


GWWDG NACHRICHTEN 12|21

Services for Research
Data Management

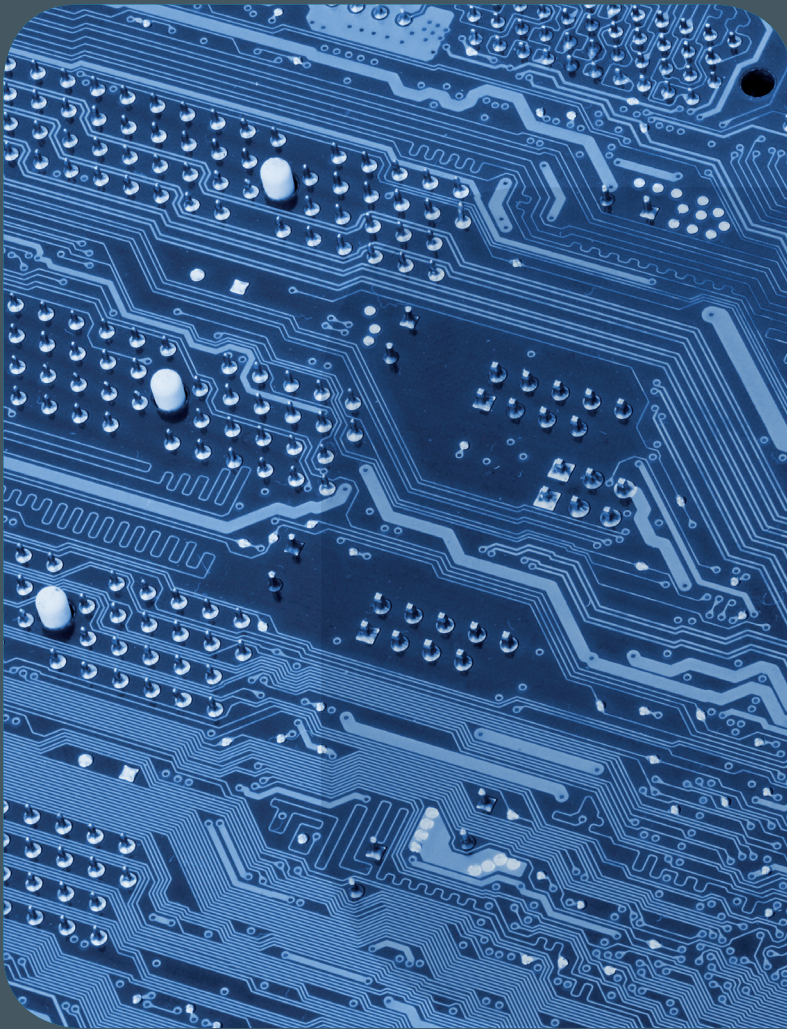
Veranstaltungsmanagement
mit Indico

GÉANT TCS PKI-Backend

ZEITSCHRIFT FÜR DIE KUNDEN DER GWWDG



Frohe
Weihnachten
und einen
guten Rutsch
ins neue Jahr!



GWDG NACHRICHTEN

12|21 Inhalt

4 Services for Research Data Management

6 Veranstaltungsmanagement mit Indico

9 Das GÉANTTCS PKI-Backend für DRAOs

21 Kurz & knapp 23 Stellenangebot

24 Personalia 25 Academy

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
44. Jahrgang
Ausgabe 12/2021

Erscheinungsweise:
10 Ausgaben pro Jahr

www.gwdg.de/gwdg-nr

Auflage:
550

Fotos:

© sutichak - stock.adobe.com (1)
© monsitj - stock.adobe.com (5)
© edelweiss - Fotolia.com (8)
© pterwort - Fotolia.com (22)
© nito - Fotolia.com (23)
© Robert Kneschke - Fotolia.com (25)
© MPIbpc-Medienservice (3, 24)
© GWDG (2)

Herausgeber:

Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen
Burckhardtweg 4
37077 Göttingen
Tel.: 0551 39-30001
Fax: 0551 39-130-30001

Redaktion:

Dr. Thomas Otto
E-Mail: thomas.otto@gwdg.de

Herstellung:

Maria Geraci
E-Mail: maria.geraci@gwdg.de

Druck:

Kreationszeit GmbH, Rosdorf



Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de
0551 201-1545

*Liebe Kund*innen und Freund*innen der GWDG,*

im Rückblick wird das Jahr 2021 wahrscheinlich als Übergangsjahr in Erinnerung bleiben. Die diversen Einschränkungen durch die Pandemie waren zwar nicht mehr neu, aber eine Normalisierung hat sich noch nicht eingestellt. Homeoffice und Videokonferenzen dominierten weiterhin den Arbeitsalltag, während die ebenfalls wichtige soziale Interaktion leider zu kurz kam. Für die GWDG gab es mit dem Bezug des neuen Rechenzentrums größere Veränderungen, welche aber erst in 2022 zum Tragen kommen, wenn mehr Infrastruktur aufgebaut ist und mehr Mitarbeitende regelmäßig im Gebäude arbeiten. Die GWDG war in diesem Jahr weiterhin erfolgreich, um Forschungsprojekte zu unterstützen und überregionale Infrastrukturinitiativen zu begleiten. Ich bin zuversichtlich, dass im kommenden Jahr neue Herausforderungen zu Chancen werden. So wünsche ich Ihnen und Ihren Familien geruhsame Feiertage und einen guten Start in ein erfolgreiches Jahr 2022 in allerbesten Gesundheit.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Services for Research Data Management

Text and Contact:

Prof. Dr. Philipp Wieder
philipp.wieder@gwdg.de
0551 201-1576

Nowadays, researchers frequently produce and re-use large amounts of data across almost all scientific disciplines. The management of this research data became an essential task for many researchers and an integral part of the planning and execution of research projects. In order to provide our users with the best possible support also in this area, we offer a growing portfolio of services for research data management. This article provides a brief introduction into the topic and describes selected services.

RESEARCH DATA MANAGEMENT

Integrated and concise data management is a core pillar of innovative research. The respective research data life-cycle comprises steps like plan and design, collect and capture, collaborate and analyse, manage, store and preserve, share and publish, as well as discover, re-use and cite [1]. The implementation of such a life-cycle at an institute or in a project normally involves a number of different expertise from domain experts, data scientists, or IT specialists, and contributions as well as services from various players like libraries, service providers, or data centres.

As a service provider for the Max Planck Society, the Georg-August-Universität Göttingen, and many other academic customers, we see it as our mission to support you here and provide long-lasting services for research. Over the years, the GWDG has therefore developed together with partners like the Göttingen eResearch Alliance (eRA) [2] a growing portfolio of services for research data management. These services are available for individual researchers, projects, and whole institutions. They are already integrated into research life-cycles of various SFBs, projects from the National Research Data Infrastructure (NFDI) [3] or related to EOSC [4].

In this article, we briefly highlight a selection of the research data management services that we offer to the Georg-August-Universität Göttingen, the Max Planck Society, and other user communities from research and academia.

DATA REPOSITORY

GRO.data [5] is a universal repository for research data that we operate based on the open-source software Dataverse [6]. In addition to its primary purpose, which is the publication of research data, it offers a variety of functions that support you working with research data management. You can edit your data and metadata, use version control, and share individual data sets or data collections with your colleagues. Once you are ready, you can publish your data including metadata and receive a persistent reference like a DOI to be used as a reference in publications. Furthermore, it is possible to apply project-specific metadata schema. This has

been already successfully implemented for large collaborative projects like SFBs to sustain large amounts of data also after the end of the projects.

GRO.data is available to all customers of the GWDG. The service is integrated into the GWDG infrastructure and accessible through single sign-on. External project and collaboration partners can also be invited to use the service.

DATA MANAGEMENT PLANNING

With GRO.plan [7] we offer a service that guides you step by step towards the definition of a data management plan (DMP). Depending on the research subject or the funding programme, GRO.plan offers tailored questionnaires. Requirements of the DFG and the European Commission, among others, are taken into account. Status and progress of the plans remain visible and adaptable through versioning. You can adapt your DMPs over the lifetime of your project, share DMPs, export them to different formats and publish them.

GRO.plan is based on the open-source software RDMO [8] and can be used by all customers of the GWDG. It is accessible through single sign-on and can also be used by your project and collaboration partners.

Services für das Forschungsdatenmanagement

Heutzutage werden von Forschenden in fast allen wissenschaftlichen Disziplinen große Mengen an Daten produziert und wiederverwendet. Das Management dieser Forschungsdaten ist für viele Forschende zu einer wesentlichen Aufgabe geworden und darüber hinaus ist es mittlerweile ein integraler Bestandteil der Planung und Durchführung von Forschungsprojekten. Um unsere Nutzer*innen auch in diesem Bereich bestmöglich zu unterstützen, bieten wir ein wachsendes Portfolio an Dienstleistungen für das Forschungsdatenmanagement an. Dieser Artikel gibt eine kurze Einführung in das Thema und beschreibt ausgewählte Dienste.



MANAGEMENT OF LARGE INSTRUMENTS

GRO.instruments offers you a web-based management platform for research instruments and enables collaboration across laboratories, institutes or organisational boundaries. The service can be used to manage instruments, schedule their usage, generate usage reports, and maintain an institutional overview. Furthermore, it is possible to manage usage requests directly and grant access to selected users on specific instruments.

GRO.instruments is currently used in production by selected customers of the GWDG. In case you are interested to use it for your institute or service unit, please contact support@gwdg.de.

PERSISTENT IDENTIFIERS

Persistent identifier (PID) services offer you the possibility to generate permanent and referable identifiers for research results like data, papers, or images [9]. Furthermore, you can receive institutional prefixes that make all generated PIDs recognisable as belonging to your institution. You can create and maintain PIDs via either a GUI or REST interface. The GWDG operates a local resolver for PIDs and, as a partner of the ePIC consortium [10], provides access to a highly available European PID infrastructure. In addition, especially for the humanities, you have the possibility to get DOIs via the service GRO.identifiers of the eRA.

We offer quick and easy access to all customers to the creation of individual PIDs via a self-service area. There you have the possibility to create and edit PIDs via the browser and to maintain a list of your PIDs. If you need a larger number of PIDs or would like to integrate them into your application, please contact us via support@gwdg.de.

DATA ARCHIVING

We operate archive servers for easy and long-term storage of large amounts of data [11]. Via hierarchical storage management

(HSM), files are automatically transferred to tape storage after longer periods of inactivity and also automatically restored in a few minutes if required.

In addition, we consult users and implement tailored solutions for large-scale archiving tasks. Examples include “Archival Cultural Heritage Online” [12] as part of the Research Program “History of the Max Planck Society” and the long-term preservation system of the German National Library [13]. Such archiving and preservation solutions are built for archiving structured data sets where metadata should remain searchable and easy to find even when archived. We are happy to work with you on archiving particularly large data sets and developing customised research data management solutions for you. Please also use support@gwdg.de for your request.

REFERENCES AND FOOTNOTES

- [1] <https://www.yorksj.ac.uk/students/library/research-support/research-data-management/>
- [2] <https://www.eresearch.uni-goettingen.de/>
- [3] <https://www.nfdi.de/>
- [4] <https://eosc-portal.eu/>
- [5] <https://data.goettingen-research-online.de/>
GRO refers to “Göttingen Research Online”, a collection of research data management services. Despite the brand name, the services are available to all users of GWDG services.
- [6] <https://dataverse.org/>
- [7] <https://plan.goettingen-research-online.de/>
- [8] <https://rdmorganiser.github.io/en/>
- [9] <https://www.gwdg.de/research-data-management/persistent-identifier-pid/epic-pid-search>
- [10] <https://www.pidconsortium.net/>
- [11] <https://www.gwdg.de/storage-services/data-archiving>
- [12] <https://gmpg.mpiwg-berlin.mpg.de/de/forschungsprogramm/kooperationspartner>
- [13] <https://www.dnb.de/EN/Professionell/Erhalten/LZA-System/lza-system.html>

Veranstaltungsmanagement mit Indico

Text und Kontakt:
Sina Trabert
sina.trabert@gwdg.de
0551 39-30289

Die GWGD bietet seit dem 20. September 2021 für das Konferenz- und Veranstaltungsmanagement die Open-Source-Software „Indico“ im Rahmen eines Pilotprojektes an. Indico löst damit für diesen Anwendungsbereich die bisher eingesetzte Software „Lotus Notes“ ab. Im Unterschied zu Lotus Notes können die Pilotnutzer*innen mit Indico ihre Veranstaltungen nun selbstständig erstellen und verwalten, was ihnen zudem eine große Flexibilität und viele neue Designmöglichkeiten bietet.

INDICO BEI DER GWGD

Indico ist eine vom CERN entwickelte Open-Source-Software und findet im Bereich des Konferenz- und Veranstaltungsmanagements weite Verbreitung. Sie ist eine Webanwendung. Mithilfe von Indico können Vorträge, Meetings und Konferenzen organisiert werden. [1]

Aktuell befindet sich die GWGD mit Indico in einer Pilotphase, um in einem kleinen Rahmen zunächst wertvolle Erfahrungen zu sammeln und die Software ausgiebig zu erproben, bevor der Dienst dann in den Regelbetrieb geht. Von der Max-Planck-Gesellschaft nehmen einige Institute als Pilotinstitute an dem Pilotprojekt teil. Des Weiteren setzt die Verwaltung eines Departments der Universität Göttingen Indico ein. Von der GWGD partizipieren zudem zurzeit deren Öffentlichkeitsarbeit und Verwaltung. Weitere Interessenten sind herzlich eingeladen, an dem Pilotprojekt teilzunehmen. Partizipieren können alle Kund*innen der GWGD mit ihren Instituten und Abteilungen. Wenn Sie an dem Pilotprojekt teilnehmen möchten, melden Sie sich bitte per Single Sign-on (SSO) mit Ihrer primären E-Mail-Adresse auf <https://events.gwdg.de> an und erstellen sich dann dort ein Indico-Profil. Für das Erstellen des Profils benötigen Sie außer Ihrer E-Mail-Adresse nur noch Ihren Vor- und Nachnamen. Anschließend senden Sie uns bitte Ihre Anfrage an veranstaltungen@gwdg.de.

