6.1.4.1.10434.4.2.7.1.0
Document Version	v0.03-20160416 (DRAFT)
Last Modified	2016-04-17
Last Edited By	David Groep

Table of Contents

Document Revision History

Version	Date	Comments
0.01	*Feb 13, 2016*	*Initial draft*
0.02	*Feb 29, 2016*	*Added permissible subordinate subject name to include old Nikhef MS CA*
0.03	*Apr 16, 2016*	*Incorporated review comments by Reimer*

1 INTRODUCTION

1.1 OVERVIEW

The DutchGrid and Nikhef Certification Authorities Service – hereafter called the DutchGrid CA (DCA) Service - provides a differentiated set of offers for identity certification for science and research for the purpose of cross-organisational distributed resource access, solely in the context of academic and research and similar, not-commercially competitive, applications. These services are primarily intended for the practitioners of scientific research in the Netherlands, appropriately taking into account the European and global nature of research and collaboration.

The DCA Service operates a set of PKI X.509 certification authorities (CAs), including self-signed issuing CAs (e.g. the DutchGrid and Nikhef Medium-Security X.509 Certification Authority), a Root CA that only certifies subordinate CAs, and a set of subordinate issuing CAs (ICAs).

This Policy and Practice Statement is pertinent to the DutchGrid Root G1 CA (2016 edition).

1.2 DOCUMENT NAME AND IDENTIFICATION

This is the DCA Service Root (2016 edition) Certificate Policy and Certification Practice Statement. It is generally identified by urn:oid:1.3.6.1.4.1.10434.4.2.7.1. This version is specifically identified as urn:oid:1.3.6.1.4.1.10434.4.2.7.1.0.

The document shall be referenced as the "DutchGrid Root CP/CPS".

The "DutchGrid and Nikhef Certification Authorities Service Root Generation 1 CA" (2016 edition) shall be referenced as the "DCA Root G1".

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

The DCA Root G1 is an off-line CA that exclusively issues certificates to subordinate CAs operated by, on behalf of, or under mutual understanding with the DutchGrid CA Service.

1.3.2 Registration Authorities

The DCA Root G1 is directly operated by the CA administrators, who also take the role of registration authority. All registration will be performed by the CA administrators, exclusively via documented in-person processes.

1.3.3 End Entities

The DCA Root G1 shall only issue certificates to subordinate CAs as stipulated in section 1.3.1

1.3.4 Relying Parties

Relying parties are individuals or organizations using the certificates to verify the identity of CAs signed with the DCA Root G1. This CP/CPS does not limit the community of relying parties.

1.3.5 Other participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Usage

Certificates issued by this CA are intended to be used in compliance with this CP/CPS.

The certificates issued by the DCA Root G1 CA are not appropriate for any application other than for science, research, and innovation, and then for the purpose of (cross-organisational) distributed resource access, solely in the context of academic and research and similar, not-commercially competitive, applications.

The DCA Root G1 certificates are primarily intended for the practitioners of scientific research in the Netherlands, appropriately taking into account the European and global nature of research and collaboration.

1.4.2 Prohibited Certificate Usage

Certificates shall be used exclusive in compliance with this CP/CPS – other use is prohibited.

Certificates must not be used for unlawful purposes, and must not be used in any way that could harm, be defamatory, cause injury, or be detrimental to the reputation, safe operation or good standing of the DCA Root G1 CA, the DCA Service, Nikhef or its partners and personnel, or SURF, or if the use would result in liability (financial or otherwise) of Nikhef, SURF, or any individual involved in the operation of the DCA Service.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

This document is administered by the DCA Service, which is managed by Nikhef, the Dutch national institute for subatomic physics for the benefit and purpose of the Dutch National e-Infrastructure coordinated by SURF.

The Organisation contact details are:

DutchGrid CA c/o Nikhef
Science Park 105, NL 1098 XG Amsterdam, The Netherlands
Phone: +31 20 592 2000, Fax: +31 20 592 5155
Email: ca@dutchgrid.nl

The Policy Management Authority of the DCA Root G1 shall be its Administrators.

1.5.2 Contact person

The responsible Managers of the DCA Service are:

David L. Groep, davidg@nikhef.nl, postal address as above

The responsible Adminstrators of the DCA Root G1 are:

David L. Groep, davidg@nikhef.nl, postal address as above
Dennis van Dok, dennisvd@nikhef.nl, postal address as above

1.5.3 Person determining CPS suitability for the policy

This document contains both the Policy and the applicable Practice Statement, hence a CPS suitability determination is not relevant for the CPS of the DCA Root G1.

The suitability of Certificate Policy and Certification Practice Statements for subordinate CAs that are to be certified by the DCA Root G1 is determined by the DCA Service Managers.

1.5.4 CPS approval procedures

Changes to the Policy and the Practice Statements are approved by the DCA Service Manager, having consulted with relevant accreditation bodies and representative stakeholder bodies.

1.5.5 Modification of the CP/CPS

Modifications of the CP/CPS may be done any time. Changes will take affect after 14 days following its adoption by the DCA Service Manager in accordance with section 1.5.4, and having been published.

1.6 DEFINITIONS AND ACRONYMS

Conventional PKI definitions apply. The following terms are specific to this document:

DCA	DutchGrid and Nikhef Certification Authority
DCA Service	The ensemble of services and CAs offered by the DCA
DCA Managers	The individual(s) responsible for the coordination of the DCA policy, its interpretation, adoption, evolution, accreditation, and verification.
DCA Administrators	The individuals responsible for the technical development and implementation of the DCA Service and for ensuring its continued compliance with the Policy and documented Practices
DCA Operators	The individuals that can issue certificate and publish updated revocation information for the specific DCA CA for which they have been granted an operational privilege. For the DCA Root CA, the only DCA Operators shall be the DCA Administrators
DCA Root	The self-signed off-line root certification authority of the DCA

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The DCA Root G1 shall publish its own self-signed certificate, the certificates it issues, and its policies, and ancillary public document in an on-line accessible repository at

http://ca.dutchgrid.nl/dcaroot/

The DCA Root G1 shall publish revocation lists at

http://crl.dutchgrid.nl/dcaroot/crl/

2.2 PUBLICATION OF CA INFORMATION

The DCA Root G1 shall make the following publicly available on the relevant on-line repositories:

1. The DCA Root G1 CA's self-signed certificate in at least DER encoding, and with a textual representation thereof
2. A DER-formatted CRL
3. A copy of this CP/CPS document and of any previous versions pertaining to valid issued certificates.

2.3 TIME OR FREQUENCY OF PUBLICATION

Changes to the materials contained in the repository shall be published promptly.

