DutchGrid (Legacy) CA

DutchGrid and Nikhef Medium-Security X.509 Certification Authority

Privacy Policy and Transparency

The goal of the *Medium-Security (Legacy) DutchGrid CA* 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 global academic and research distributed digital infrastructures.

1.1 Identity and contact details of the controller

The service is operated by the Physics Data Processing group at Nikhef, the Dutch National Institute for Sub-atomic Physics, Science Park 105, NL 1098 XG Amsterdam, The Netherlands.

You can directly contact the service operators at Nikhef via email at ca@dutchgrid.nl, or by phone at +31 20 592 2000.

1.2 Purposes and legal basis for the processing

In order to provide the service of issuing persistent, non-reassigned identifiers to its subscribers, the *Medium-Security (Legacy) DutchGrid CA (MSDCA)* service needs to keep a record of personal information, both the data returned to the user in the credential, as well as enough information to reliably re-establish the identity of the user at a later date when re-issuance of a new credential to the same user (with the same name) is needed.

The MSDCA service processes data necessary for

- the performance of a contract (based on art. 6.1(b) of the GDPR) for the information contained in the issued credential: name, professional affiliation, the public part of your cryptographic key
- the purposes of the legitimate interests pursued by the service (based on art. 6.1(f) of the GDPR) for other information (see below) that we collect: for protecting the integrity of the service itself, and for response to security incidents supporting secure operation and management of global academic and research distributed digital infrastructures.

1.2.1 Why we collect the information we do ('balancing test')

The service you're using is about assigning something unique (a credential subject name) to you, the subscriber of the service, and about the ability of re-assigning the name only and exclusively to you again – and not to anybody else. A secondary aim is to support response to security incidents in which your credential has been abused (e.g. because the password you used to protect your own secret key has been compromised).

The following information will be collected from you and processed:

- The name (given and family name) of the user
- A business electronic mail address of the user, optionally - at the user's free request - embedding it in the issued certificate
- 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 (to contact you in case of an enquiry or an incident involving your credential)
- 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 'public' part of your credential keys, which we will digitally sign in the certificate
- Your hand-written signature (and if you are a registration authority, we use that to verify that it's you who verified the information on the paper user registration form)

The following generated information will also 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

Since it's the purpose of the service to issue persistent, non-reassigned credentials to users, and to ensure the integrity (security) of the infrastructures in which these are used, the above is precisely the minimal information we need to collect to provide you the service: with this information, we can contact you, the user, in case of issues with your credential. If you let your credential renewal lapse, based on the information above (contact information, your signature, and some digits of the serial number of your photo-ID) we can at a later time confirm you are actually the original assignee of the name.

Similarly, the credentials issued to you are important to protect the security (integrity, accountability) supporting secure operation and management of global academic and research distributed digital infrastructures. This security support, involving wherever possible contacting you as the user in case your credential is abused in such an infrastructure, is a vital element of the digital research infrastructure – as you would expect from a personal credential. What we collect is necessary to contact you, and in case of severe incidents, retain just enough information for official authorities to trace you based on the serial number of the photo-ID in case your contact details are no longer current.

In the course of your use of the credential, you will yourself on a continuous basis expose your credential subject name (your name, professional affiliation, and public key) to the parties with which you will communicate. Remember that by nature (because of the technical protocol), such authentications reveal this data usually in clear text.

Taking all the above into account, we conclude that the processing of the above data has limited impact on your interests and rights, and is just sufficient to address the legitimate interests to protect the service and the global academic and research distributed digital infrastructures that rely on this service from harmful security incidents.

1.2.2 Personal data are collected from the data subject

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, nor do we obtain personal data from anyone else.

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, and only where these other parties guarantee similar confidentiality of data.

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 (this document) will describe the types of personal data that will be processed, the fact that this information may be shared with other authorised participants, and contain a reference to the Certification Policy and Practice Statement which indicates in more detail how such data will be processed (http://ca.dutchgrid.nl/medium/policy/).

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.

Note that the MSDCA reserves the right to refuse service (and thus to accept inbound personal data) from applicants that do not qualify for using the service. In particular, the service is not available to consumers, being natural persons not acting in a professional capacity or in the context of business (in this case being research and scholarship).