Im Moment wird die Indico-Version 3.03 verwendet. Indico löst im Bereich Veranstaltungsmanagement die bisher dafür eingesetzte Software „Lotus Notes“ ab. Die Software „Indico“ bietet eine große Flexibilität, indem die Pilotnutzer*innen ihre Veranstaltungen selbstständig erstellen und verwalten können. In Indico gibt es u. a. die Funktion der Änderungsverfolgung, mit der nachvollzogen werden kann, welche Personen Änderungen an den Kategorien oder den Veranstaltungen vorgenommen haben. Des Weiteren bietet Indico einen Export von Veranstaltungsinformationen zum Kalenderimport an. Hier können die Nutzer*innen die zukünftigen Veranstaltungen als iCalendar-File oder als Link in ihren Kalender importieren lassen.

ERSTELLEN UND VERWALTEN VON KATEGORIEN

Es besteht die Möglichkeit, in Indico Kategorien zu erstellen. Kategorien werden erstellt, um weitere (Unter-)Kategorien anzulegen oder um Veranstaltungen gruppieren zu können. Die oberste Kategorie in Indico ist die Home-Kategorie. Ihr sind alle anderen Kategorien untergeordnet. [2]

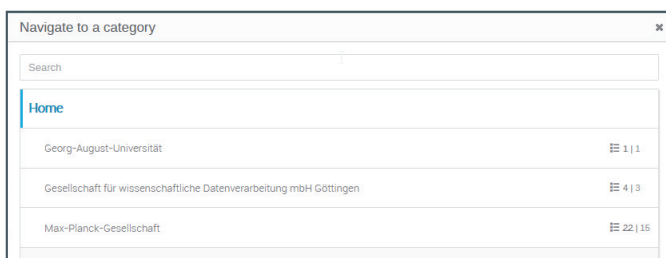
In einer Kategorie kann entweder eine neue Unterkategorie oder eine neue Veranstaltung erstellt werden. Allerdings ist es nicht möglich, in einer Kategorie gleichzeitig eine Veranstaltung und eine Unterkategorie anzulegen. [3]

Im Moment finden sich unter der Hauptkategorie „Home“ drei weitere Unterkategorien: die Georg-August-Universität, die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen und die Max-Planck-Gesellschaft (siehe Abbildung 1). In jeder dieser drei Kategorien befinden sich jeweils weitere Unterkategorien der einzelnen Institute und Abteilungen. In den Unterkategorien können die einzelnen Institute und Abteilungen weitere Unterkategorien oder Veranstaltungen erstellen. Nutzer*innen bekommen jeweils eine Berechtigung an der entsprechenden Kategorie, sodass sie nur in der eigenen Kategorie neue Veranstaltungen oder weitere Unterkategorien erstellen und verwalten können.

In Indico gibt es viele Designmöglichkeiten, indem z. B. bei den einzelnen Kategorien ein eigenes Logo hinzugefügt werden

Event Management with Indico

Since September 20, 2021, the GWGD offers the open source software "Indico" for conference and event management as part of a pilot project. Indico replaces the previously used software "Lotus Notes" for this area of application. In contrast to Lotus Notes, the pilot users can now create and manage their events independently with Indico, which also offers them great flexibility and many new design options.



1_Kategorienstruktur

kann. Auch besteht die Möglichkeit, bei jeder Kategorie ein Icon hinzuzufügen.

VERANSTALTUNGSTYPEN

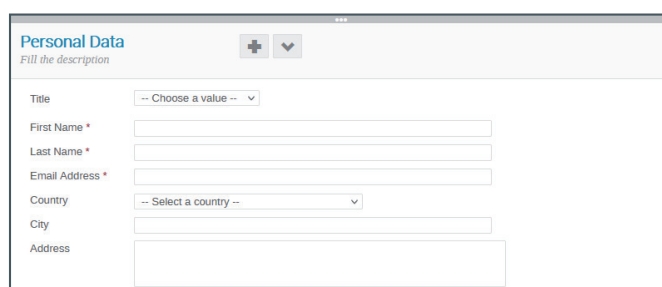
In Indico gibt es drei verschiedene Veranstaltungstypen: den Vortrag, das Meeting und die Konferenz. Ein Vortrag kann eine Präsentation beinhalten und mit vielen Redner*innen oder einem/einer Redner*in abgehalten werden. Normalerweise umfasst ein Meeting mehrere Präsentationen. Die Dauer eines Meetings kann variieren: Ein Meeting kann einen Tag oder mehrere Tage dauern, wobei ein Meeting aber häufig nur an einem Tag veranstaltet wird. Es besteht die Möglichkeit der Organisation von Beiträgen für das Meeting. In einem Meeting können außerdem noch Protokolle hinzugefügt werden. Eine Konferenz umfasst in der Regel einige Tage und es können mehrere Sitzungen parallel abgehalten werden. Außerdem besitzen Konferenzen den Vorteil, dass sie Arbeitsabläufe zum Bearbeiten von Abstracts und Unterlagen flexibel ermöglichen. [4]

Nutzer*innen können bei allen drei Eventtypen verwaltet werden. Auch sind Anmeldungen und die Nutzung von u. a. kollaborativen Tools möglich. Außerdem können Erinnerungs-E-Mails für Events versendet werden. Im Material-Editor können Ordner erstellt und PDFs hochgeladen werden. Nutzer*innen können in wenigen Schritten ihre erste Veranstaltung erstellen. [5]

Im Vergleich zu einer Konferenz hat ein Vortrag weniger Funktionen und ist in den Designoptionen nicht so flexibel. Bei der Konferenz gibt es viele verschiedene Designoptionen; es können ein Logo und die Farbe des Headers angepasst werden. Des Weiteren können eigene implementierte Stylesheets in Konferenzen verwendet werden. Bei allen Veranstaltungstypen besteht die Möglichkeit, einen Klon von der Veranstaltung zu erstellen. Durch die Verwendung dieser Funktion können Nutzer*innen einfach und schnell eine neue Veranstaltung auf Basis einer bereits angelegten ähnlichen Veranstaltung erstellen. Indico ist einfach und intuitiv zu verwenden. Sie ist so aufgebaut, dass nach der Erstellung einer Veranstaltung einzelne Module aktiviert werden können. Je nach dem Typ der Veranstaltung können unterschiedliche Module aktiviert werden.

ERSTELLEN EINES ANMELDEFORMULARS

Ein aktivierbares Modul ist das Anmeldeformular. Nach seiner Aktivierung können einzelne Felder zum Anmeldeformular hinzugefügt, gelöscht oder deaktiviert werden. Es stehen verschiedene Feldtypen zur Auswahl, die einem Anmeldeformular



2_Beiispiel eines Anmeldeformulars

hinzugefügt werden können: u. a. freier Text, Textinput, Zahlen, ein Textfeld, eine Checkbox, ein Kalender, ein Dropdown-Menü, eine Radio Group oder ein Datei-Upload. Zu beachten sind außerdem die Einstellungen für die Registrierungsmöglichkeiten der Teilnehmer*innen. In Indico gibt es die Option, dass die Registrierung entweder umgehend erfolgen kann oder auch, dass ein Datum mit Uhrzeit für die Eröffnung der Registrierung festgelegt wird und sie dann ab diesem angegebenen Zeitpunkt möglich ist. Dieselbe Funktionalität gibt es auch beim Schließen der Registrierung der Teilnehmer*innen.

CALL FOR ABSTRACTS

Bei der Konferenz gibt es u. a. das Modul „Call for Abstracts“. Dieses Modul kann aktiviert werden, um das Einreichen von Abstracts zu ermöglichen. Es kann ein Regelsatz für das Submitting von Abstracts erstellt werden, damit die Teilnehmer*innen eine E-Mail-Benachrichtigung erhalten. Anschließend können Gutachter*innen beim Reviewing Abstract die eingereichten Abstracts bewerten, indem sie u. a. Kommentare zu den Abstracts schreiben. Richter*innen können die Abstracts ablehnen oder akzeptieren.

WEITERE INFORMATIONEN

Einsteiger-Workshop

Um Indico kennenzulernen, bieten wir je nach Bedarf einen ca. einstündigen virtuellen Einsteiger-Workshop zum Thema „Die ersten Schritte mit Indico“ an. In diesem Workshop zeigen wir Ihnen u. a., wie Sie in wenigen Schritten einen Vortrag in Indico erstellen können. Außerdem werden die verschiedenen Eventtypen vorgestellt. Falls Interesse besteht, an diesem Workshop teilzunehmen, schreiben Sie bitte eine E-Mail an veranstaltungen@gwdg.de. Wenn Sie Interesse an Indico haben, besuchen Sie unsere Webseite <https://events.gwdg.de>.

Anleitung

Eine ausführliche Anleitung zum Thema „Veranstaltungsmanagement mit Indico“ finden Sie auf https://docs.gwdg.de/doku.php?id=de:services:application_services:workflow_management:event_management.

FUSSNOTEN

[1] – [5] Vgl. <https://learn.getindico.io>



Servervirtualisierung

DER EINFACHE WEG ZUM SERVER!

Ihre Anforderung

Sie benötigen zur Bereitstellung eines Dienstes einen Applikations- oder Datenbankserver. Ihnen fehlen Platz, Hardware, Infrastruktur oder Manpower. Gleichzeitig soll der Server möglichst hochverfügbar und performant sein.

Unser Angebot

Wir bieten Ihnen die Möglichkeit des Hostings von virtuellen Servern für Ihre Anwendungen basierend auf VMware ESX. Sie können Ihre eigenen virtuellen Maschinen verwalten, die in unserer zuverlässigen Rechnerinfrastruktur gehostet werden, die unterschiedliche Verfügbarkeitsgrade unterstützen. Unsere Installation hält die Best-Practice-Richtlinien von VMware ESX ein. Sie bleiben Administrator Ihres eigenen virtuellen Servers, ohne sich mit der physikalischen Ausführungsumgebung beschäftigen zu müssen.

Ihre Vorteile

- > Leistungsfähiges VMware-Cluster mit zugehörigem Massenspeicher

- > Hohe Ausfallsicherheit und Verfügbarkeit durch redundante Standorte und Netzwerkverbindungen sowie USV-Absicherung
- > Bereitstellung aller gängigen Betriebssysteme zur Basisinstallation
- > Umfassender administrativer Zugang zu Ihrem Server im 24/7-Selfservice
- > Möglichkeit der automatisierten Sicherung des Servers auf unsere Backupsysteme
- > Zentrales Monitoring durch die GWDG
- > Große Flexibilität durch Virtualisierungstechnologien wie Templates, Cloning und Snapshots
- > Schutz vor Angriffen aus dem Internet durch leistungsfähige Firewallsysteme sowie ein Intrusion Prevention System

Interessiert?

Jede*r Nutzer*in mit einem gültigen Account bei der GWDG kann das VMware-Cluster nutzen. Um einen virtuellen Server zu beantragen, nutzen Sie bitte die u. g. Webadresse.

Das GÉANT TCS PKI-Backend für DRAOs

Text und Kontakt:

Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 39-30307

Mit der Migration der DFN-PKI im Sicherheitsniveau „Global“ in Richtung GÉANT TCS PKI-Backend leitet der DFN-Verein einen Übergang seiner bisher selbst betriebenen Public-Key-Infrastruktur (PKI) in die vom GÉANT TCS betriebene Infrastruktur ein, die nach bisherigen Vorstellungen Ende 2023 abgeschlossen sein soll. In diesem Artikel sollen für die zuerst betroffenen Teilnehmerservice-Mitarbeiter*innen der MPG-, Uni Göttingen- und GWDG-CA, im neuen Sprachgebrauch DRAOs genannt, die wichtigsten Funktionen und Möglichkeiten beschrieben werden, damit diese in die Lage versetzt werden, nach und nach Server- und Nutzerzertifikate in das neue GÉANT TCS PKI-Backend zu migrieren.

EINLEITUNG

Durch die immer strenger werdenden Auflagen des CA/Browser-Forums [1] zum Betrieb von öffentlichen Certifications Authorities (CAs) wird es für den DFN-Verein immer schwieriger, die DFN-PKI im Sicherheitsniveau „Global“ noch weiter sinnvoll zu betreiben. Deshalb hat sich der DFN-Verein entschlossen, sich dem GÉANT Trusted Certificate Service, kurz GÉANT TCS, anzuschließen und dessen für National Research and Education Network, kurze NREN, bereitgestellte PKI zu nutzen. Durch einen Wechsel des CA-Anbieters Ende letzten Jahres sah der DFN-Verein nun eine gute Gelegenheit, beim GÉANT TCS mit einzusteigen. Nach einer Pilotphase in Q1/Q2 2021, bei der die GWDG einer dieser Pilotteilnehmer war, wurde das Ausrollen an die gesamten Teilnehmer des DFN-Vereins, unter anderem auch die MPG, Uni Göttingen und GWDG, in Q3 gestartet. Ende September waren dann für alle drei CAs (MPG, Uni Göttingen und GWDG) die gesamte Infrastruktur und alle Zugänge für die DRAOs und deren Zuordnung zu deren Departments erfolgt. Seit diesem Zeitpunkt ist es nun möglich, Server- und Nutzerzertifikate von der DFN-PKI in Richtung GÉANT TCS zu migrieren.

Dies sollte auch getan werden, da der DFN-Verein selber einen entsprechenden Zeitplan hat, die DFN-PKI im Sicherheitsniveau „Global“ durch GÉANT TCS abzulösen. Dieser sieht vor, dass nur noch bis Ende 2022 Serverzertifikate und bis Ende 2023 Nutzerzertifikate in bisheriger Form beantragt werden können. Und gerade bei den Serverzertifikaten drohen ja die Browser-Hersteller damit, in absehbarer Zeit nur noch Serverzertifikate mit einer Laufzeit von 90 Tagen als gültig anzuerkennen. Der damit einhergehende Aufwand der Beantragung und Ausstellung von Zertifikaten beim Vorhandensein vieler Server steht dann in keinem vertretbaren Aufwand mehr und muss dringend automatisiert werden.

Als vorweggenommenes Fazit kann gesagt werden, das GÉANT TCS ist weniger bürokratisch und von den Abläufen schlanker sowie besser automatisierbar.

BEGRIFFSERKLÄRUNGEN

In der GÉANT TCS gibt es neue Namen für bisherige Funktionen in der DFN-PKI. Hier eine Liste dieser neuen Namen in der Form DFN-PKI -> GÉANT TCS

- DFN -> Mandant
- CA -> Organisation
- RA -> Department
- DFN-MA -> MRAO (Mandant Authority Officer)
- HP-PKI -> RAO (Registration Authority Officer)
- TS-MA -> DRAO (Department Registration Authority Officer)

LOGIN/ANMELDUNG

Nach dem Login im Sectigo Certificate Manager unter [2] muss das initiale Passwort zwingend geändert werden. Danach bitte gleich den privaten Schlüssel für die Zertifikatwiederherstellung erzeugen und gut abspeichern (siehe Abschnitt

The GÉANT TCS PKI Backend for DRAOs

With the migration of the DFN PKI in the security level “Global” towards the GÉANT TCS PKI backend, the DFN-Verein is initiating a transition of its previously self-operated public key infrastructure (PKI) into the infrastructure operated by GÉANT TCS, which according to previous ideas should be completed by the end of 2023. In this article, the most important functions and possibilities are to be described for the first affected subscriber service employees of the MPG-, Uni Göttingen- and GWDG-CA, called DRAOs in the new parlance, so that they are enabled to gradually migrate servers and user certificates to the new GÉANT TCS PKI backend.