2.4 ACCESS CONTROLS ON REPOSITORIES

The DCA Root G1 CA imposes no access control restrictions to the published information including policy, certificate, issued certificates and CRLs. Excluding reasonable scheduled maintenance or unforeseen failures, the on-line repository will be available on a continuous basis.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The DCA Root G1 assigns subjectName in its issued certificates as non-empty X.501 distinguished names (DNs). Each assigned subjectName identifies a single entity and shall never be re-assigned to any other entity.

The issuerName in the issued certificates shall be set to the name of the DCA Root G1 CA, which is represented as a non-empty X.501 DN.

3.1.2 Need For Names to be Meaningful

The Subject Name will represent the subordinate CA in a clear manner. It shall name its subordinate CA in the subjectName in a way that – at the time of initial issuance – will clarify the purpose, scope, constituency, target audience, or technical model of the subordinate CA.

3.1.3 Anonymity Or Pseudonymity of Subscribers

The DCA Root G1 will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Names will use the PrintableString sub-set encoding and will contain only upper- and lower-case characters , numerals, space, dash, dot, and (round) brackets. These should be interpreted as per the encoding used.

3.1.5 Uniqueness of Names

The subjectName shall be unique and – once assigned to an entity – will not be re-assigned to any other entity.

3.1.6 Recognition, Authentication and Role of Trademarks

Where this is known to the DCA Service, brands and trademarks recognised in the Benelux will not be used without appropriate authentication of the entity named, and will be assigned only to or with endorsement of the recognised brand and trademark holder, or where reasonable expectation exists that such an assignment will meet with consent of the brand or trademark holder.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The requester must prove possession of the private key which corresponds to the public key in the certificate request. This is done through the submission of a digitally signed PKCS #10 request.

3.2.2 Authentication of Organization Identity

The DCA Root G1 issues certificates to subordinate CAs operated by, on behalf of, or under mutual understanding with the DutchGrid CA Service. It will authenticate any external entities, i.e. entities that are not the DCA Service itself and not Nikhef, by identifying their representatives by name, validating these names by comparison with official government-recognised photo identification documents during an in-person meeting, and by recording their affiliation with the organisation through independent validation and/or public sources.

3.2.3 Authentication of Individual Identity

In the course of any necessary authentication of individuals in the course of validating subordinate CAs, the DCA Root G1 registrars will identify individuals by name, validating these names by comparison with official government-recognised photo identification documents during an in-person meeting. It will record sufficient information in order to establish that the same individual re-authenticated at a later date. This information will include: (i) the full name of the individual, (ii) a hand-written signature of the individual, (iii) the trailing part of the serial number of the identity piece and type and its issuing authority and/or issuing country, (iv) physical and electronic business contact information of the individual. This information must be in substantial accordance with the information on the authenticated photo identification document.

The authentication document shall include confirmation that the individual is associated with the private key pertaining to the issued certificate, e.g. by including either a digest of the public key or the entire public key material.

The authentication document shall be dated and counter-signed by a DCA Root Administrator.

3.2.4 Non-verified Subscriber Information

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.

3.2.5 Validation of Authority

Beyond the need for names to be meaningful and non-confusing, the DCA Root G1 registrars will not verify more information than is needed to associate an individual with the organisational entity. DCA Service Administrators are *ipse facto* authoritative for any DCA subordinate CA entities.

3.2.6 Criteria for Inter-operation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION OF RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine re-Key

Routine re-key shall be accomplished using the same procedures as for initial registration.

3.3.2 Identification and Authentication for re-Key after Revocation

Identification and authentication for re-key after revocation shall be accomplished using the same procedures as for initial registration.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Anyone can make certificate revocation requests to the DCA Root G1 CA, in-person, by email, or by phone. A revocation request will be authenticated, unless the request is made directly by the Administators of the DCA service named in section 1.

In all other cases, 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. It can also be made by duly so-authorized individuals of the organisation that was validated in support of the issuance of the subordinate CA certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

Applications for a subordinate CA certificate, to be signed by the DCA Root G1, can be submitted by (i) Administrators of the DCA Service, (ii) other qualified individuals or organisations that – at the discretion of the DCA Service Administrators – can reasonably demonstrate the benefit of their certification by the DCA Root G1 CA for Nikhef, for the Dutch National e-Infrastructure coordinated by SURF, for the members and operational partners of SURF, or for other infrastructures, projects and endeavours in the domain of multi-domain distributed authentication for innovation and scientific research to which a Dutch research organisation is a party or in which a Dutch research organisation has a reasonable interest.

Acceptance of any certificate application is at the exclusive discretion of the DCA Managers and of Nikhef. Their decision, be it single or jointly, shall be final, without recourse, and no correspondence will be entered into.

4.1.2 Enrollment Process and Responsibilities

No stipulation.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

A certificate application shall be delivered in person by the requester to the DCA Services personnel in the form of secure off-line media. This shall be done at the point of authentication of individual identity and during the same in-person meeting.

Alternatively, the DCA Root G1 Administrators may permit generation of a key pair on the designated off-line system in the presence of and under the responsibility of the applicant. This key pair will be generated by well-known cryptographic software using a cryptographically sound PRNG. The key pair, including the signed certificate, will then be made available on secure off-line media to the applicant.

In either case, the procedure shall be witnessed and logged.

4.2.2 Approval or Rejection of Certificate Applications

If the certificate request does not meet one or more of the criteria set in item 4.1.1, or that does not meet the technical requirements for certificates, or for trustworthy operation of certification authorities, will be rejected.

4.2.3 Time to Process Certificate Applications

Certificates requests, having been validated and approved, are processed without undue delay.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

A DCA Service Operator will perform any actions necessary to issue a correct certificate, in accordance with this CP/CPS. A single DCA Service Administrator may issue the certificate, as

long as other witnesses are present and the action is duly logged. The list of those present will be logged and archived.

The DCA Service Administrator in charge will verify the issued certificate for correctness.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

When the issued subordinate CA certificate has been applied for by an organisation or individual not being the DCA Service itself, it shall inform the applicant of issuance by sending the issued certificate by email.

When the key material has been generated for the subordinate CA by the DCA Service itself on its own designated off-line system, any private key material will be stored only on secure off-line media, and will only be present during an in-person meeting with the authenticated entity, having validated the person by means of the valid government-issued photo identification document. The authenticated entity generates its own key material on specific media on the off-line system made available by the DCA Service.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

Certificates issued by the DCA Root G1 CA will be published in the on-line repository at the discretion of the DCA Service and/or on request of the subscriber. This publication will usually be limited to only currently valid certificates.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

Apart from the publication of certificates in the on-line repository, the DCA Root G1 CA will not normally notify any other entity but the applicant about certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The subscriber (subordinate CA) private key and certificate usage shall be guided by the respective CAs CP/CPS, which has been assessed for suitability by the DCA Root Managers.