1.3 Categories of personal data concerned

We collect the information listed above in 1.2.1.

1.4 Recipients (or categories of recipients) of the personal data

The data contained in the credential (certificate) – basically only name and affiliation - we issue to you we:

- give directly back to you (by email). In the course of your use of the credential, the information contained therein will inherently be disclosed as part of the security (TLS) handshake protocol and thus is not usually protected.
- allow to be searched for on a web page – so you can retrieve it later, and others can collect that public data to be able to send you encrypted communications

The MSDCA provides authentication services that are an important element in the protection of integrity, availability and security of the international distributed digital infrastructures. Thus, the other data – email address, contact details, signatures, interaction and 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.

Such transfer only happens if the recipients commit to maintain confidentiality of that data and use it exclusively for purposes of security response and dispute resolution. Unless it is detrimental to the conduct of the specific security incident response, we will first inform you, the user, of such a transfer. We cannot prevent the transfer of data to law enforcement if they present us with a valid order to do so.

Obviously, we never sell your data to anyone else.

1.5 Details of transfers to third countries and safeguards

The data in the credential (certificate) which is issues to you will implicitly be exposed by you yourself if you use that credential to authenticate to another party (service, some web site, &c). These may be anywhere on the Internet, within Europe or outside. You are yourself responsible for such actions.

For security incident response for the service itself and for the global academic and research distributed digital infrastructures that rely on the issued credentials for their own security, data about you may be transferred to third countries. Such transfer only happens if the recipients commit (e.g. by adherence to a commonly agreed community standard, policy set, or code of conduct) to maintain confidentiality of that data and use it exclusively for purposes of security response and dispute resolution. Unless it is detrimental to the conduct of the specific security incident response, we will first inform you, the user, of such a transfer.

1.6 Storage period

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 that are not also contained in the issued certificate are removed 3 years after the validity of the last certificate based on this user subject name has expired.
- data regarding registration authorities (their signature and contact details) are retained for as long as there are valid credential for which this data has been used for verification

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.

1.7 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.

1.8 Rights of the Data Subject

Users can request access to information regarding all their data at any time, and all reasonable requests to correct, rectify, and/or amend the data will be processed promptly, and we will promptly answer to requests for restriction or objections to processing.

You can also request erasure of your data. In those cases, your credential will no longer be made available through the search mechanism. Due to the nature of the service, the MSDCA service claims a continuing a legitimate interest in recording the audit data 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.

You have a right to data portability, and all data pursuant to 6(1)(b) (the certificate itself) is immediately and directly released to you. On request, we will also send a copy of your audit trail (the electronic archive) and registration data to you; its format is a set of plain-text files.

1.8.1 Right to objection to processing

You have the right to object – on grounds relating to your particular situation – at any time to processing of your personal data, if you do not agree with the considerations on legitimate interest as described in the balancing test above (in section 1.2.1), or for the establishment, exercise or defence of legal claims.

We do not process your data for direct marketing or profiling purposes of any kind.

1.9 Consent

This processing is not based on consent. Yet we hope that with this transparency statement we give you enough information to make an informed choice about using the service. Note that there are very good *alternatives* to this service available to you if you prefer!

1.10 Right to lodge a complaint

In accordance with Article 77 of the General Data Protection Regulation, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence or place of work. In the Netherlands, that is the *Autoriteit Persoonsgegevens*. See http://autoriteitpersoonsgegevens.nl/ for details.

1.11 No statutory or contractual requirement

Note that there is no statutory requirement to provide your data to the MSDCA credential service. However, we cannot provide the service without all of the information we request: this is the minimal set as explained above in the balancing test (section 1.2.1).

1.12 Source from which the personal data originate

We collect all data directly from you, the user.

The registration authority (the person who verifies and countersigns your application) does not add anything to this data, and merely verifies the correctness of the data you supplied on the form.

1.13 No automated decision-making

The MSDCA service does not employ automated decision making. Due to the nature of the service, all data is manually reviewed and the credentials issued via a manual process on an off-line dedicated system.