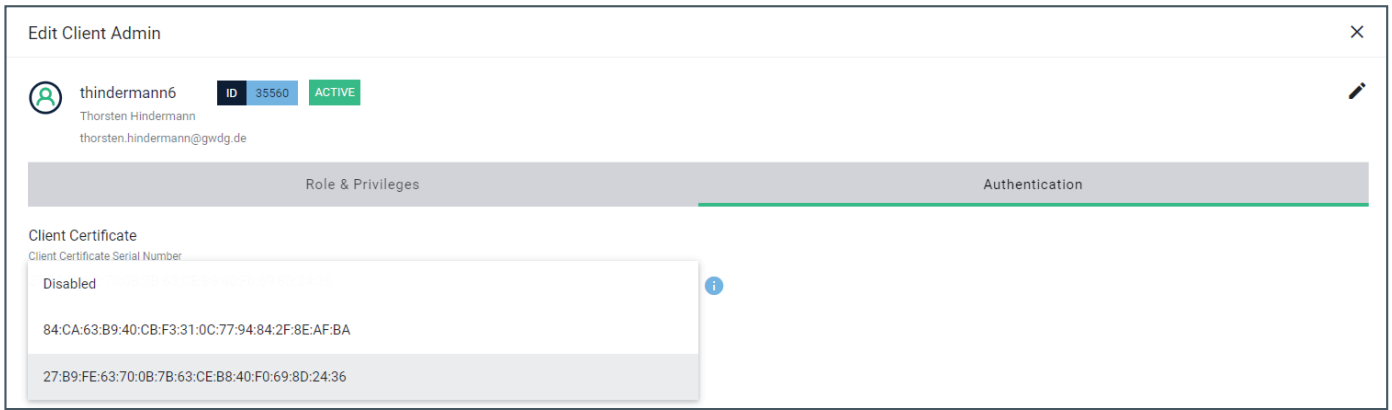


Abb. 1



Abb. 3

„Schlüsselsicherung für Ihr Department (Key escrow“).

Weitere Einstellungen

Für die weiteren Login-Optionen empfiehlt es sich, ggf. einen weiteren „Arbeits“-Account anzulegen, der zusätzlich mit einem Zertifikat als zweiter Faktor abgesichert werden kann oder für den die Anmeldung per SSO eingestellt wird.

Zertifikat

Um den Account mit einem Zertifikat als zweiten Faktor abzusichern (neben Nutzernamen und Passwort), muss folgende Bedingung erfüllt sein: Die E-Mail-Adresse des DRAO-Accounts muss mit der E-Mail-Adresse in einem Nutzerzertifikat übereinstimmen. Erst dann wird in der Dropdown-Liste das entsprechende Zertifikat angezeigt.

Um dorthin zu gelangen, ist wie folgt vorgehen: ≡ > Settings > Admins, den zu bearbeitenden DRAO-Account anklicken und auf die Schaltfläche „Edit“ klicken. In dem Dialog auf „Authentication“ klicken und mit einem Klick auf die Auswahlliste das entsprechende Zertifikat auswählen (siehe Abbildung 1).

SSO-Login

Für die Anmeldung mittels SSO-Login müssen alle Voraussetzungen für SSO erfüllt sein. Um zu überprüfen, ob alle Voraussetzungen erfüllt sind, schauen Sie bitte im Abschnitt „Vorbereitende Schritte für den SSO-Login“. Wenn die in diesem Abschnitt beschriebenen Anmeldungen ohne Fehlermeldungen funktionieren, sind die Voraussetzungen geschaffen.

Als DRAO können Sie sich selber nicht den SSO-Login einstellen. Dazu geben Sie dem Autor dieses Artikels als RAO Bescheid, denn als RAO kann er die zusätzliche SSO-Anmeldung für Sie einschalten.

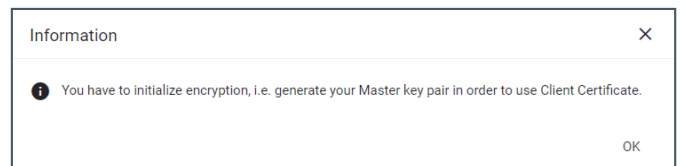


Abb. 2

SCHLÜSSELSICHERUNG FÜR IHR DEPARTMENT (KEY ESCROW)

Wichtiger Hinweis vorweg: Schlüssel- bzw. Zertifikatwiederherstellung funktioniert nur mit von Ihnen als DRAO in Ihrem Department manuell angelegten Nutzerzertifikaten, nicht für die vom Nutzer via SSO-Login beantragten und ausgestellten Zertifikate.

Damit Sie in der Lage sind, Zertifikate wiederherzustellen, müssen Sie den privaten Schlüssel Ihres Departments erzeugen und sicher speichern und verwahren. Wenn Sie mehr als ein DRAO in Ihrem Department sind, sprechen Sie sich bitte ab, damit die Generierung des privaten Schlüssels für das Department nur einmal ausgeführt wird.

Solange Sie den Schlüssel nicht erzeugt haben, wird Ihnen bei jedem Login in Ihr Department

- eine Warnung angezeigt und (siehe Abbildung 2) und
- können Sie vorher keine Zertifikate ausstellen.

Die Schlüsselerzeugung für die Zertifikat-Wiederherstellung erreichen Sie unter ≡ ->Settings->Legacy Key Encryption. Klicken Sie das entsprechende Department an und anschließend auf die Schaltfläche „Initialize Encryption“ (siehe Abbildung 3).

Folgen Sie den Anweisungen in dem nun erscheinenden Dialog, der den privaten Schlüssel für das Wiederherstellungszertifikat enthält (siehe Abbildung 4). Wenn Sie den privaten Schlüssel sicher gespeichert haben, klicken Sie auf die Schaltfläche „Done“. Es erfolgt eine Sicherheitsabfrage. Jetzt können Sie mit einem Klick auf die Schaltfläche „YES“ bestätigen (siehe Abbildung 5).

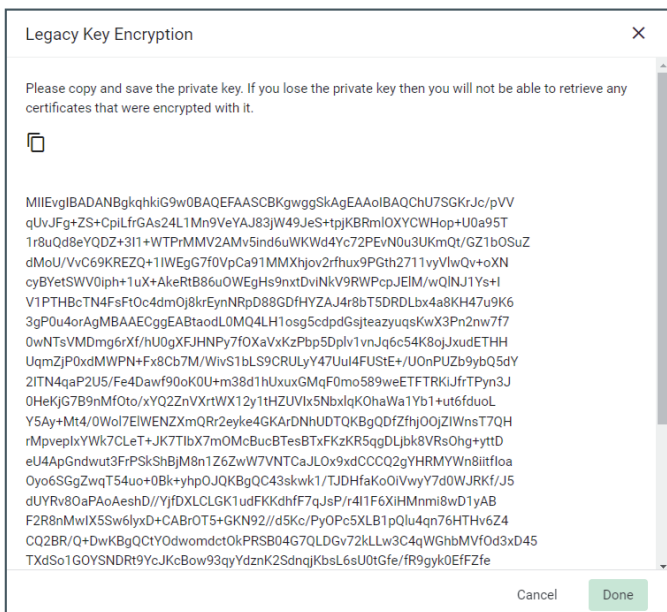


Abb. 4

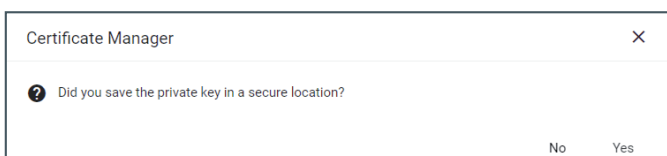


Abb. 5

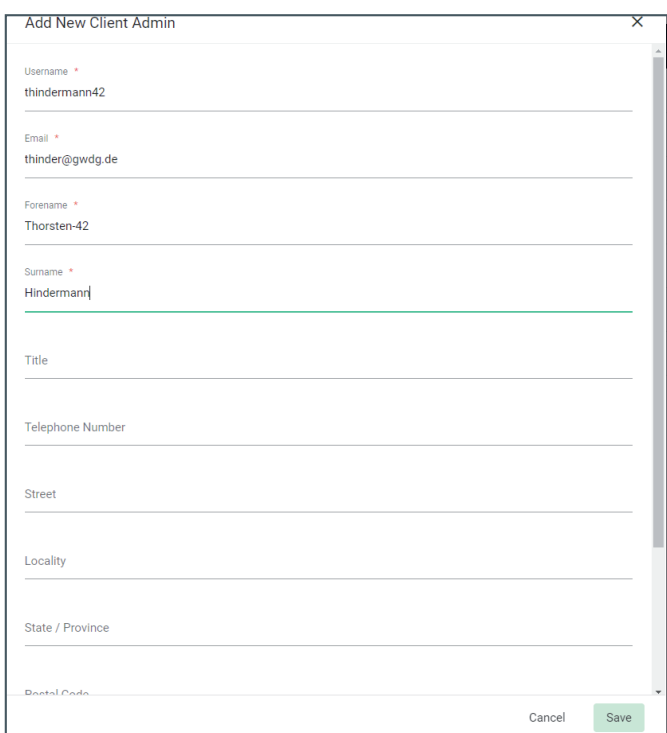


Abb. 7



Abb. 6

Nach der Aktion ist der öffentliche Schlüssel in Ihrem Department für die Zertifikatswiederherstellung vorhanden (siehe Abbildung 6).

ANLEGEN WEITERER DRAOS

Als DRAO haben Sie die Möglichkeit, selber weitere Kolleg*innen als DRAOs anzulegen. Unter ≡ >Settings > Admins klicken Sie oben ganz rechts auf die Schaltfläche „+“ und erstellen einen neuen Account für den weiteren DRAO. Im Dialogfeld füllen Sie Pflichtangaben für den neuen DRAO aus und klicken anschließend auf die Schaltfläche „Save“ (siehe Abbildung 7).

Unter dem Registerkartenreiter „Roles & Privileges“ können Sie mit den Schaltern einstellen, für welche Zertifikattypen der neue DRAO zuständig sein soll (siehe Abbildung 8). Wenn Sie einen Schalter nach rechts verschieben wird ein Bereich mit einem Stift-Symbol sichtbar. Klicken Sie auf diesen Stift, um das oder die Departments auszuwählen, in der bzw. denen der neue DRAO für diesen Zertifikattyp zuständig sein soll. Mit einem Klick auf die Schaltfläche „OK“ wird diese Auswahl bestätigt (siehe Abbildung 9).

Soll der neue DRAO seinerseits weitere DRAOs in Ihrem Department anlegen können, so können Sie das unter „Privileges“ als DRAO selber nicht anklicken. In diesem Fall treten Sie wieder mit uns in Kontakt, damit wir diese Privilegien für den neuen DRAO einmalig setzen. Denn die Vergabe dieser Privilegien können nur wir als RAO einrichten.

Im Registerkartenreiter „Authentication“ vergeben Sie noch das initiale Passwort für den neuen DRAO. Dieses wird zwangsweise bei der ersten Anmeldung des neuen DRAO geändert. Sollte der DRAO dann auch über ein Nutzerzertifikat verfügen, dessen E-Mail-Adresse gleich der E-Mail-Adresse des DRAO-Accounts ist, besteht die Möglichkeit der Absicherung der Anmeldung an der Sectigo-Webseite (Sectigo Certificate Manager, kurz SCM) über den zweiten Faktor dieses Zertifikats, das in der Ausklappliste ausgewählt werden kann (siehe Abbildung 10).

Mit einem Klick auf „Save“ ist der neue DRAO angelegt. Lassen Sie diesem die Zugangsdaten zukommen, damit er sich anmelden kann.

VORBEREITENDE SCHRITTE FÜR DEN SSO-LOGIN

Für den Test, ob alle Vorbereitungen für den SSO-Login an den Sectigo-Webseiten funktionieren, gibt es zwei URLs:

1. Von der DFN-AAI -> [3]
2. Von Sectigo -> [4]

Erst wenn Sie sich an diesen beiden Shibboleth-Testwebseiten erfolgreich anmelden konnten, wird auch Ihre Anmeldung

Abb. 8

Abb. 9

displayName	urn:oid:2.16.840.1.113730.3.1.241	Johnny Doe	USED for CN.
cn	urn:oid:2.5.4.3	John Doe	fallback for CN.
sn	urn:oid:2.5.4.4	Doe	fallback for CN.
givenName	urn:oid:2.5.4.42	John	fallback for CN.
mail	urn:oid:0.9.2342.19200300.100.1.3	john DOE@example.edu	yes
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	jd@example.edu	yes
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	urn:mace:terena.org:tcs:personal-user	yes
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	example.edu	yes

Tabelle 1: Sectigo SSO-Attribute

als DRAO mittels SSO-Login funktionieren. Und wenn auch diese gemachten Einstellungen auf die Accounts Ihrer Kolleg*innen übertragen werden, können sich diese ebenfalls ab diesem Zeitpunkt per SSO-Login ein Zertifikat erstellen.

Ihr Identity Provider, kurz IdP, muss folgende Attribute an den Service Provider, kurz SP, senden (siehe Tabelle 1):

Die Abbildungen 11 und 12 zeigen, wie Beispiele für erfolgreiche SSO-Logins an den beiden genannten Webseiten [3] und [4] aus, wenn alle Attribute erfolgreich übermittelt worden sind.

SERVERZERTIFIKATE

Bei den Serverzertifikaten gibt es zwei Möglichkeiten, dass Server zu ihren Zertifikaten kommen, die z. B. für die Absicherung von Webseiten per HTTPS notwendig sind.

Certbot

Neben dem von Let's Encrypt bekannten das ACME-Protokoll unterstützenden certbot [5] für UNIX und Windows gibt es noch ein paar andere Programme, die das ACME-Protokoll unterstützen, z. B. win-acme [6] speziell für Windows oder acme.sh [7] für UNIX.