Subscribers (subordinate CAs) may not use their certificate issued by the DCA Root G1 if they operate outside their stated policy and practices. They may also not use their certificate if they engage in activities incompatible with the scope, purpose and policy as described in this document, or if the use of their DCA Root G1 certificate would in any way harm, be defamatory, cause injury, or be detrimental to the reputation, safe operation or good standing of the DCA Root G1 CA or the DCA Service, or if the use would result in liability (financial or otherwise) of Nikhef, SURF, or any individual involved in the operation of the DCA Service.

4.5.2 Relying Party Public Key and Certificate Usage

The usage of the subject CA public key and certificate by relying parties shall be specified by the respective CP/CPS.

Relying parties may not use a certificate of the DCA Root G1 CA if such use would in any way harm, be defamatory, cause injury, or be detrimental to the reputation, safe operation or good standing of the DCA Root G1 CA or the DCA Service, or if the use would result in liability (financial or otherwise) of Nikhef, SURF, or any individual involved in the operation of the DCA Service.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances for Certificate Renewal

A certificate, be it the certificate of the DCA Root G1 CA itself or any issued (subordinate CA) certificate may be renewed or extended, provided that

- The maximum permissible usage period of the private key, being 30 years for the DCA Root G1 CA and 20 years for any subscriber (subordinate CA), has not yet been reached
- The private cryptographic key material is intact, of sufficient cryptographic strength at the time of renewal, and has not been compromised
- The applicant requesting renewal is authenticated according to the requirements of section 3, and represents the same entity.

Renewed certificates may be pre-dated to start at the time of issuance of the original first certificate.

4.6.2 Who May Request Renewal

Only authenticated representatives and individuals of the same entity to which the original certificate was issued may request renewal, as long as the conditions stated in section 4.1.1 are met. This may be the DCA Service itself.

4.6.3 Processing Certificate Renewal Requests

Requests may be processed as per section 4.2, or the DCA Root G1 CA – having recorded and retained the original PKCS certificate signing request – may re-issue based on the data that was originally submitted.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

As per section 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to other Entities

As per section 4.4.3.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

The DCA Root G1 CA shall re-key a subject CA certificate on request made by an authorized and authenticated representative of the certified entity or subordinate CA. This may be the DCA Service itself.

Re-key for subordinate CAs is discouraged. The DCA Root G1 CA recommends that a variant name is used and a new certificate issued.

4.7.2 Who May Request Certification of a New Public Key

As per section 4.1.1.

4.7.3 Processing Certificate Re-keying Requests

Re-keying requests shall be processed following the same procedures as for a new certificate issuance.

4.7.4 Notification of new Certificate Issuance to Subscriber

As per section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

As per section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

As per section 4.4.3.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

The DCA Root G1 CA treats modification requests as certificate renewal with modified extensions. The subjectName and issuerName cannot be modified. The validFrom and validUntil dates can be modified as defined in section 4.6. serialNumbers are assigned uniquely and at random by the DCA Root G1 CA and their modification on re-issuance is implicit.

All modification requests must also meet the criteria for certificate renewal.

4.8.2 Who May Request Certificate Modification

As per section 4.6.2.

4.8.3 Processing Certificate Modification Requests

As per section 4.6.3.

4.8.4 Notification of New Certificate Issuance to Subscriber

As per section 4.6.4.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per section 4.6.5.

4.8.6 Publication of the Modified Certificate by the CA

As per section 4.6.6.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As per section 4.6.7.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

A certificate will be revoked in the following circumstances:

1. The subscriber (subordinate CA) does not comply with this policy.

2. The certificate is not required any more by the subscriber (subordinate CA)
3. The subordinate CA ceases to function, ceases to function in accordance with its own policy, or violates its policy as approved at the time of certification.
4. The subordinate CA changes its policy without endorsement of the DCA Root Policy Management Authority.
5. The private key is lost or suspected to be compromised.
6. The information in the certificate is wrong or inaccurate.
7. The entity to which the certificate has been issued has been retired.

4.9.2 Who Can Request Revocation

Any entity who can prove or gains knowledge of the occurrence of any of the circumstances for revocation listed in section 4.9.1 should request revocation of the pertinent certificate.

4.9.3 Procedure for Revocation Request

The entity requesting revocation of a certificate shall submit their revocation request to the DCA Root G1 CA Administrators using the contacts in section 1.5.1.

Upon receipt of a revocation request, the DCA Root G1 CA shall:

1. Verify the circumstances for revocation
2. Verify the identity of the revocation requester in accordance with section 4.9.2

If all the conditions are met, DCA Root G1 CA shall then revoke the certificate.

4.9.4 Revocation Request Grace Period

Any party that becomes aware of circumstances for revocation should request a revocation as soon as possible but not later than within one business day.

4.9.5 Time within which CA must Process the Revocation Request

All reasonable requests for revocation shall be acted upon promptly, without undue delay, and with appropriate urgency. Once the request has been validated, the DCA Root G1 CA shall revoke the certificate forthwith, and publish updated revocation information.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties may rely on a certificate only as long as that certificate has not been included in a published certificate revocation list and/or only for as long as an available authoritative OCSP service gives a “valid” response.

Relying parties should check freshness of their revocation data as often as relevant, based on their own risk assessment. In absence of specific risks we recommend to download CRL data not more frequently than once every 60 minutes.

4.9.7 CRL Issuance Frequency

The DCA Root G1 CA shall issue a CRL at least once every 390 days and immediately after a certificate revocation. The CRL shall have nextUpdate set to 400 days after the issuance date.

4.9.8 Maximum Latency for CRLs

Following a revocation, a new CRL will be issued forthwith.

4.9.9 On-line Revocation/Status Checking Availability

The DCA Root G1 CA does not operate a production OCSP service.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

There are no other forms of revocation advertisement available.

4.9.12 Special Requirements Re-key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

A certificate may be suspended by temporary, reversible revocation.

Certificates may be suspended if one of the circumstances for revocation as stated in section 4.9.1 is deemed likely to be fulfilled, but such cannot be ascertained beyond reasonable doubt within one business day.

In such cases the DCA Root G1 CA, at its sole discretion, may decide to revoke a certificate and include it in a certificate revocation list, retaining the option to resurrect the validity of such a certificate at a later date if the circumstances proved not to be fulfilled.

