# 1 Privacy Policy

The Legacy Medium-Security DutchGrid CA (MSDCA) Service will keep a minimal amount of personal information, compatible with the goals of the service.

## *1.1 Goal of the information processing*

The goal of the MSDCA data processing is to provide a service that issues unique, long-term, non-reassigned identity assertions to its subscribers, their explicitly authorized (software) agents, and networked services for the purpose of access control to and secure operation and management of academic and research distributed digital infrastructures.

All personal data processed by the MSDCA is a result of an explicit, user-initiated request, to which the user is a conscious and informed participant. The MSDCA does not collect in any way or form information about the user without that user having initiated a request for service to the MSDCA.

Besides this processing for delivering the certificate service, the MSDCA Service will store user information in log files and audit archives. These logs and audit records are used solely for administrative, operational, monitoring, security, and dispute resolution purposes of the MSDCA service. It may be shared for security incident response purposes with other authorised participants in the academic and research distributed digital infrastructures via secured mechanisms, only for the same purposes and only as far as necessary to provide the incident response capability.

## *1.2 User consent*

Before authenticating the applicant, the service will inform the user regarding the goal of the service and give the applicant the choice to continue or abort the authentication. The information will describe the types of personal data that will be processed, the fact that this information may be shared with other authorised participants as stated in section 9.4.1.1, and contain a reference to the Certification Policy and Practice Statement which indicated how such data will be processed.

The user will submit information either on paper, or by submitting a signing request containing the full name and current professional affiliation and email address of the user via a web form on which the user is explicitly asked to consent to the processing, or via actively sending an email with this information to the submission address.

The user will be informed when a certificate is requested, and can at that point object to the processing of the data. By continuing the certificate request process, the user agrees to the processing for the goals stated above.

## *1.3 What information will be processed and stored*

The following information will be processed:

- The name (given and family name) of the user
- A business electronic mail address of the user
- The professional affiliation of the user, for the purpose of embedding it in the certificate and for the security logs and audit records
- Business contact information for the user, including postal address and telephone number
- The name of the identity verifier (Registration authority) who verified likeness of the applicant based on photo-ID documents
- The serial number of the photo-ID document. The last four digits will be stored in an electronic archive, the full number will be stored only in a paper-based record system for dispute resolution and incident response.

The following generated information will be stored:

- The issued certificates, containing the name of the user and the initial professional affiliation
- In the security audit logs, the certificate subject name including the information listed above
- Any interactions between with the MSDCA email service and the MSDCA web site, during which will be stored
    - for all users: the internet protocol address, user agent (browser) identification, and time of interaction
    - in addition for applicants: the applicants full name, email address, and affiliation

## *1.4 Where will the information be processed*

The information is processed by the MSDCA Service at Nikhef, Amsterdam, The Netherlands, in a secured room to which access is controlled and limited to designated personnel, and in a locked area to which only staff of the MSDCA have access. Electronic information is stored in on systems in a designated secure cabinet to which access is limited to Nikhef and MSDCA security personnel and MSDCA operations staff, hosted on systems dedicated to hosting security functions only. These conditions are further described in the MSDCA CP/CPS section 5.1. Backups of data are stored under a confidentiality agreement by the contracted backup service provider.

## *1.5 Who may receive the information*

The information is received and processed by the MSDCA service, and the DCA Managers, Administrators and Operators responsible for this service.

### 1.5.1 Certificate data is considered public

Certificates and the information contained therein (name, initial affiliation, and – when so requested by the user – the email address) will be disclosed, the users having been so informed. In the course of the users work, such information will inherently be disclosed as part of the security (TLS) handshake protocol and thus is not usually protected. This same information is made available publicly through a search interface on the MSDCA web site.

### 1.5.2 Security Incident Response and audit data

The MSDCA provides authentication services that are an important element in the protection of integrity, availability and security of the international distributed digital infrastructures. For incident response purposes, besides any public information contained in the certificate, contact information of the organisational affiliation and those auditable events that are minimally necessary to conduct the investigation of a (suspected) security incident may be shared such purposes with other authorised participants in the academic and research distributed digital infrastructures via secured mechanisms, only for the same purpose, and only as far as necessary to provide the incident response capability.

Information may be shared with law enforcement if the MSDCA, the DCA Service, Nikhef, or the Foundation NWO-I is so required by Dutch law.

## *1.6 User information and transparency*

The user is informed about her or his data that is processed by the service via this privacy policy, a link to which will be presented to the user each time a certificate is requested, and a link to which will be posted on the MSDCA public repository.

For more information the user is referred to this comprehensive policy and practice statement at https://ca.dutchgrid.nl/medium/policy/.

Users 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, the MSDCA service has a legitimate interest in recording the information recorded for as long as the certificate is valid plus the audit log retention period, solely for the purposes of dispute resolution and security incident response.

## 1.7 Protection of personal data

The personal data is protected in accordance with the MSDCA CP/CPS, specifically sections 5.1 and 5.2. Specifically the data is exclusively processed on

- The CA front-end web server and the registration web server, both of which are maintained at a high level of security and behind a double firewall both at the edge of the network and on the system itself, and where the software is maintained in accordance with best practices for vulnerability management and patching. It will run a minimal set of services. Operational management access is via secure, encrypted and authenticated means only, and only from selected networks to which DCA service personnel have access.
  These systems are contained in a dedicated locked cabinet in a secure data centre to which access is individually controlled.
  The front-end web server contains the public certificate information of all issued certificates. The separate registration web server contains data about all auditable on-line events, the information on the applicant verification process, and the last four digits of the serial number of the photo-ID for users.
- The off-line CA issuance system, which is contained in a separate locked room in a dedicated locked cabinet to which only DCA operational staff have access. This locked cabinet contains the paper registration forms for all users including organisational contact information and telephone numbers, the signature of the user and the serial number of the photo-ID document used.
- The on-site disk back service, which is only accessible over a network from designated systems within Nikhef designated for secure system management operations, or through a VPN tunnel to which users authenticate with individual credentials, and to which only specifically authorized systems management personnel of Nikhef and the DCA service have access. This system is contained in a secure data centre to which access is individually controlled.
- The off-site redundant tape backup service, which is managed under contract in the Netherlands, to which only authorized service personnel have access, and which is located in a vault inside a secure data centre where access is individually controlled.

All software is kept up to date and vulnerabilities in the software are patched promptly. Databases containing personal data are not accessible from outside the system.

The specific data protection measures are disclosed and discussed with accrediting bodies and qualified relying parties. Incidents involving personal data shall be pro-actively disclosed with the active users of the service, based on the communications information available at that time.

## 1.8 Information retention periods

The information that is stored will be retained for the following periods:

- issued certificates, including the information contained therein, are stored for an indefinite period to enforce persistent uniqueness.
- data regarding auditable events are removed 3 years after the validity of the last certificate based on this user subject name has expired.

The information in the archive is accessible only to the DCA Administrators and will be used exclusively for dispute resolution and security incident response purposes.

In addition to the above, backups of all data are stored – under confidentiality agreements and only for the purpose of security investigations and data recovery– for a period of 90 days.