All den genannten Programmen ist gemeinsam, dass sie das External Account Binding, kurz EAB, unterstützen. Die EAB-Unterstützung ist ein wichtiger Punkt, den Sie beachten müssen, wenn Sie sich für ein solches Programm entscheiden.

In diesem Artikel wird sich auf den certbot konzentriert, weil das komplette Angebot an ACME-Clients nicht erschöpfend abdeckt und beschrieben werden kann.

Add New Client Admin
✕

thindermann42
Thorsten-42 Hindermann
thinder@gwdg.de

✎

Role & Privileges
Authentication

Password

Password *

.....

Confirm Password *

.....

Client Certificate

Client Certificate Serial Number

Disabled
i

42:60:6E:31:3E:5C:39:F0:AD:54:24:D3:28:D0:32:F7

Abb. 10

DFN-AAI: Attribute

Die vom IdP übermittelten Attribute:

```
eduPersonEntitlement="urn:mace:dir:entitlement:common-lib-terms;urn:mace:dir:entitlement:common-lib-terms"
persistent_id="https://shibboleth-idp.gwdg.de/gwdg/shibboleth!https://testsp3.aai.dfn.de/shibboleth!7d06b78c897e046649149e1c4237597957f361b1"
```

Session Details

[Logout](#)

Abb. 11

Successful SSO Check

Thanks for visiting the Sectigo Certificate Manager SSO Check page. You have successfully authenticated to the configured IdP so basic functionality seems to be work correctly.

Session Information

Identity Provider	https://shibboleth-idp.gwdg.de/gwdg/shibboleth
Protocol	urn:oasis:names:tc:SAML:2.0:protocol
Authentication Time	1.12.2021, 09:16:48
Session Expiration	479 minute(s)
Authentication Context Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Authentication Context Decl	n/a

Session Attributes

Attribute Name	Attribute Value(s)	Required
cn	<ul style="list-style-type: none"> thinder Thorsten Hindermann 	No
displayName	<ul style="list-style-type: none"> Thorsten Hindermann Thorsten Hindermann 	No
entitlement	<ul style="list-style-type: none"> urn:geant:dfn.de:dfn-pki:slcs urn:mace:terena.org:tc:personal-user urn:mace:dir:entitlement:common-lib-terms https://example.org/entitlement/entitlement1 urn:mace:dir:entitlement:common-lib-terms 	No
eppn	<ul style="list-style-type: none"> thinder@gwdg.de 	Yes
givenName	<ul style="list-style-type: none"> Thorsten 	No
mail	<ul style="list-style-type: none"> thorsten.hindermann@gwdg.de 	Yes
schacHomeOrganization	<ul style="list-style-type: none"> gwdg.de 	No
sn	<ul style="list-style-type: none"> Hindermann 	No

Abb. 12

Create ACME Account
✕

Name *

example-server-42

Organization *

Gesellschaft für wissenschaftliche Datenverarbeitung mbH

Department

PKI6

Validation Type OV

Domains

Domains	Remove All
gwdg.de	✖
*.gwdg.de	✖

Cancel
Save

Abb. 13

Account hinzufügen

Unter ≡ > Enrollment > ACME klicken Sie [8] an und klicken anschließend auf die Schaltfläche „Accounts“. In dem dann neu erscheinenden Dialog klicken Sie rechts auf die Schaltfläche „+“.

In dem Eingabefeld „Name“ geben Sie den Namen des Servers ein. Unter „Organization“ wählen Sie die Organisation aus, unter der Ihr Department angesiedelt ist. Bei den Departments



Abb. 14

können Sie entweder nur Ihr Department auswählen, für das Sie zuständig sind, oder sollten Sie für mehr als nur ein Department zuständig sein, dann können Sie hier wählen, in welchem Department dieser ACME-Server-Account angesiedelt werden soll. Anschließend noch die benötigten Domänen hinzufügen. Danach auf die Schaltfläche „Save“ klicken (siehe Abbildung 13).

Im nächsten Dialog werden Ihnen die External Account Binding Information angezeigt. Die drei Informationen ACME URL, Account bzw. Key ID und HMAC Key übermitteln Sie an die das System verwaltende Person (siehe Abbildung 14).

Im folgenden Abschnitt finden Sie eine E-Mail-Vorlage, die sich inzwischen als Informations-E-Mail für die die Systeme verwaltenden Personen bewährt hat. Diese können Sie, wenn Sie möchten, kopieren und für Ihre Zwecke verwenden und abwandeln.

Beispiel einer bewährten Vorlage für eine Informations-E-Mail an Systemverwalter*innen

Betreff: ACME Account-Informationen für example-server-42

Liebe/r <Name Admin>!

Den certbot können Sie unter diesem URL herunterladen: [5]. Auf dieser Webseite wird angeboten den Web-Server und das verwendete Betriebssystem auszuwählen. Daraufhin bekommen Sie eine Anleitung, wie der certbot via den gängigen Paket-Managern installiert werden kann.

==ALTERNATIVE==

*Inzwischen existiert im puppet-Repository der GWDG für den certbot ein puppet-Modul. Bitte wenden Sie sich an die puppet-Kolleg*innen der GWDG, wie Sie dieses Modul einbinden und in Ihrer Server-Konfiguration verwenden.*

==Weitere Alternative==

Als eine weitere Alternative für UNIX-Systeme gibt es acme.sh [7].

Für example-server-42 sind das die folgenden Parameter:

ACME URL: `https://acme.sectigo.com/v2/OV`

Key ID: `<Platzhalter>`

HMAC Key: `<Platzhalter>`

How to use External Account Binding (EAB) with Certbot

When Certbot is registering an ACME account, use ACME URL

(`--server`), Key ID (`--eab-kid`) and HMAC Key (`--eab-hmac-key`).

Die Parameter `--email`, `--domain` und `--certname` müssen noch angepasst werden:

Bei `--domain` den Full Qualified Domain Name, kurz FQDN, des Systems angeben. Wenn Subject Alternative Names, kurz SANs, mit in dem Zertifikat aufgenommen werden sollen, diese in einer kommaseparierten Zeichenkette angeben.

Beispiel: `--domain FQDN_1,FQDN_2,...,FQDN_N`

Alternative: `-d FQDN_1 -d FQDN_2 ... -d FQDN_N`

Bei `--cert-name` z. B. den Systemnamen oder einen anderen geeigneten, aussagekräftigen Namen angeben. Dieser Name dient dem certbot für Verwaltungsaufgaben als Ziel, welches Zertifikat aktuell verwaltet werden soll.

Bei `--email` am Besten die E-Mail-Adresse eines Funktions-Accounts wie z. B. `<Funktions-Accountname>@gwdg.de` eingeben.

KURZANLEITUNG UND WEITERE AUFRUFBEISPIELE

Erster Aufruf und einmaliger Aufruf mit Key-ID und HMAC-Key

Key-ID und HMAC-Key werden nur beim allerersten Aufruf verwendet und müssen danach nicht mehr mit angegeben werden.

Nachfolgend eine Beispiel-Kommandozeile (unter Linux mit sudo und unter Windows in einer Kommandozeile mit administrativen Rechten ausführen):

```
certbot certonly --standalone --non-interactive --agree-tos
--email example.email@gwdg.de --server https://acme.sectigo.com/v2/OV --eab-kid 3WzoNkPjwDjxp8qRqUHBkR --eab-hmac-key xX9tPjMinjxvAAZ2h5DQ2/CGxX9tPjMinjxvAAZ-2h5DQ2/CGxX9tPjMinjxvAAZ2h5DQ2/CGxX9tPjMinjxvAAZ --domain example-dns1.top.gwdg.de,example-dns2.gwdg.de --cert-name EXAMPLE-DNS
```

oder

```
certbot certonly --standalone --non-interactive --agree-tos
--email example.email@gwdg.de --server https://acme.secti-
go.com/v2/OV --eab-kid 3WzoNkPjwDjxp8qRqUHBkR --eab-
hmac-key xX9tPjMinjxvAAZ2h5DQ2/CGxX9tPjMinjxvAAZ2h-
5DQ2/CGxX9tPjMinjxvAAZ2h5DQ2/CGxX9tPjMinjxvAAZ -d
example-dns1.top.gwdg.de -d example-dns2.gwdg.de --cert-
name EXAMPLE-DNS
```

Zweiter Aufruf und weitere Aufrufe ...

Hinweis: Vorher aber immer das aktuelle Zertifikat revoked!

```
certbot certonly --standalone --non-interactive --server htt-
ps://acme.sectigo.com/v2/OV -d example-dns1.top.gwdg.de
-d example-dns2.gwdg.de --cert-name EXAMPLE-DNS
```

oder

```
certbot certonly --standalone --non-interactive --ser-
ver https://acme.sectigo.com/v2/OV --domain exemp-
le-dns1.top.gwdg.de,example-dns2.gwdg.de --cert-name
EXAMPLE-DNS
```

... mit vielen SANs und dem Parameter -d

```
certbot certonly --standalone --non-interactive --server htt-
ps://acme.sectigo.com/v2/OV -d example-dns1.top.gwdg.
de -d example-dns2.gwdg.de -d example-dns3.gwdg.de -d
example-dns4.gwdg.de -d example-dns5.gwdg.de -d exam-
ple-dns6.gwdg.de -d example-dns7.gwdg.de -d example-
dns8.gwdg.de -d example-dns9.gwdg.de -d example-dns10.
gwdg.de -d example-dns11.gwdg.de -d example-dns12.
gwdg.de --cert-name EXAMPLE-DNS
```

... mit vielen SANs und dem Parameter --domain oder --domains

Wichtiger Hinweis: Bei der Kommaliste dürfen keine Leerzei- chen dazwischen sein!

```
certbot certonly --standalone --non-interactive --server htt-
ps://acme.sectigo.com/v2/OV --domain example-dns1.top.
gwdg.de,example-dns2.gwdg.de,example-dns3.gwdg.
de,example-dns4.gwdg.de,example-dns5.gwdg.de,example-
dns6.gwdg.de,example-dns7.gwdg.de,example-dns8.
gwdg.de,example-dns9.gwdg.de,example-dns10.gwdg.
de,example-dns11.gwdg.de,example-dns12.gwdg.de --cert-
name EXAMPLE-DNS
```

Bei den Subcommands wie *renew* oder *revoke* am Besten immer die Option *--cert-name* mit angeben, damit certbot weiß, welches Zertifikat verwaltet werden soll.

```
certbot renew --cert-name EXAMPLE-DNS
```

Optional kann Folgendes mit angegeben werden: *--force-renewal* (Erzwingung der erneuten Ausstellung des Zertifikats, obwohl das aktuelle noch gültig ist); *--dry-run* (Testlauf, der nichts

verändert); *--server https://acme.sectigo.com/v2/OV*

```
certbot renew --dry-run --cert-name EXAMPLE-DNS
certbot renew --force-renewal --cert-name EXAMPLE-DNS
certbot revoke --cert-name EXAMPLE-DNS
```

Manuell

Neben der automatisierten Zertifikatbeantragung mittels certbot & Co. können auch manuell Serverzertifikate erstellt werden. Dazu muss Ihnen die den Server verwaltende Person einen mit z. B. openssl erzeugten Certificate Signing Request, kurz CSR, zukommen lassen.

Unter ≡ >Certificates >SSL Certificates rechts auf die Schaltfläche „+“ klicken und den daraufhin erscheinenden, mehrstufigen Dialog bis zum Ende durchlaufen (siehe Abbildung 15).

Mit einem Klick auf die Schaltfläche „Next“ geht es zum nächsten Schritt. Hier werden die Organisation, Department, Zertifikatprofil und externe Beantragende sowie die Systemverwalter*innen, ausgewählt bzw. hinzugefügt. Beim Zertifikatprofil sollten am Besten die OV-Zertifikatprofile „OV SSL“ oder „OV Multi-Domain“ ausgewählt werden. Bei „OV SSL“ können Sie nur genau einen Full Qualified Domain Name, kurz FQDN, im Common Name, kurz CN, des Zertifikats angeben. Bei „OV Multi-Domain“ können Sie noch weitere FQDNs in den Subject Alternative Names, kurz SANs, aufnehmen, unter denen der Server zu erreichen ist (siehe Abbildung 16). Mit einem Klick auf die Schaltfläche „Next“ geht es zum nächsten Schritt weiter.

Hier können Sie den Inhalt der Certificate Signing Requests Datei, kurz CSR, entweder per Drag-and-drop in das Pflicht-Eingabefeld „CSR“ ziehen und ablegen, den Inhalt der Datei in einem Editor markieren, kopieren und in diesem Feld einfügen, oder aber die komplette Datei mit einem Klick auf die Schaltfläche mit dem Pfeil nach oben direkt hochladen. Letztere Methode ist die einfachere und weniger fehleranfällige Variante (siehe Abbildung 17).

Mit dem Klick auf die Schaltfläche „Next“ geht es weiter zum nächsten Schritt. Hier besteht bei dem Zertifikatprofil „OV Multi-Domain“ die Möglichkeit, noch weitere SANs hinzuzufügen, die nicht in der CSR enthalten waren. In diesem Beispiel war in dem CSR nur der SAN *gwdg-c5058.top.gwdg.de* enthalten. Durch Eingabe in das Eingabefeld „Subject Alternative Names“ kann ein Wert eingefügt werden, in dem Beispiel *gwdg-c5058.gwdg.de*, und durch Klick auf das kleine Plus rechts außen hinzugefügt werden. Wenn auf diese Weise alle SANs hinzugefügt worden sind, geht es mit einem Klick auf die Schaltfläche „Next“ weiter zum nächsten Schritt (siehe Abbildung 18).

In diesem abschließenden Schritt kann noch die Zertifikaterneuerung eingeschaltet werden und ab welcher Zeit vor Ablauf des Zertifikats dieser Prozess gestartet wird. Mit einem Klick auf die Schaltfläche „OK“ wird dieser mehrteilige Dialog abgeschlossen (siehe Abbildung 19).

Wenn das Zertifikat final von der CA ausgestellt worden ist, werden der/die Beantragende und der/die angegebene Systemverwaltende über die Ausstellung des Zertifikats per E-Mail benachrichtigt. Diese so oder so ähnliche E-Mail-Vorlage – je nachdem, ob Sie als DRAO diese selber angepasst haben –, sieht wie in Abbildung 20 dargestellt aus.