4.9.14 Who can Request Suspension

As per section 4.9.2.

4.9.15 Procedure for Suspension Request

As per section 4.9.3. Suspension will only follow if the criteria for suspension cannot be validated to an extent sufficient to fulfil the requirements of section 4.9.3.

4.9.16 Limits on Suspension Period

The DCA Root G1 CA will not resurrect suspended certificates after 30 days of suspension.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The DCA Root G1 CA shall publish a full CRL in the on-line repository.

4.10.2 Service Availability

The on-line repository containing the CRL is provided with an intended continuous availability.

4.10.3 Optional Features

None.

4.11 END OF SUBSCRIPTION

A subscription ends upon the expiry of the certificate if it is not re-keyed or re-newed before that date, or once the subordinate CA has been revoked.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The DCA Root G1 CA does not provide a key escrow service. In case the DCA Service permitted generation of a key pair on its own off-line system, the private key material of the subordinate CA shall be entirely, irrevocably and verifiably be transferred to the applicant, and shall not be present on persistent storage on the off-line system. The witnessing of the transfer by knowledgeable experts shall be deemed sufficient to confirm key transfer.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The DCA Root G1 CA is located at Nikhef, Watergraafsmeer, Amsterdam.

The Nikhef building is constructed out of reinforced concrete with brick inner walling.

The off-line CA system is located in a locked room, that uses a key scheme with special-access requirements. Within this locked room, a dedicated locked cabinet contains the safe with the off-line media. The cabinet has a padlock mechanism protecting the two doors, the safe has battery-operated hinges controlled by an independent pin panel. The off-line system, devoid of private key material unless an operator is present, is off-line and permanently placed within the locked cabinet.

The on-line CA repository systems are located in a data centre at Nikhef to which access is controlled via secure RFID and a key scheme with special-access requirements. The on-line CA repository server is hosted on a virtualised environment exclusively dedicated to security sensitive services for certificate authority and trust operations. The host systems are located in a security cabinet within the data centre, with access to the cabinet controlled by number padlocks.

5.1.2 Physical Access

Access to the locked room is limited to Nikhef Computer Technology department systems management (CT) personnel and CA personnel. Access to the cabinet containing the CA off-line system and the safe is restricted to Administrators and Operators of the DCA Service.

Access to the data centre containing the on-line CA system is limited to Nikhef CT personnel. Access to the secured cabinet containing the hosting systems is limited to DCA Service personnel.

5.1.3 Power and Air Conditioning

The off-line CA system is connected to public electricity mains only.

The on-line CA system is located in the high-availability data centre, connected to two independent no-break feeds. Sufficient redundant cooling is available.

5.1.4 Water Exposures

All CA systems are above sea level. Installations that contain water near the CA systems are periodically tested for pressure bearing capabilities. The data centre is equipped with moisture sensors and monitored continuously.

5.1.5 Fire Prevention and Protection

The data centre is equipped with an inert-gas fire extinguishing system and has appropriate smoke-sensitive detectors.

5.1.6 Media Storage

All media containing the private key material of the DCA Root G1 CA are kept in the locked safe near the off-line machine. Copies of private key material are also kept inclusively in locked safes under the control of the DCA Administrator, and to which DCA Operators are granted access.

All other media, except for transfer media, of the DCA Root G1 CA are kept inside the locked cabinets. Transfer media are kept in either the locked cabinet or kept under the control of the DCA Administrators or the applicant.

5.1.7 Waste Disposal

Waste carrying potential confidential information is physically destroyed before being trashed.

5.1.8 Off-site backup

The back-up of the private key of the DCA Root G1 CA is kept off-site in a safe under the direct personal control of a DCA Service Manager.

Other, non-sensitive, material of the DCA Root G1 CA, including the state of the CA, index files, and related material of the off-line CA are regularly transferred to a distinct location within the building but physically distant from the originals.

The on-line repository system is backed-up to two off-site, geographically distinct, locations in the Netherlands.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All roles related to the operation of the DCA Root G1 CA shall be performed by the DCA Service Administrators only. They shall be permanent employees of Nikhef (as conventionally defined within the framework of the Nikhef collaboration).

5.2.2 Number of Persons Required per Task

The Administrators are permitted to act singly, unless elsewhere in this Policy a specific action is required to be performed in the presence of witnesses or another Administrator or operator.

5.2.3 Identification and Authentication for Each Role

Use of media containing the private key of the DCA Root shall be by DCA Administrators only, who will record their identity, full name, and any actions taken in a log book. They will exclusively use the off-line DCA system for connecting media containing the private key.

The DCA Manager will identify the DCA Administrators at least once based on official government photo-identification documents.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

DCA Root G1 CA Administrators shall all be personnel with a sound understanding of PKI, its implementation, and its trust implications. They are experienced in operating CA infrastructures and are knowledgeable about this document and the requirements stipulated herein. The DCA Operators shall all be personnel with a proper understanding of PKI, and trained in following the operational procedures implementing this CP/CPS.

Beyond being employees in good standing, there are no specific clearance requirements.

5.3.2 Background Check Procedures

The background of each additional DCA Administrator shall be assessed by his or her peers.

5.3.3 Training Requirements

The DCA Administrators and Operators will ensure they are capable of fulfilling their tasks.

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

If an authorized action is observed, the DCA Service Administrators will take appropriate measures to prevent re-occurrence, may revoke any privileges, and will correct any inappropriate results. Other sanctions are possible as specified in the terms of employment.

5.3.7 Independent Contractor Requirements

The DCA Root G1 CA shall not employ contractors for its operation. However, it does rely on vendors to supply hardware, software, and other (physical) infrastructure. It will obtain such supplies in a way that does not knowingly expose the DCA Root G1 CA to security compromises.

5.3.8 Documentation Supplied to Personnel

The DCA Root G1 CA Administrators and any operators are given a copy of this document as well as any ancillary documentation.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

The following events will be recorded by the DCA Root G1:

- System boots and shutdowns of the off-line machine
- Certificate application, issuance and revocation
- Key pair generation
- Activation and deactivation of the CAs signing key

5.4.2 Frequency of Processing Log

Audit logs will be analysed

- at the time of any certificate signing - by inspecting the content of the DCA files and logsheets
- during annual audits
- whenever an incident occurs or is suspected

5.4.3 Retention Period for Audit Log

Audit logs are retained for at least three years after the certificate pertaining to the log entry has expired or has been revoked.

5.4.4 Protection of Audit Log

The audit logs are stored in the locked cabinet of the off-line CA system, to which only DCA Service personnel has access.