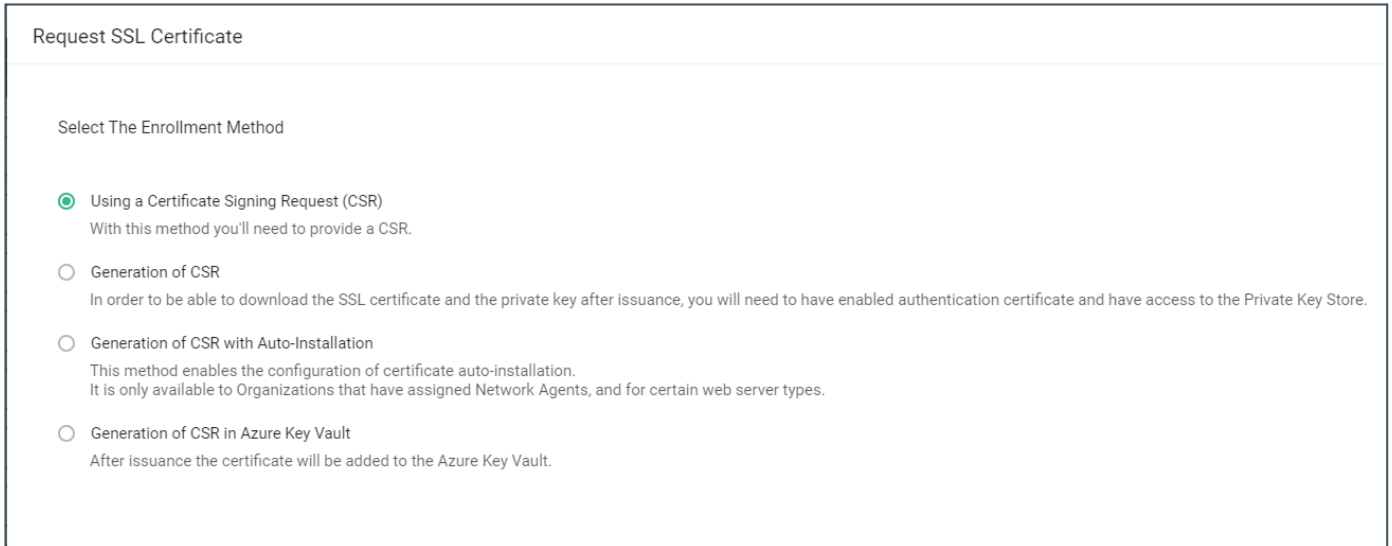


Abb. 15

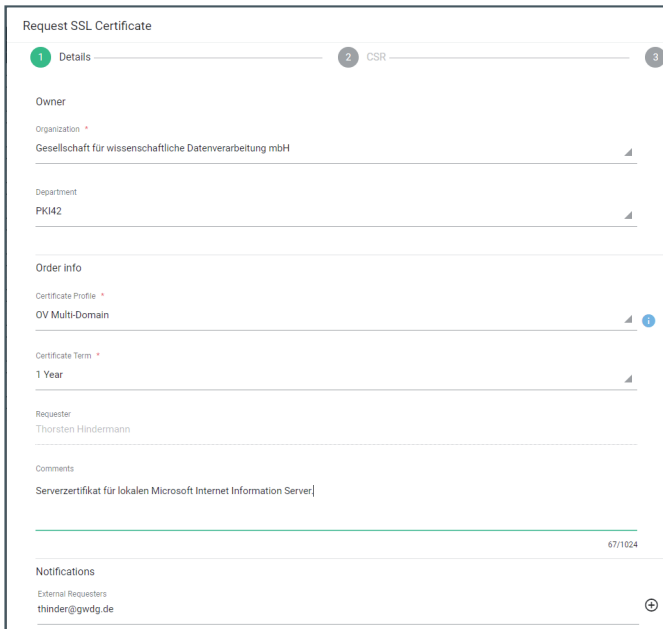


Abb. 16

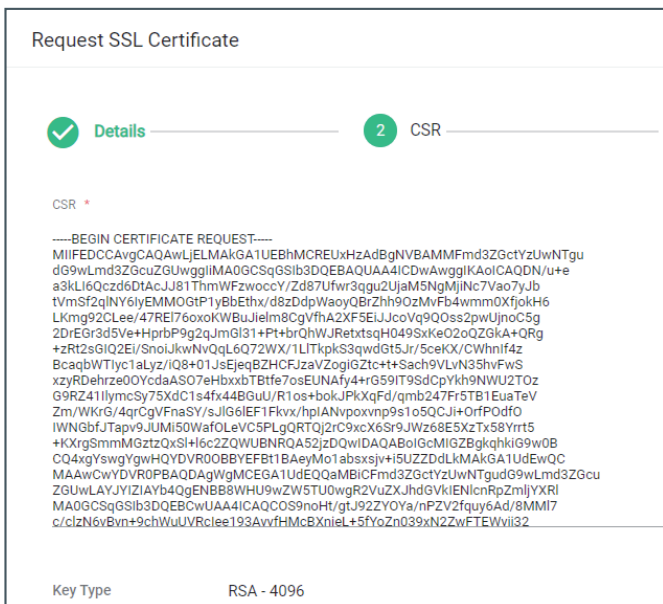


Abb. 17

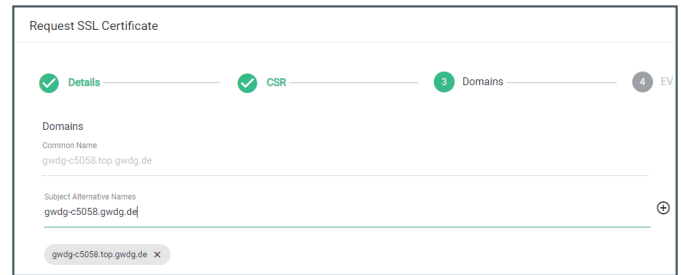


Abb. 18

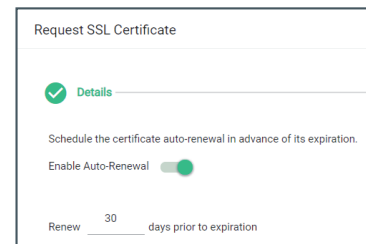


Abb. 19

NUTZERZERTIFIKATE

Für Nutzerzertifikate sind zwei Fälle zu unterscheiden, auf welchem Beantragungsweg das Zertifikat für Nutzer*innen erstellt werden soll:

SSO-Login

Wenn keine (!) Zertifikatwiederherstellung benötigt wird und auch nur eine E-Mail-Adresse im Zertifikat benötigt wird, ist die Zertifikatbeantragung per SSO-Login möglich, wenn der Account des Nutzers bzw. der Nutzerin entsprechend vorbereitet worden ist (siehe die Attribute im früheren Abschnitt „Vorbereitende Schritte für den SSO-Login“).

Ein Nachteil ist: Sie sehen das Zertifikat als DRAO nicht (!) in Ihrem Department. Dieses so beantragten und ausgestellten Zertifikate sehen nur die RAOs der Organisation in deren Ansichten. Der URL für Beantragung von Nutzerzertifikaten mittels SSO-Login ist [9].

Nach der erfolgreichen SSO-Anmeldung bei der Heimatorganisation sieht das Sectigo-Interface für die Nutzer*innen wie in Abbildung 21 dargestellt aus und die dort abgebildeten Einstellungen sollten von Ihnen vorgenommen werden.

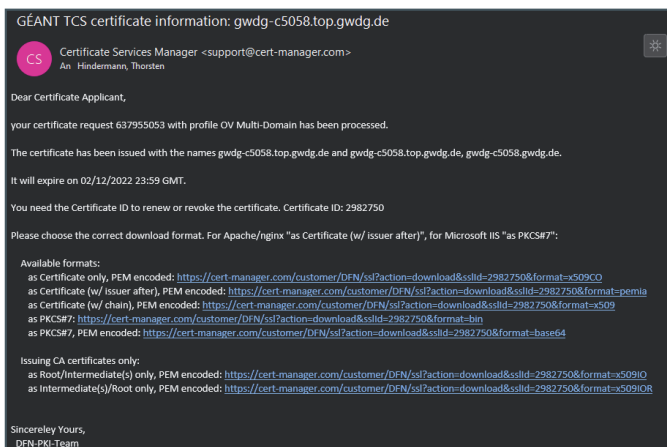


Abb. 20

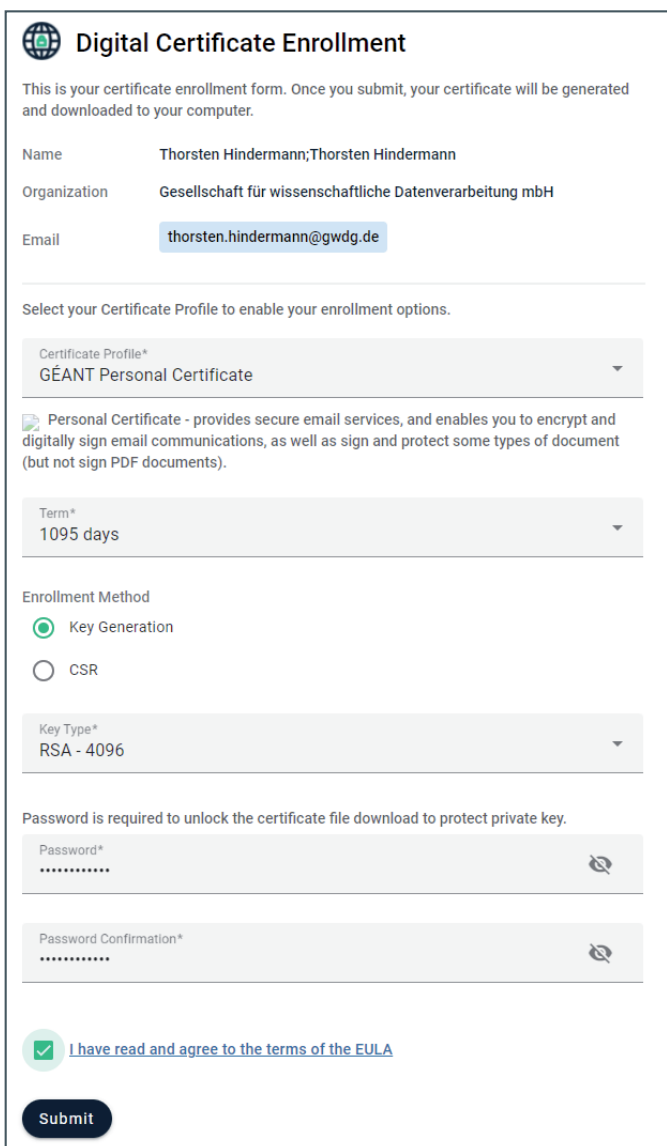


Abb. 21

Hierbei ist es absehbar, dass die Beantragenden eine Begleitung in Form einer guten Dokumentation benötigen. Die optimalen Einstellungen sehen Sie in der Abbildung 21.

Falls diese Art der Zertifikatbeantragung für Nutzer*innen nicht gewollt oder gewünscht ist, gibt es die manuelle Beantragung (siehe den folgenden Abschnitt „Manuell“). Dort geben Sie als DRAO schon für die Nutzer*innen vor, welches die richtigen

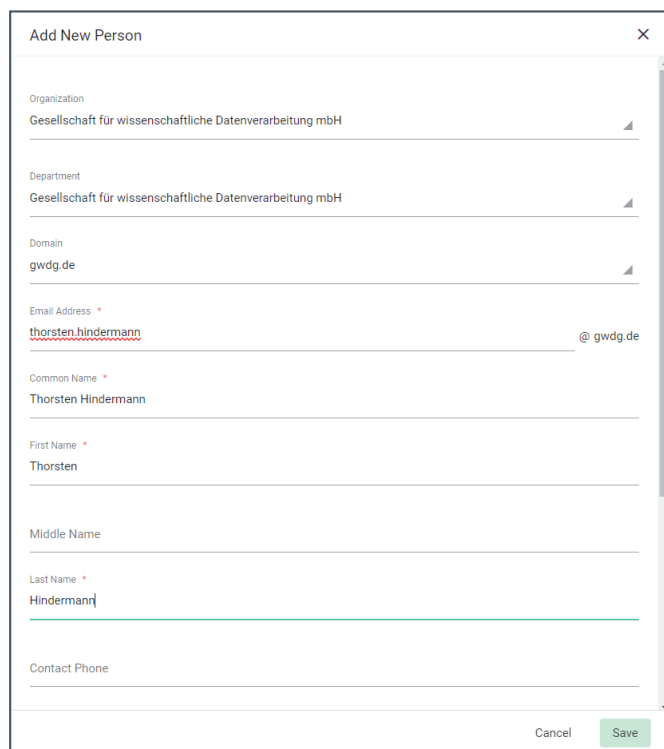


Abb. 22

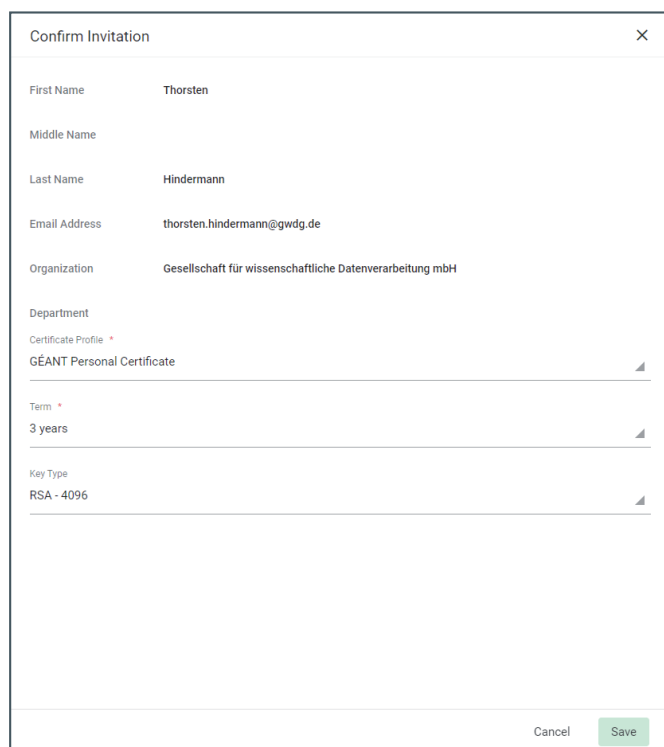


Abb. 23

Einstellungen sind und der/die Nutzer*in muss außer der Passwort-eingabe nichts mehr selber einstellen.

Manuell

Wenn die Zertifikatwiederherstellung benötigt wird und mehr als eine E-Mail-Adresse im Zertifikat vorhanden sein soll, dann sollten Sie als DRAO die entsprechenden Accounts unter ≡ > Persons mit einem Klick auf die Schaltfläche „+“ rechts außen anlegen (siehe Abbildung 22).