5.4.5 Audit Log Backup Procedures

All audit logs as recorded on the off-line removable media are periodically copied to other off-line media and stored in a safe. All audit logs of the on-line repository system pertaining to the import of CRLs and subscriber (subordinate CA) certificates are routinely backed-up as per section 5.1.8.

5.4.6 Audit Collection System (internal vs. external)

All audit logs collected by the the DCA Root G1 CA are stored internally.

5.4.7 Notification to Event-causing Subject

The DCA Root G1 is neither required to nor prevented from notifying event-causing subjects.

5.4.8 Vulnerability assessments

Vulnerability of the audit logs are assessed during periodic self-audits and whenever a change to section 5.4 of this CP/CPS is considered.

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

The DCA Root G1 CA will archive the following data:

- All certificate application data, issued certificates, and CRLs
- Any CRLs on which on-line revocation status information is based
- User operations on the on-line and off-line CA systems, including startup, reboot, and login actions
- Any documentary evidence and witness reports of key generation ceremonies, key transfer and certificate acceptance
- Sufficient information to verify the validation of organisation and individual identities

5.5.2 Retention Period for Archive

Records will be kept for at least three years following the expiration or revocation of the certificates to which they pertain.

5.5.3 Protection of Archive

The archive is stored in the locked off-line CA cabinet and on the off-line secure media in a safe. Where not contrary to the off-line requirements, records will be backed up to other on-line and tape archives in geographically distinct locations.

The records are accessible by DCA Service personnel. Off-site backup copies of non-sensitive material from the on-line repository system are managed confidentially under contract by the backup service providers of Nikhef.

5.5.4 Archive Backup Procedures

All off-line electronic records are backed up on removable media and stored in the safe. Archives may be bundled and stored on distinct media, after which the rolling archive on operational media is re-set.

5.5.5 Requirements for Time-stamping of Records

Records are dated and timestamped by using reasonably accurate clocks, periodically synchronised by the DCA Service personnel. Clocks will be adjusted before issuance of CRLs and certificates. Its uncertainly will not be more than 5 minutes.

For on-line systems, these will be synchronised frequently using the ntp protocol from trusted time sources operated by Nikhef, SURFnet, and/or a distributed NTP pool.

5.5.6 Archive Collection System (internal or external)

All archives are collected internally or stored on services under contract of Nikhef.

5.5.7 Procedures to Obtain and Verify Archive Information

Information from the archive may be inspected by auditors. In addition, subscribers or third parties may request the DCA Root CA for permission to inspect or obtain information from the archives if such – at the discretion of the DCA Root CA – is pertinent to the proper operation and trust of the DCA Root CA. The DCA Service may require prior compensation for reasonable costs associated with such requests.

At all times, individuals shall have the right to inspect, and in case of omissions, errors or inconsistencies, have the right to amend and correct data regarding themselves.

5.6 KEY CHANGEOVER

The DCA Root G1 CA key pair shall be changed once the maximum validity period of 30 years expires or when the cryptographic data on which it is based is no longer considered appropriate to protect the certificates it issues. It may change key material at any time prior to these conditions.

If the DCA Root G1 CA key changes, the overlap between the old and the new key pair shall be at least 400 days. From the time of the key changeover, only the new key will be used to sign certificates.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

In the event of an incident which compromises the integrity of the DCA Root G1 CA, the DCA personnel shall initiate an incident analysis immediately. Further steps to be undertaken will depend on the outcome of the analysis.

5.7.2 Computing Resources, Software, and/or Data are corrupted

The DCA will take all reasonable precautions to enable recovery. In order to be able to resume operation, the following measures are implemented:

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

If any part of the running system is corrupted, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a read-only medium and estimated to be uncorrupted. Unless in the exceptional case that all copies of the DCA Root G1 private key have been destroyed or lost, and as long as these are not compromised, the operation shall be re-established as soon as possible. This will not constitute a need to revoke any issued certificates.

5.7.3 Entity Private Key Compromise Procedures

In the event of private key compromise of its own key, the DCA Root G1 shall immediately cease issuing certificates and request revocation of any cross-signed certificates. It shall also forthwith inform all its subscribers, and all bodies to which it has been accredited. Circumstances that led to the compromise will then be fixed and eliminated, and these remedial actions documented. A new key and certificate for the CA may then be re-created and operations restarted with a certificate based on a new key pair, and with a new subjectName.

In case a key of a subscriber (subordinate CA) certificate has been compromised, the DCA Root G1 CA will revoke the corresponding certificate and will not accept new certificate applications from this entity until the incident has been satisfactorily closed. Subscribers will also be informed of this incident.

5.7.4 Business Continuity Capabilities after a Disaster

Following a disaster, the DCA Administrators and/or Manager will – as soon as reasonably practical – assess the extent of the disaster and its impact on the operational of the DCA Service. Having established that no compromise has occurred and that sufficient elements are available to recover from the disaster, it shall proceed to re-establish operations, if so needed from back-up media.

When it is deemed likely that the disaster will result in long-term outage for a period over 30 days, the DCA may opt to suspend operations by informing its subscribers and any bodies to which it has been accredited.

5.8 CA or RA TERMINATION

Upon termination of service of the DCA Root CA, the DCA Managers will

1. Inform all bodies to which it has been accredited at least three months before the actual termination
2. Inform all subscribers at least three months before the actual termination
3. Announce termination on DCA repository website.
4. Terminate the issuance and distribution of certificates and CRLs following a reasonable grace period.
5. Archive all relevant information in accordance with section 5.5
6. Revoke all certificates.
7. Notify relevant security contacts.
8. Destroy all copies of private keys.
9. Notify as widely as possible the end of the service.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The DCA Root CA shall generate and store its private keys in an off-line system which is stored in a locked cabinet in accordance with section 5.1.

The DCA Root CA key pair generation shall be performed with a recent trustworthy version of the OpenSSL software which has been verified for integrity with its source. The generation will be witnessed by experts knowledgeable about PKI, and they shall witness that the private key pair material is stored on removable media and not further distributed beyond the reach of the DCA Administrators and Manager. The DCA Manager may transport the generated private key and any other DCA Root materials without further supervision to a safe at a geographically separate location under the direct personal control of the CA Manager. The DCA Root CA shall not proceed to include its self-signed certificate in external trust anchor distributions until the DCA Manager confirms that the private key material has been deposited in said safe.

6.1.2 Private Key Delivery to Subscriber

The DCA Root CA does not generate key pairs for its subscribers (subordinate CAs). It will permit at its discretion the generation of key material by the subscriber by use of the DCA off-line system, but only on applicant-provided media.