Nach dem Anlegen des Accounts diesen dann anklicken und

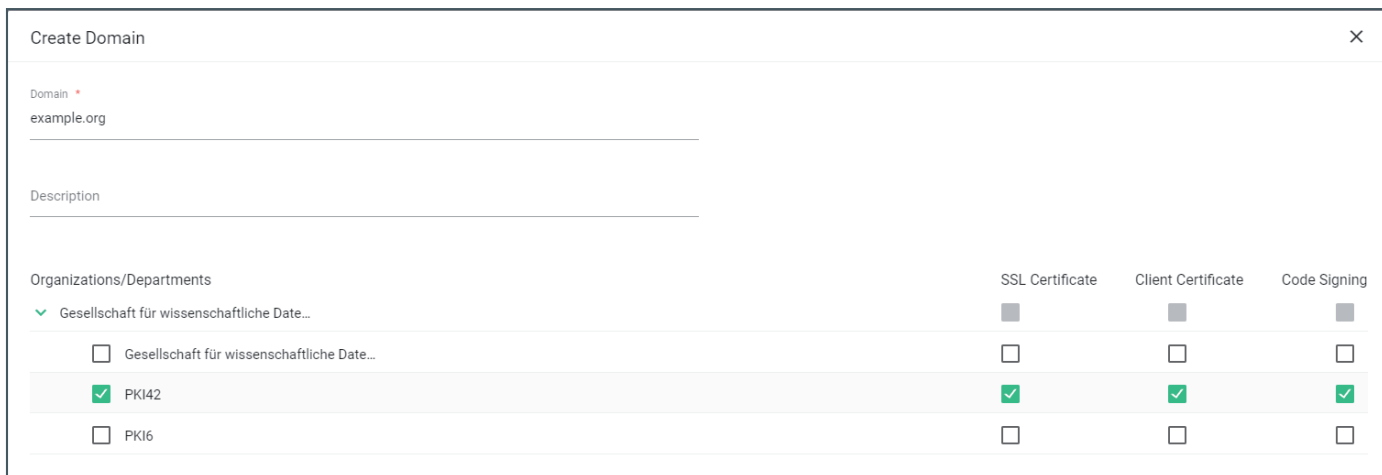


Abb. 24

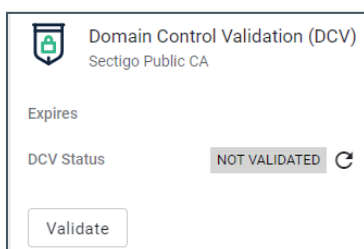


Abb. 25

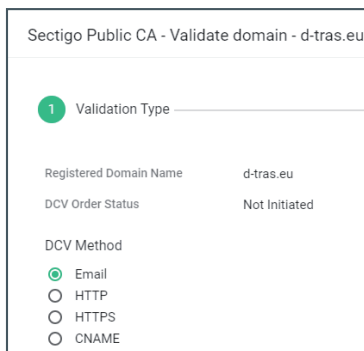


Abb. 26

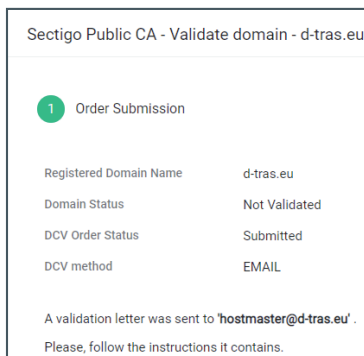


Abb. 28

auf die Schaltfläche „Certificates“ klicken. In dem daraufhin erscheinenden Dialog auf die Schaltfläche „Send Invitation“ klicken. In diesem Dialog geben Sie als DRAO für die Nutzer*innen schon die richtigen Einstellungen für das E-Mail-Zertifikat vor. Mit einem Klick auf die Schaltfläche „Save“ wird eine Einladungse-Mail an den entsprechenden Nutzenden gesendet (siehe Abbildung 23).

Klickt der Nutzende auf den Link in der Einladungse-Mail, wird die Beantragung im Zusammenspiel mit dem Nutzer fertiggestellt. Dieser Vorgang ist nicht Bestandteil dieses GWDG Nachrichten Artikels, sondern wird in einem eigenen GWDG Nachrichtenartikel beschrieben werden. Das so beantragten und vom Nutzenden heruntergeladene Zertifikat sehen Sie als DRAO in Ihren Ansichten in Ihrem Department und können sowohl die Zertifikate als auch die Nutzende selber gut verwalten und haben alles im Überblick.

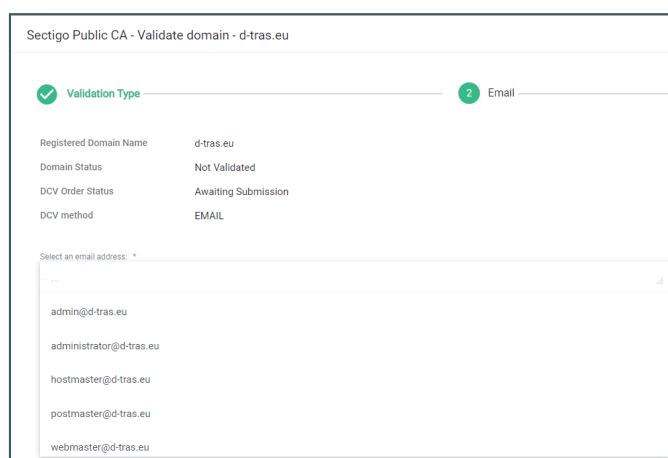


Abb. 27

unterstützt, um E-Mail-Challenges zu versenden, gibt Sectigo nur eine begrenzte Anzahl von Standard-adressen vor. Aber durch zwei weitere Validierungs-Methoden kann dieser Nachteil ausgeglichen werden.

Domänen hinzufügen

Unter ≡ > Domains rechts auf die Schaltfläche „+“ die Hauptdomain, z. B. „example.org“, Ihres Instituts hinzufügen und an Ihr Department „delegieren“. Mit einem Klick auf die Schaltfläche „Save“ diesen Vorgang abschließen. Der DFN-PCA muss diese Delegation manuell bestätigen. Dieser Vorgang kann bis zu einem Tag dauern (siehe Abbildung 24).

Domänen DCV (Validierung)

Nach erfolgreicher Delegation unter ≡ > Domains die Domäne auswählen und auf der rechten Seite in der Gruppe „Domain Control Validation (DCV)“ auf die Schaltfläche „Validate“ klicken, um den DCV-Prozess zu starten (siehe Abbildung 25). Wenn Sie CAA-Records nutzen, so müssen diese bereits in diesem Schritt zum TCS-Anbieter passen: [10]

Erst wenn die Hauptdomain den Zustand „Validated“ anzeigt, fügen Sie auch noch **.<hauptdomain>*, also **.example.org*, hinzu, damit auch FQDNs und Subdomains beantragt werden können. Diese **.<hauptdomain>* erhält automatisch ohne weiteres Zutun der DFN-PCA den Zustand „Validated“.

Hinweis: Solange die Domain nicht den Zustand „Validated“ zeigt, ist keine Zertifikatbeantragung möglich. Der TCS-Anbieter Sectigo führt die Freischaltung automatisch durch, sobald Sie alle

REGISTRIERUNG VON DOMÄNEN

Die Validierung von Domains funktioniert bei Sectigo im Detail etwas anders als beim DFN-Verein. Während der DFN-Verein in seinem PKI-Backend die E-Mail-Adresse aus dem Start of Authority Record, kurz SOA-Record, im DNS zusätzlich zu den Standardadressen *hostmaster@<domain>* und *webmaster@<domain>*

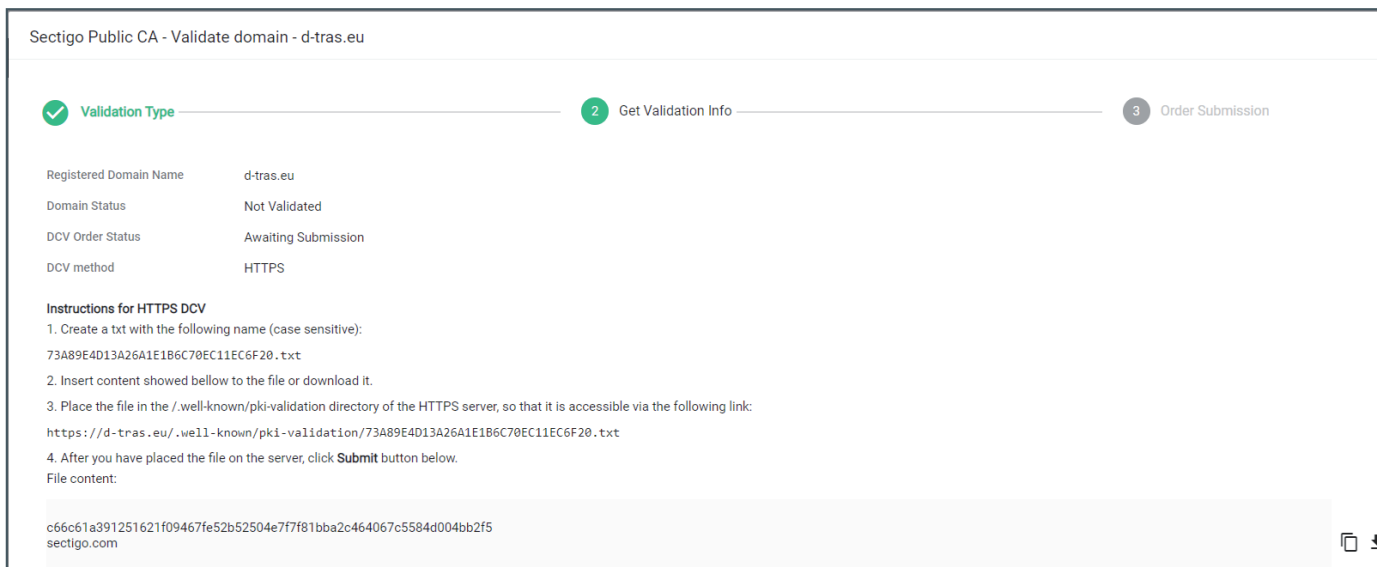


Abb. 29

Schritte der Domainfreischaltung korrekt durchgeführt haben: [11]

Methoden der Domain-Validierung

Sectigo bietet drei Methoden zur Validierung von registrierten Domains an: E-Mail, HTTP(S) und CName (siehe Abbildung 26). Nach Auswahl der DCV-Methode klicken Sie auf die Schaltfläche „Next“, um mit den nächsten Schritten der gewählten Methode fortzufahren.

E-Mail

Wenn eine der angegebenen E-Mail-Adressen für die registrierte Domäne im Domain Name System, kurz DNS, eingetragen ist und auch E-Mails empfangen kann, kann die Validierung sehr einfach mittels einer der vorgegebenen E-Mail-Adressen erfolgen. Nach der Auswahl auf die Schaltfläche „Submit“ klicken (siehe Abbildung 27).

Die E-Mail ist an die ausgewählte E-Mail-Adresse versendet worden und erwartet vom Empfänger, dass die in der E-Mail stehenden Anweisungen befolgt werden (siehe Abbildung 28). Erst danach ist die Domäne erfolgreich validiert.

HTTP(S)

Wenn Sie den Dienst „kontrollieren“, also z. B. die Webseite bei Ihnen im Institut auf einem Webserver betrieben wird, können Sie die registrierte Domäne mittels HTTP(S) validieren. Dazu müssen Sie den angezeigten Anweisungen folgen (siehe Abbildung 29).

Beispielanweisungen für HTTPS DCV

1. Erstellen Sie eine txt-Datei mit dem folgenden Namen (Groß-/Kleinschreibung beachten):
`73A89E4D13A26A1E1B6C70EC11EC6F20.txt`
2. Fügen Sie den unten angezeigten Inhalt in die Datei ein oder laden Sie ihn herunter.
3. Legen Sie die Datei in das Verzeichnis `./well-known/pki-validation` des HTTPS-Servers, so dass sie über folgenden Link erreichbar ist:
`https://d-tras.eu/.well-known/pki-validation/73A89E4D13A26A1E1B6C70EC11EC6F20.txt`

4. Nachdem Sie die Datei auf dem Server abgelegt haben, klicken Sie unten auf die Schaltfläche „Submit“.

Dateiinhalt:

```
c66c61a391251621f09467fe52b52504e7f7f81bba2c-464067c5584d004bb2f5
sectigo.com
```

CNAME

Wenn Sie den DNS-Eintrag bei sich im DNS-Server verwalten, können Sie die registrierte Domäne mittels eines CNAME-Records in Ihrem DNS validieren.

Hier ein Beispiel, wie Sie herausbekommen, wer den DNS-Eintrag der Domäne verwaltet:

```
dig d-tras.eu soa
```

Ergebnis:

```
;; QUESTION SECTION:
;d-tras.eu.      IN  SOA

;; ANSWER SECTION:
d-tras.eu. 60 IN SOA dns1.gwdg.de. hostmaster.gwdg.de.
```

In dem Beispiel für die Domäne `d-tras.eu` ist das `hostmaster@gwdg.de` und der DNS-Server `dns1.gwdg.de`. Somit ist klar, dass dieser DNS-Eintrag von der GWGD verwaltet wird. Für die Validierung muss anschließend den angezeigten Anweisungen auf der Webseite gefolgt werden (siehe Abbildung 30).

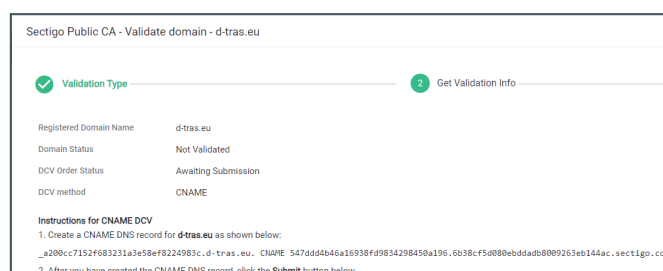


Abb. 30

Beispielanweisungen für CNAME DCV

1. Erstellen Sie einen CNAME-DNS-Eintrag für *d-tras.eu* wie unten gezeigt:
`_a200cc7152f683231a3e58ef8224983c.d-tras.eu. CNAME 547ddd4b46a16938fd9834298450a196.6b38cf5d080ebddadb8009263eb144ac.sectigo.com.`
2. Nachdem Sie den CNAME-DNS-Eintrag erstellt haben, klicken Sie unten auf die Schaltfläche „Submit“.