Where the subscriber is a subordinate CA operated by the DCA Service, the off-line media of the DCA Root CA and such subordinate CAs may be stored in the same safe.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber's public key is delivered to the CA in the form of a PKCS#10 request.

6.1.4 CA Public Key Delivery to Relying Parties

The public keys of the DCA Root CA can be downloaded in the form of an X.509 certificate from the on-line repository.

6.1.5 Key sizes

The signing key of the DCA Root CA shall be an RSA key and shall be 4096 bits long.

6.1.6 Public Key Parameters Generation and Quality Checking

The DCA Root CA will refuse to certify public keys not matching its quality requirements.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

DCA Root CA keys may be used for certificate signing and for CRL signing.

Subscriber (subordinate CA) keys may be used for certificate signing and for CRL signing.

6.2 PRIVATE KEY PROTECTIONS AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The DCA Root G1 CA is an off-line CA that does not use a separate cryptographic module. Key material is stored in files on removable media in encrypted form, under conditions described in

sections 5.1.6 and 5.1.8. The key shall never be stored in an unencrypted form. The removable media shall never be connected to a machine that is or has been connected to a network.

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

There is no requirement for any role to be performed in the presence of more than one person.

6.2.3 Private Key Escrow

The DCA Root CA does not escrow any keys.

6.2.4 Private Key Backup

The DCA Root CA private key is backed up on multiple removable media, stored in geographically separated locations.

6.2.5 Private Key Archival

The private key is not archived beyond its active use or post the termination of the CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The DCA Root CA does not employ a separate cryptographic module. Key material is stored as described in section 6.2.1.

6.2.7 Private Key Storage on Cryptographic Module

The DCA Root G1 CA does not employ a separate cryptographic module. Key material is stored as described in section 6.2.1.

6.2.8 Method of Activating Private Key

The private key of the DCA Root G1 CA is activated by a pass phrase of at least 15 characters, which meets the best practices for choosing good pass phrases.

6.2.9 Method of Deactivating Private Key

The private key is de-activated by removing the pass phrase from memory in the off-line machine and powering down of the off-line system memory for at least 10 seconds.

6.2.10 Method of Destroying Private Key

Following termination of CA operations, all copies of the private key will be securely destroyed according to then-current best practice for the destruction of sensitive materials.

6.2.11 Cryptographic Module Rating

Not applicable: the DCA Root G1 CA does not employ a separate cryptographic module.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The DCA Root CA archives all issued certificates including the DCA Root self-signed certificate on the off-line system as well as on removable storage media kept in a secure place. The DCA Root public key and the public keys of subscribers are also published in the on-line repository, and periodically backed-up to off-site locations as per section 5.1.8.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The DCA Root CA's certificate shall have a validity period of no longer than 20 years.

The certificates issued by the DCA Root CA shall have a validity period of no longer than 20 years, and for no longer than the issuing DCA Root CA certificate itself is valid. The usage period of the associated key pairs shall be no longer than 30 years for the DCA Root CA and 20 years for any key pairs of subscribers (subordinate CAs).

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The DCA Root G1 CA does not generate activation data for its subscribers (subordinate CAs).

Subscriber to the DCA Root CA must generate their key pair:

- On a software device or media, with a secure pass phrase acting as activation data of at least 20 characters;
- On a FIPS-140 level 3 hardware device, protected with a pin of at least 15 elements
- On both of these, e.g. in case of an external key generation ceremony, where the activation pass phrase for the key stored on a software device is at least 20 characters, and where it is protected with a pin of at least 15 elements when imported in a FIPS-140 level 3 device or a FIPS-140 level 2 device with additional security controls protecting against physical removal of the hardware device.

The pass phrase used to activate the DCA Root CA private key is generated on the off-line machine and will have a minimum length of 32 characters.

6.4.2 Activation Data Protection

Each subscriber is responsible to protect the activation data for the its own private key.

The DCA Root CA uses a pass phrase to activate its private key which is

- only ever entered on the off-line machine,
- known exclusively to DCA Managers and DCA Administrators, who for the DCA Root CA are the only Operators,
- is never stored in the same cabinet or safe as the private key itself,
- may be distributed on paper as long as these are kept in sealed, tamper-evident containers (envelopes), away from the key material, at distinct, widely separated geographical locations (at least 10 km), and in locked cabinets.

Old activation data is destroyed according to current best practices.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The off-line system is maintained at a high level of security by applying all patches relevant to an off-line system. It is kept within a controlled area and never connected to any network, either during installations, configuration, or operation. Patches are transferred using external media.

The on-line repository system environment, as well as any hosting platform on which the on-line repository system is running, is maintained at a high-level of security by timely application of all relevant patches. The on-line system is a virtual system, hosted in a redundant virtualisation environment that itself exclusively contains security-sensitive services at the same or higher level than the DCA Service on-line repository. The virtualisation environment is controlled and managed by DCA Service Administrators.

Furthermore:

1. Any software change is monitored and dealt with by the DCA Administrators.

2. System and service configuration is reduced to the bare minimum needed to provide the service in the necessary quality and availability.

6.5.2 Computer Security Rating

The systems and environment do not have a security rating.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Necessary systems development will be performed on separate systems. Beyond the certificate manipulation software[1] no specific software is employed.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The DCA Root CA off-line system does not have a network.

The DCA Service on-line repository is on a dedicated network segment containing only managed services dedicated to security and trust operations. The systems are protected by network-switch level and host-level packet filters permitting traffic to only intended ports. Management access to these systems shall be limited to such network endpoints that are the minimal necessary for DCA Administrators to access the system, and will not be possible from outside Nikhef without further network authentication steps.

6.8 TIME-STAMPING

Time stamping of certificates will be done based on the internal system clock, which is synchronised with external clocks borne by DCA Administrators before performing CRL and certificate signing operations.

[1] OpenSSL (www.openssl.org) is employed – interaction to this is via explicit commands and scripted command sequences.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

All certificates shall be formatted as X.509 version 3 certificates.

7.1.2 Certificate Extensions

The CA certificate of the DCA Root CA shall have the following extensions:

Basic Constraints	Critical, CA:True
Key Usage	Critical, Certificate Sign, CRL Sign
Subject Key Identifier	keyid:*identifier*
Certificate Policies	Policy: 1.3.6.1.3.1.10434.4.2.7.1.1

The certificates issued to subscribers (subordinate CAs) shall have the following extensions:

Basic Constraints	Critical, CA:True
Key Usage	Critical, Certificate Sign, CRL Sign
Subject Key Identifier	*The keyID identifier of the subscribers public key*
Authority Key Identifier	keyid:*identifier*
CRL Distribution Points	Full Name: URI:http://crl.dutchgrid.nl/dcaroot/g1/crl/crl.crl
Certificate Policies	Policy: 1.3.6.1.3.1.10434.4.2.7.1.1

where the *identifier* shall be composed of the 160-bit SHA-1 hash of the value of the BIT STRING containing the pertinent public key (excluding the tag, length, and number of unused bits) as per option 1 of section 4.2.1.2 of RFC 5280.

7.1.3 Algorithm Object Identifiers

The appropriate object identifiers shall be included in the certificates.

For the DCA Root CA, these shall be id-sha256 (1.3.14.3.2.26), rsaEncryption (1.2.840.113549.1.1.1), and sha256WithRSAEncryption (1.2.840.113549.1.1.5).

7.1.4 Name Forms

The subject and issuer names of the DCA Root CA certificate shall be the ordered sequence of sets of size one, comprising

domainComponent (DC)	IA5String	nl
domainComponent (DC)	IA5String	dutchgrid
organisationName (O)	PrintableString	Certification Authorities
commonName (CN)	PrintableString	DCA Root G1 CA

Subsequent generations of the DCS Root CA shall carry an G2, G3, etc instead of G1.

The subject name of subscribers shall be one of the following sequences of sets of size one:

domainComponent (DC)	IA5String	nl
domainComponent (DC)	IA5String	dutchgrid

organisationName (O)	PrintableString	Certification Authorities
commonName (CN)	PrintableString	*name of the subordinate CA as per section 3.1*

or

domainComponent (DC)	IA5String	eu
domainComponent (DC)	IA5String	rcauth
organisationName (O)	PrintableString	Certification Authorities
commonName (CN)	PrintableString	*name of the subordinate CA as per section 3.1*

or

country (C)	PrintableString	NL
organisationName (O)	PrintableString	NIKHEF
commonName (CN)	PrintableString	NIKHEF medium-security certification auth

and where the list of permissible subscriber subjectNames may in the future be extended by amending this CP/CPS according to the provisions of section 1.5.

7.1.5 Name Constraints

The DCA Root CA does not include name constraints in its issued certificates.

7.1.6 Certificate Policy Object Identifier

Issued certificates may contain the object identifier of the DCA Root CA policy under which they are issued.

7.1.7 Usage of Policy Constraints extension

The DCA Root CA does not include a policy constraints extension in its issued certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

The DCA Root CA does not include a policy qualifier in its issued certificates.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The DCA Root CA does not include a critical policy extension in its issued certificates.

7.2 CRL PROFILE

7.2.1 Version Number(s)

The DCA Root CA issues X.509 version 2 CRLs compliant with RFC5280.

7.2.2 CRL and CRL Entry Extensions

The DCA Root CA issues CRLs using the SHA-256-with-RSA-encryption signature algorithm. It includes the CRL number extension, which will be monotonically increasing.

7.3 OCSP PROFILE

The DCA Root CA does not operate an authoritative OCSP service.

7.3.1 Version Number(s)

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8 COMPLIANCE, AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The DCA Root CA will ensure that all its procedures and processes are carried out in compliance with the provisions of this CP/CPS. To this end, it shall at least once a year perform a self-assessment to check the compliance of the operation with the CP/CPS document in effect, and effectuate a review of staff.

The DCA Root CA accepts to be audited by qualified external peers, by bodies to which is has been accredited, and by qualified relying parties in order to verify its compliance with the rules and procedures prescribed herein. Any costs associated with such audit must be covered by the requesting party.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The assessor must be a knowledge expert in the domain of assessing public key infrastructures for research and scholarly purposes.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

No stipulations.

8.4 TOPICS COVERED BY ASSESSMENT

An audit may verify that the services provided by the CA comply with the version of the CP/CPS currently in force.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In the event of a deficiency, the DCA Service will communicate the steps that will be taken to remedy the deficiency, including relevant time lines. If a discovered deficiency has direct consequences on the reliability of the certification process, or if certificates are likely to have been affected by the deficiency they will be revoked with immediate effect.

8.6 COMMUNICATION OF RESULTS

Results on any assessment are maintained in confidence between the assessor, the audit requesting party or parties, and the DCA Service. Results will be disclosed to any bodies to which the DCA Root CA has been accredited. Results may be disclosed to other parties when so agreed to by the DCA Service Manager.

Revocation of certificates that is an effect of an identified deficiency are communicated via the CRL.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No fees are charged for certificate issuance or renewal.

9.1.2 Certificate Access Fees

No fees are charged for access to certificates.

9.1.3 Revocation or Status Information Access Fees

No fees are charged for access to certificate status information or CRLs.

9.1.4 Fees for Other Services

A reasonable reimbursement of costs may be charged for other services.

9.1.5 Refund Policy

There shall be no refunds.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Nikhef does not accept any financial responsibility for the use or failure to use any of the certification services, or of any information provided by, on behalf of, or by way of the DCA Service.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

Neither Nikhef nor the DCA Service as such provides any insurance or warranty for end-entities and subscribers, of whatever type. Reliance on DCA Service material and services is at your own sole risk.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The DCA Root CA, in its validation of individual and organisational identity, will collect personal data about subscribers. This data collection is subject to the Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens). The subscriber acknowledges that the stated data is being collected by the CA and permits storage of any such data in the secure repository intended in section 5 according to the stipulations made therein.

Apart from the published certificates, certificate revocation lists, and the information on the on-line repository, the DCA Root CA considers all data confidential.

9.3.2 Information not within the Scope of Confidential Information

Information included in certificates and CRLs shall not be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

The DCA Service shall not disclose confidential information unless so specified in this policy (to auditors and assessors), unless to its DCA Managers, Administrators and Operators, and unless required by law or regulation.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The DCA Service will keep a minimal amount of personal information, solely sufficient to ensure that the same identifier is not re-assigned to a different entity. It will process personal data in accordance with Dutch Law.

The DCA Root CA issues certificates to subordinate CAs, so that its subscribers are solely organisations and organisational entities. It collect information about the representatives of its subscriber and applicant organisations in order to establish their relationship with the organisation, and to ensure that there is a chain of documentary evidence as to the issuance of any certificates. It will not collect more personal information than:

- the information recorded as per section 3.2.3;
- the communications identifiers (email addresses, telephone numbers, internet protocol addresses, and any user agent information if so supplied by the applicant) that have been used to complete the validation as per section 3.2.3.