Automatisierung per Skript

Die Domänenregistrierung und -validierung lässt sich sehr gut mit Hilfe von Skripten durchführen. Wenn Sie selber die Möglichkeit haben, Skripte in Ihrem Institut zu erstellen, empfehlen wir Ihnen die Sectigo-Dokumentation der REST-API unter [12]. Für die eigenen Zwecke hat der Autor des Artikels ein paar einfache PowerShell-Skripte geschrieben, die Interessierten DRAOs gerne zur Verfügung gestellt werden können.

AUTOMATISIERUNG

REST-API-Dokumentation

Die REST-API-Dokumentation kann über [13] abgerufen werden. Hierbei wird eine einzelne HTML-Datei mit den benötigten Informationen auf den lokalen Datenträger heruntergeladen. Diese HTML-Datei wird sehr zeitnah auf die neuesten Versionen des Sectigo Certificate Manager (SCM) aktualisiert, wenn der SCM ein entsprechendes Versions-Update bekommen hat.

WS API only use Account

Für die Automatisierung empfehlen wir Ihnen, einen eigenen Account für genau diesen Zweck anzulegen. Dieser weitere Account ist, wie weiter oben im Artikel beschrieben, anzulegen.

Nach dem Anlegen einmal als diese*r Nutzer*in anmelden und das initiale Kennwort ändern. Da Sie als DRAO den Haken bei „WS API use only“ nicht setzen können, geben Sie uns per E-Mail an gwdg-ca@gwdg.de einen Hinweis. Dann wird der Haken für diesen Account von uns entsprechend gesetzt (siehe Abbildung 31).



Abb. 31

PowerShell-Beispiel-Skripte

An einigen Stellen ist die Bedienung des Sectigo Certificate Managers durch die Ausführung von Skripten besser handhabbar. Die Automatisierung ist mit allen Programmier- und Skriptsprachen möglich, die sich darauf verstehen, mit einer REST-API zu kommunizieren.

In den ersten Versuchen mit dieser REST-API hat der Autor angefangen, die Automatisierung des SCM mit Hilfe von PowerShell Core-Skripten durchzuführen. Die Dokumentation selber hält Beispielaufufe der API mit Hilfe von cURL bereit, ebenfalls ein sehr guter Startpunkt für die Automatisierung.

Für alle Interessierten stellt der Autor diese PowerShell-Skripte unter [14] zu Ihrer Verwendung zur Verfügung. Sie können sie entweder so oder auch als Beispiele für eigene Skripte, zusätzlich zu den cURL-Beispielen in der Sectigo REST-API-Dokumentation, nutzen. Die PowerShell-Skripte sind in der PowerShell Core (Version 7.x und höher) ausführbar und somit lauffähig unter Linux,

macOS und Windows, auf denen Sie eine PowerShell Core installiert haben.

Im Laufe der Zeit werden in diesem git-Repository sicherlich noch weitere Skripte hinzukommen und bestehende Skripte werden fehlerkorrigiert, falls nötig bzw. wenn Sie uns entsprechende Rückmeldungen geben.

ZUSAMMENGEFASSTE TEILNAHMEBEDINGUNGEN AM GÉANT TCS

Durch die Teilnahme an GÉANT TCS verpflichteten Sie sich,

- das TCS Certificate Practice Statement (CPS) einschließlich der dazugehörigen Zusatzdokumente, Practice Statements, Policies und Certificate Terms of Use, die im TCS Repository veröffentlicht sind [15], einzuhalten,
- dass Mitarbeiter*innen des Departments, die mit TCS zu tun haben, die Bedingungen im TCS Certificate Practice Statement (CPS) und den zugehörigen Richtlinien, die im TCS Repository veröffentlicht sind, zur Kenntnis nehmen und einhalten,
- die im TCS CPS beschriebenen Praktiken und Verfahren zu befolgen und in Übereinstimmung mit den Bedingungen, die dem Teilnehmer durch das CPS auferlegt werden, zu handeln und
- TCS-Zertifikate nur für legale und autorisierte Zwecke in Übereinstimmung mit den vorgeschlagenen Verwendungen und Praktiken im TCS CPS zu verwenden.

Dem Department/DRAO ist bekannt, dass an ihn ausgestellte Zertifikate auch sehr kurzfristig durch den DFN-Verein, GÉANT oder den Diensteanbieter (zum Zeitpunkt der Erstellung dieses Artikels Sectigo) gemäß den im TCS CPS einschließlich der dazugehörigen Zusatzdokumente, Practice Statements, Policies und Certificate Terms of Use angegebenen Bedingungen widerrufen werden können.

Der DRAO ist dafür verantwortlich, der GWDC unter gwdg-ca@gwdg.de oder den DFN-Verein zu benachrichtigen, wenn sich zu irgendeinem Zeitpunkt, während ein Zertifikat gültig ist, die ursprünglich eingereichten Informationen seit der Beantragung geändert haben.

WEITERE INFORMATIONEN

DFN

Eine kurze „Erste Schritte“-Anleitung findet sich unter [16], eine Sammlung von vielen Fragen und Antworten – auf Grund der Länge etwas unübersichtlich, aber als weitere Informationsquelle durchaus sehr nützlich –, unter [17].

GÉANT TCS


Eine FAQ-Seite von GÉANT für den TCS ist unter [18] zu finden, ein GÉANT-Wiki mit vielen Informationen rund um den TCS unter [19].

Sectigo

Der URL für den Sectigo Certificate Manager (SCM) für den Mandanten DFN liegt unter [20]. Handbücher für den SCM sind unter [21] zu finden. Die Sectigo-Statusseite liegt unter [22] – über die Subscribe-Schaltfläche (oben rechts) können Sie sich über viele Status der Sectigo-Plattform per E-Mail informieren lassen. Das ist

eine sehr nützliche Funktion, um sich einfach per E-Mail SCM-Status-Informationen zusenden zu lassen. [23] ist Webseite, um Auskunft über vom SCM ausgestellten Serverzertifikate zu erhalten.

LINKS

- [1] <https://cabforum.org/>
- [2] <https://cert-manager.com/customer/DFN>
- [3] <https://testsp3.aai.dfn.de/>
- [4] <https://cert-manager.com/customer/DFN/ssocheck/>
- [5] <https://certbot.eff.org/>
- [6] <https://www.win-acme.com/>
- [7] <https://github.com/acmesh-official/acme.sh>
- [8] <https://acme.sectigo.com/v2/OV>
- [9] <https://cert-manager.com/customer/DFN/idp/clientgeant>
- [10] <https://doku.tid.dfn.de/de:dfnpki:tcsfaq#caa-records>
- [11] https://doku.tid.dfn.de/de:dfnpki:tcsfaq#domainvalidierung_domain_control_validation_dcv
- [12] <https://sectigo.com/knowledge-base/detail/Sectigo-Certificate-Manager-SCM-REST-API/kA01N000000XDkE>
- [13] https://support.sectigo.com/Com_KnowledgeDetailPage?Title=Sectigo@+Certificate+Manager+%28SCM%29+REST+API&Id=kA01N000000XDkE
- [14] <https://gitlab.gwdg.de/pki/geant-tcs/automate/psscripts>
- [15] <https://wiki.geant.org/display/TCSNT/TCS+Repository>
- [16] <https://doku.tid.dfn.de/de:dfnpki:tcsfaq:ersteschritte>
- [17] <https://doku.tid.dfn.de/de:dfnpki:tcsfaq>
- [18] <https://wiki.geant.org/display/TCSNT/TCS+2020+FAQ>
- [19] <https://wiki.geant.org/display/TCSNT/TCS+wiki+%282020%29+Sectigo>
- [20] <https://cert-manager.com/customer/DFN#0>
- [21] https://support.sectigo.com/Com_KnowledgeProductPage?c=Sectigo_Certificate_Manager_SCM
- [22] <https://sectigo.status.io>
- [23] <https://crt.sh/> 

Kurz & knapp

Erreichbarkeit der GWDG um Weihnachten und Neujahr 2021/2022

Die Service-Hotline der GWDG ist vom 24.12. bis zum 26.12.2021 sowie vom 31.12.2021 bis zum 02.01.2022 telefonisch nicht erreichbar. Vom 27.12. bis zum 30.12.2021 ist sie lediglich von 9:00 bis 17:00 Uhr telefonisch erreichbar.

Falls Sie sich an den Tagen, an denen die Service-Hotline telefonisch nicht erreichbar ist, an die GWDG wenden möchten, erstellen Sie bitte eine Anfrage über unsere Support-Webseite unter <https://gwdg.de/support> oder schicken eine E-Mail an support@gwdg.de. Das dahinter befindliche Ticket-System wird auch an diesen Tagen von Mitarbeiter*innen der GWDG regelmäßig überprüft. Wir bitten alle Nutzer*innen, sich darauf einzustellen.

Das Rechenzentrum der GWDG bleibt nach wie vor aufgrund der aktuellen Pandemiesituation bis auf Weiteres geschlossen.

Pohl

DFG fördert neuen Sonderforschungsbereich am Göttingen Campus

Die Deutsche Forschungsgemeinschaft (DFG) fördert ab dem 1. Januar 2022 einen neuen Sonderforschungsbereich (SFB) der Universität Göttingen und ihrer Partner am Göttingen Campus mit dem Titel „Kognition der Interaktion“. Die Förder-summe beträgt rund 12,5 Millionen Euro für zunächst vier Jahre. Neben der Universität sind das Deutsche Primatenzentrum – Leibniz-Institut für Primatenforschung (DPZ), das European Neuroscience Institute Göttingen, das Max-Planck-Institut für Dynamik und Selbstorganisation, die GWDG, das Universitätsklinikum Hamburg-Eppendorf und das Weizmann Institute of

Science in Rehovot, Israel, beteiligt.

Prof. Dr. Philipp Wieder, stellvertretender Leiter der GWDG, leitet in diesem SFB das Teilprojekt INF als Principal Investigator. Mit der Beteiligung am SFB wird zudem die erfolgreiche Arbeit der Göttingen eResearch Alliance fortgesetzt.

Weitere Informationen sind in der Presseinformation Nr. 186 der Universität Göttingen vom 25.11.2021 unter dem URL <https://www.uni-goettingen.de/de/3240.html?id=6493> und in der DFG-Pressemitteilung Nr. 48 vom 25.11.2021 unter dem URL https://www.dfg.de/service/presse/pressemitteilung/2021/pressemitteilung_nr_48/index.html zu finden.

Otto

Kursprogramm der GWDG Academy für das erste Halbjahr 2022

Das Kursprogramm der GWDG Academy für das erste Halbjahr 2022 wurde jetzt unter <https://www.gwdg.de/academy/programme> veröffentlicht. Aufgrund der aktuellen Corona-Situation finden alle Kurse, wie schon in den vergangenen Monaten, in einem geeigneten Online-Format und nicht als Präsenzkurse statt. Nähere Informationen dazu finden Sie bei den jeweiligen Kursen. Sie können sich weiterhin wie gewohnt zu unseren Kursen anmelden. Alle angemeldeten Teilnehmer*innen erhalten rechtzeitig nach Ablauf der Anmeldefrist die erforderlichen technischen Informationen zur Teilnahme an den jeweiligen Kursen.

Otto

Doppelausgabe 01-02/2022 der GWDG-Nachrichten

Die nächsten GWDG-Nachrichten erscheinen wie gewohnt als Doppelausgabe 01-02/2022 ca. Mitte Februar 2022.

Otto



Software und Lizenzverwaltung

DER EINFACHE WEG ZUR SOFTWARE!

Ihre Anforderung

Sie benötigen eine Software, für die es keine von Ihnen nutzbare Rahmenvereinbarung gibt. Die Anzahl der erforderlichen Lizenzen ist nicht genau festgelegt.

Unser Angebot

Wir verfügen über eine Reihe von Rahmen- und Campusvereinbarungen mit namhaften Softwareherstellern und -lieferanten, über die Software auch in geringerer Stückzahl bezogen werden kann. Wir wickeln für Sie die Beschaffung der erforderlichen Lizenzen ab. Wir können uns bei Vertragsverhandlungen und Bedarfsanalysen engagieren. Zugriffslizenzen können auch über Lizenzserver verwaltet werden.

Ihre Vorteile

- > Sie können die benötigte Software in vielen Fällen sofort nutzen.

- > Sie brauchen kein eigenes Ausschreibungs- und Beschaffungsverfahren durchzuführen.
- > Sie ersparen sich die zeitraubenden Verhandlungen mit den Softwareherstellern und -lieferanten.
- > Die Anzahl der benötigten Lizenzen wird Ihnen flexibel zur Verfügung gestellt.
- > Wir können die Nachfrage von verschiedenen Nutzern für neue Lizenzvereinbarungen bündeln.

Interessiert?

Informationen zu bestehenden Lizenzvereinbarungen sind auf der u. g. GWDG-Webseite zu finden. Falls Sie nach spezieller Software suchen, die noch nicht auf unserer Webseite erwähnt ist, kommen Sie bitte auf uns zu. Wir werden prüfen, ob wir eine Vereinbarung abschließen können und bündeln die Nachfrage mit anderen Nutzer*innen.

Stellenangebot

Nr. 20211122

Die GWDG sucht zum nächstmöglichen Zeitpunkt zur Verstärkung des High-Performance-Computing-Teams der Arbeitsgruppe „eScience“ (AG E) drei

Expert*innen (m/w/d) für Deep Learning

mit einer regelmäßigen Wochenarbeitszeit von 39 Stunden. Die Vergütung erfolgt nach dem Tarifvertrag für den öffentlichen Dienst (Bund); die Eingruppierung ist je nach Qualifikation bis zur Entgeltgruppe TVöD E 13 vorgesehen. Die Stellen sind teilzeitgeeignet und zunächst auf zwei Jahre befristet. Die GWDG strebt eine langfristige Zusammenarbeit an. Bei Interesse besteht die Möglichkeit zur Promotion

In 2020 wurde die Universität Göttingen mit der GWDG als eines von acht Rechenzentren in den Verbund Nationales Hochleistungsrechnen (NHR) aufgenommen und betreibt mit dem HLRN-IV-System „Emmy“ einen der leistungsstärksten Rechner der Welt. Des Weiteren wurde in Göttingen das Campus-Institut Data Science (CIDAS) gegründet, mit dem fakultätsübergreifend am gesamten Campus Forschung und Lehre im Bereich Data Science gefördert werden.