Data owners can request access to information regarding all their data at any time, and all reasonable requests to correct and/or amend the data will be processed promptly. Due to the nature of the service, it has a legitimate interest in recording the information recorded as per section 3.2.3 for as long as the certificate is valid plus the audit log retention period.

9.4.2 Information Treated as Private

Any information not explicitly made public is treated as private information. The DCA Service protects private information using appropriate safeguards and an appropriate degree of care.

9.4.3 Information not Deemed Private

The following information collected by the DCA Root CA is deemed not to be private:

1. subscriber's organisation email address
2. subscriber's organisation name
3. subscriber's certificate

9.4.4 Responsibility to Protect Private Information

The DCA Service is responsible for protecting private information as stipulated in this policy.

9.4.5 Notice and Consent to Use Private Information

Whenever private information is leaked or destroyed in a way that significantly impacts a person, it will be so communicated to the person involved.

Unless prohibited by Law, the novel use of private information will be communicated to the impacted person without undue delay.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The DCA Service and/or Nikhef may be forced to disclose confidential information to law enforcement agencies in the Netherlands.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The DCA Service does not claim Intellectual Property Rights on issued certificates or CRLs.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

Except as stated in this CP/CPS or in a separate agreement with Nikhef and the DCA Service, neither Nikhef, nor any of the Nikhef parties, nor the DCA Service, nor any DCA Service Managers, Administrators or Operators make any representations regarding its services.

The DCA Service represents to the extent specified in this CP/CPS that it

- complies with this CP/CPS;
- the certificates issued by the DCA Root CA will be issued solely in compliance with this CP/CPS;
- it will maintain an on-line accessible repository containing the published information with an intended continuous availability.

9.6.2 RA Representations and Warranties

The DCA Root G1 CA Managers and Administrators, being the RAs, represent that the RA will act in accordance with the provisions in this CP/CPS.

9.6.3 Subscriber Representations and Warranties

Subscribers are responsible for any representations and warranties made by them to the DCA Service, their relying parties, and any other third parties, and for any actions that use the private key of the subscriber, regardless whether such use was authorized, for as long as the certificate is valid and for as long as a CRL including revocation information for this certificate has not been published.

The subscriber represents to the DCA Service and third parties that it will act in accordance with all the provisions in this CP/CPS document; inform without undue delay the DCA Root CA of any material changes that pertain to the certificate or the information contained therein; use the certificate only for lawful purposes; and that it will cease using the certificate if so instructed by the DCA Root CA. The subscriber will inform the DCA Root CA Managers of any material changes of its CP/CPS, and agrees such changes will only take effect following endorsement by the DCA Root CA Managers.

Subscribers represent and warrant that certificates are only used for purposes compatible with section 1.4.

9.6.4 Relying Party Representations and Warranties

Each relying party represents that, before relying on any certificate of the DCA Root CA, it shall have read, understood, and act in compliance with this CP/CPS, that it has appropriate knowledge of PKI and appropriate technical implementations to validate certificates issued by the DCA Root CA, and that it shall have obtained the up-to-date certificate status information as published by the DCA Root CA and act in accordance therewith.

Each relying party shall represent that it bear the sole responsibility for reliance on any certificate issued by the DCA Root CA, any such reliance it at its own risk, and that it has thereto executed an appropriate risk assessment.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

All certificates and any related materials, software, publications, and service are provided 'as-is' and 'as available', without any warranties. To the maximum extent permitted by law, the DCA Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, and all others involved in the DCA Service disclaim all express and implies warranties and liabilities, including all warranties of merchantability, fitness for a particular purpose, and non-infringement. Neither the DCA Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, not any others involved in the DCA Service warrant that any service, product, certificate or other artefact will meet any expectations or that access to certificates will be timely or error-free, or that it is available at any time. The DCA Root G1 CA and the DCA Service may discontinue any service at any time following the provisions of section 5.8.

9.8 LIMITATIONS OF LIABILITY

The DCA Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, and all others involved in the DCA Service decline any liability for damages incurred by any subscriber, relying party, or third party relying on the certificates or information issued or published by the DCA Root CA or DCA Service. It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the DCA Root CA.

9.9 INDEMNITIES

To the extent permitted by law, each subscriber and relying party shall indemnify the DCA Service, Nikhef, Nikhef partners, SURF, and all others involved in the DCA Service, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the subscriber's or relying party's (i) breach of this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP/CPS and any amendments are effective when published in the on-line repository as per the date there stated, and will remain in effect until replaced with a newer version or withdrawn.

9.10.2 Termination

This CP/CPS will remain in effect until replaced with a newer version or withdrawn.

9.10.3 Effect of Termination and Survival

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

All conditions related to retention of data and audit logs, and all conditions related to the protection of personal information will survive the termination of the DCA Root CA.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Individuals can communicate with the DCA Root CA using the information provided in section 2.2.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

This CP/CPS is reviewed annually at the time of the self-audit. Amendments are made by posting an updated version of the CP/CPS to the on-line repository.

9.12.2 Notification Mechanism and Period

The DCA Service will post changes to this CP/CPS in its on-line repository. It will inform any bodies to which it has been accredited and that request prior notification for changes to the CP/CPS in a timely fashion in accordance with the provisions of section 1.1.5 before the new CP/CPS becomes effective.

9.12.3 Circumstances Under which OID Must be Changed

Material changes to the CP/CPS, such as to be determined by the DCA Service Manager, will cause the OID as listed in section 1.2 and asserted as described in section 7.1.6 to change.

9.13 DISPUTE RESOLUTION PROVISIONS

Parties are required to notify and communicate with the DCA Service Manager and/or Administrators, and attempt to resolve disputes directly before resorting to any dispute resolution mechanism.

9.14 GOVERNING LAW

The interpretation, construction, and validity of this policy shall be governed by the laws of the Kingdom of the Netherlands.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP/CPS is subject to all applicable laws and regulations.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

This CP/CPS constitutes the entire agreement between the DCA Service and the DCA Root CA and any other party, unless a more specific agreement is in place. If such an agreement has provisions that differ from this CPS, the more specific agreement takes precedence, but only with respect to that party. No others may rely on such a more specific agreement, or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CP/CPS may not re-assign their rights or obligations without consent of the DCA Service Managers.

9.16.3 Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of this CP/CPS will remain valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The DCA Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, and all others involved in the DCA Service may seek indemnification and attorney's fees from a party for any damages, losses, or expenses related to that party's conduct.

9.16.5 Force Majeure

The DCA Service is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond the DCA Service' or Nikhef's reasonable control.

9.17 OTHER PROVISIONS

No stipulation.