Die GWDG betreibt Cluster mit GPU-Systemen und stellt diese ihren Nutzer*innen zur Verfügung. In diesem Kontext ist die Weiterentwicklung der Expertise zu skalierbarer KI auf HPC-Systemen am Standort elementar. Für den Ausbau des KI- und Deep-Learning-Teams suchen wir drei engagierte Mitarbeiter*innen mit einem nachgewiesenen Interesse in den Bereichen Deep Learning, maschinelles Lernen und KI. Sie möchten an der Verknüpfung von Hochleistungsrechnen und Deep Learning mitwirken, interdisziplinär arbeiten, neue Möglichkeiten zur Parallelisierung entwickeln oder Modelle auf maximale Performance im HPC-Bereich optimieren? Dann bewerben Sie sich!

Aufgabenbereiche

- Untersuchung der Skalierbarkeit verschiedener Algorithmen im maschinellen Lernen auf HPC-Systemen und Optimierung
- Entwicklung eigener Forschungsprojekte, Kooperationsprojekte und Services im Bereich maschinelles Lernen und Deep Learning auf HPC-Systemen
- Verbesserung von bestehenden HPC-Workflows und Simulationen durch Integration von KI
- Parallelisierung von Modellen mit Hilfe von GPUs und anderen Beschleunigern
- Unterstützung von Forschenden am Standort Göttingen im Bereich HPC und Deep Learning
- Entwicklung von Workshops an der Schnittstelle

zwischen HPC und maschinellem Lernen

- Unterstützung bei der Beratung der Nutzer*innen zum Thema KI / maschinelles Lernen

Anforderungen

- Abgeschlossenes Hochschulstudium oder vergleichbare Qualifikation mit einschlägiger Berufserfahrung
- Erfahrungen bei der Anwendung von KI-Methoden in der Wissenschaft, bspw. Medizin, Forstwirtschaft, Life Sciences oder Digital Humanities
- Theoretische Kenntnisse im Bereich maschinelles Lernen / Deep Learning / KI
- Erfahrungen bei der Nutzung von HPC-Systemen
- Wünschenswert sind Kenntnisse aus dem Performance Engineering und Erfahrungen in der GPU-Programmierung
- Gute Programmierkenntnisse in Python und anderen relevanten Sprachen
- Gutes analytisches Denkvermögen
- Selbstständige, strukturierte und systematische Arbeitsweise
- Ausgeprägte Team- und Kommunikationsfähigkeit
- Sehr gute Deutsch- und Englischkenntnisse in Wort und Schrift

Unser Angebot

- Flexible Arbeitszeiten und die Möglichkeit zu mobilem Arbeiten
- Ein modernes, vielfältiges und außergewöhnliches Arbeitsumfeld mit großer Nähe zu Wissenschaft und Forschung an der Schnittstelle mehrerer innovativer Technologiesektoren
- Mitarbeit in einem kompetenten und engagierten Team
- Unterstützung bei der Qualifizierung und Weiterentwicklung Ihrer Fähigkeiten
- Sozialleistungen des öffentlichen Dienstes

Die GWDG strebt nach Geschlechtergerechtigkeit und Vielfalt und begrüßt daher Bewerbungen jedes Hintergrunds. Die GWDG ist bemüht, mehr schwerbehinderte Menschen zu beschäftigen. Bewerbungen Schwerbehinderter sind ausdrücklich erwünscht.

Haben wir Ihr Interesse geweckt? Dann bitten wir um eine Bewerbung über unser Online-Formular unter <https://s-lotus.gwdg.de/gwdgdb/age/20211122.nsf/bewerbung>. Das Auswahlverfahren wird in zwei getrennten Verfahren durchgeführt. Beim ersten Auswahlverfahren werden die Bewerbungen berücksichtigt, die **bis zum 03.12.2021** eingehen, beim zweiten Auswahlverfahren dann die Bewerbungen, die nach dem 03.12.2021 und **bis zum 10.01.2022** eingehen.

Fragen zu den ausgeschriebenen Stellen beantwortet Ihnen:

Herr Prof. Dr. Julian Kunkel
E-Mail: julian.kunkel@gwdg.de

NEUE MITARBEITER MOHAMMAD AL NSERAT UND NIELS KENNETH PARKER

Seit dem 1. August 2021 sind Herr Mohammad Al Nserat und Herr Niels Kenneth Parker als studentische Hilfskräfte in der Arbeitsgruppe „Nutzerservice und Betriebsdienste“ (AG H) tätig. Sie unterstützen dort das Team für Microsoft 365 sowie die Supportstellen der studIT im Rahmen des neu geschaffenen Office-365-Angebots für die Studierenden und Beschäftigten der Georg-August-Universität Göttingen. Herr Al Nserat ist per E-Mail unter mohammad.al-nserat@gwdg.de und Herr Parker unter niels.parker@gwdg.de zu erreichen.



Kopp



NEUE MITARBEITER*INNEN TALIA HEIMS UND BASSEL DIB

Seit dem 1. Oktober 2021 bzw. 1. November 2021 verstärken Frau Talia Heims und Herr Bassel Dib das Support-Team im Helpdesk der GWDC als wissenschaftliche bzw. studentische Hilfskraft. Ihre Haupttätigkeiten sind der First-Level-Support, wo sie Anfragen ratsuchender Nutzer*innen entgegennehmen, diesen direkt helfen oder die Anfragen an Kolleg*innen im Second-Level-Support zur weiteren Bearbeitung übergeben. Frau Heims studiert zurzeit an der Georg-August-Universität Göttingen im Fach Kunstgeschichte und Herr Dib im Fach Angewandte Informatik.

HelImvoigt



INFORMATIONEN:
support@gwdg.de
0551 201-1523



Januar bis
Juli 2022

Academy

KURS	DOZENT*IN	TERMIN	ANMELDEN BIS	AE
WORKING WITH GRO.DATA	Király	11.01.2022 10:00 – 11:30 Uhr	10.01.2022	0
ARBEITEN MIT GRO.PLAN	Gnadt	27.01.2022 14:00 – 15:30 Uhr	26.01.2022	0
USING THE GWDG SCIENTIFIC COMPUTE CLUSTER – AN INTRODUCTION	Boden, Khuziyakhmetov	31.01.2022 9:30 – 16:00 Uhr	24.01.2022	4
WORKING WITH GRO.DATA	Király	08.02.2022 10:00 – 11:30 Uhr	07.02.2022	0
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	16.02. – 17.02.2022 9:00 – 12:00 und 13:00 – 15:30 Uhr	09.02.2022	8
XUBUNTU-LINUX: XFCE-DESKTOP ALS ALTERNATIVE ZU POPULÄREN KOMMERZIELLEN BETRIEBSSYSTEMEN	Dr. Heuer	16.02.2022 9:00 – 12:00 und 13:30 – 15:30 Uhr	09.02.2022	4
GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP	Töpfer	22.02. – 23.02.2022 9:30 – 16:00 Uhr	15.02.2022	8
INDESIGN – GRUNDLAGEN	Töpfer	08.03. – 09.03.2022 9:30 – 16:00 Uhr	01.03.2022	8
WORKING WITH GRO.DATA	Király	08.03.2022 10:00 – 11:30 Uhr	01.03.2022	0
ARBEITEN MIT GRO.PLAN	Gnadt	15.03.2022 10:00 – 11:30 Uhr	14.03.2022	0

KURS	DOZENT*IN	TERMIN	ANMELDEN BIS	AE
AWS ACADEMY CLOUD FOUNDATIONS	Sadegh	15.03. – 10.05.2022 jeweils dienstags 14:00 – 15:30 Uhr	08.03.2022	12
STATISTIK MIT R FÜR TEILNEHMER*INNEN MIT VORKENNTNISSEN – VON DER ANALYSE ZUM BERICHT	Cordes	16.03. – 17.03.2022 29:00 – 12:00 und 13:00 – 15:30 Uhr	09.03.2022	8
HIGH PERFORMANCE DATA ANALYTICS – PART I	Dr. Ogaja, Nolte	23.03. – 24.03.2022 9:30 – 16:00 Uhr	16.03.2022	8
WORKING WITH GRO.DATA	Király	12.04.2022 10:00 – 11:30 Uhr	11.04.2022	0
ADMINISTRATION VON WINDOWS-RECHNERN IM ACTIVE DIRECTORY DER GWDC	Quentin	20.04.2022 9:00 – 12:30 und 13:30 – 15:30 Uhr	13.04.2022	4
PRACTICAL COURSE IN HIGH-PERFORMANCE COMPUTING	Prof. Kunkel	25.04. – 29.04.2022 9:00 – 18:00 Uhr	10.04.2022	20
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	27.04. – 28.04.2022 9:00 – 12:00 und 13:00 – 15:30 Uhr	20.04.2022	8
HYBRID IDENTITY – INTEGRATION DES ACTIVE DIRECTORY IN MICROSOFT AZURE ACTIVE DIRECTORY	Kopp	03.05. – 04.05.2022 9:00 – 12:00 und 13:00 – 16:00 Uhr	26.04.2022	8
EINFÜHRUNG IN DIE PROGRAMMIERUNG MIT PYTHON	Zimmer	03.05. – 05.05.2022 9:30 – 16:00 Uhr	26.04.2022	12
ARBEITEN MIT GRO.PLAN	Gnadt	05.05.2022 14:00 – 15:30 Uhr	04.05.2022	0
GRUNDLAGEN DER BILDBEARBEITUNG MIT AFFINITY PHOTO	Töpfer	10.05. – 11.05.2022 9:30 – 16:00 Uhr	03.05.2022	8
WORKING WITH GRO.DATA	Király	10.05.2022 10:00 – 11:30 Uhr	09.05.2022	0
USING THE GWDC SCIENTIFIC COMPUTE CLUSTER – AN INTRODUCTION	Boden, Khuziyakhmetov	16.05.2022 9:30 – 16:00 Uhr	09.05.2022	4
PARALLEL PROGRAMMING WITH MPI	Prof. Haan	17.05. – 18.05.2022 9:15 – 17:00 Uhr	10.05.2022	8
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER*INNEN MIT VORKENNTNISSEN	Cordes	18.05. – 19.05.2022 9:00 – 12:00 und 13:00 – 15:30 Uhr	11.05.2022	8
AWS ACADEMY CLOUD ARCHITECTING	Sadegh	19.05. – 18.08.2022 jeweils donnerstags 14:00 – 15:30 Uhr	12.05.2022	12
PROGRAMMING WITH CUDA – AN INTRODUCTION	Prof. Haan	24.05.2022 9:15 – 17:00 Uhr	17.05.2022	4
AFFINITY PUBLISHER – GRUNDKURS	Töpfer	24.05. – 25.05.2022 9:30 – 16:00 Uhr	17.05.2022	8

KURS	DOZENT*IN	TERMIN	ANMELDEN BIS	AE
INDESIGN GRUNDKURS – SCHWERPUNKT POSTER-GESTALTUNG	Töpfer	01.06. – 02.06.2022 9:30 – 16:00 Uhr	25.05.2022	8
WORKING WITH GRO.DATA	Király	14.06.2022 10:00 – 11:30 Uhr	13.06.2022	0
HIGH PERFORMANCE DATA ANALYTICS – PART II	Dr. Ogaja, Nolte	15.06. – 16.06.2022 9:30 – 16:00 Uhr	08.06.2022	8
ARBEITEN MIT GRO.PLAN	Gnadt	21.06.2022 10:00 – 11:30 Uhr	20.06.2022	0
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	22.06. – 23.06.2022 9:00 – 12:00 und 13:00 – 15:30 Uhr	15.06.2022	8
INDESIGN – AUFBAUKURS	Töpfer	28.06. – 29.06.2022 9:30 – 16:00 Uhr	21.06.2022	8
STATISTIK MIT R FÜR TEILNEHMER*INNEN MIT VOR-KENNTNISSEN – VON DER ANALYSE ZUM BERICHT	Cordes	06.07. – 07.07.2022 29:00 – 12:00 und 13:00 – 15:30 Uhr	29.06.2022	8
WORKING WITH GRO.DATA	Király	12.07.2022 10:00 – 11:30 Uhr	11.07.2022	0

Teilnehmerkreis

Das Angebot der GWDG Academy richtet sich an die Beschäftigten aller Einrichtungen der Universität Göttingen, der Max-Planck-Gesellschaft sowie aus wissenschaftlichen Einrichtungen, die zum erweiterten Kreis der Nutzer*innen der GWDG gehören. Studierende am Göttingen Campus zählen ebenfalls hierzu. Für manche Kurse werden spezielle Kenntnisse vorausgesetzt, die in den jeweiligen Kursbeschreibungen genannt werden.

Anmeldung

Für die Anmeldung zu einem Kurs müssen Sie sich zunächst mit Ihrem Benutzernamen und Passwort im Kundenportal der GWDG (<https://www.gwdg.de>) einloggen. Wenn Sie zum Kreis der berechtigten Nutzer*innen der GWDG gehören und noch keinen GWDG-Account besitzen, können Sie sich im Kundenportal unter dem URL <https://www.gwdg.de/registration> registrieren. Bei Online-Kursen kann das Anmeldeverfahren abweichen. Genauere Informationen dazu finden Sie in der jeweiligen Kursbeschreibung. Einige Online-Angebote stehen Ihnen jederzeit und ohne Anmeldung zur Verfügung.

Absage

Absagen können bis zu sieben Tagen vor Kursbeginn erfolgen. Bei kurzfristigeren Absagen werden allerdings die für den Kurs angesetzten Arbeitseinheiten (AE) vom AE-Kontingent der jeweiligen Einrichtung abgezogen.

Kursorte

Aufgrund der aktuellen Corona-Situation finden zurzeit nahezu alle Kurse in einem geeigneten Online-Format und nicht als Präsenzkurse statt. Nähere Informationen dazu finden Sie bei den jeweiligen Kursen. Auf Wunsch und bei ausreichendem Interesse führen wir auch Kurse vor Ort in einem Institut durch, sofern dort ein geeigneter Raum mit entsprechender Ausstattung zur Verfügung gestellt wird.

Kosten bzw. Gebühren

Die Academy-Kurse sind – wie die meisten anderen Leistungen der GWDG – in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die den Kursen zugrundeliegenden AE werden vom AE-Kontingent der jeweiligen Einrichtung abgezogen. Für alle Einrichtungen der Universität Göttingen und der Max-Planck-Gesellschaft sowie die meisten der wissenschaftlichen Einrichtungen, die zum erweiterten Kreis der Nutzer*innen der GWDG gehören, erfolgt keine Abrechnung in EUR. Dies gilt auch für die Studierenden am Göttingen Campus.

Kontakt und Information

Wenn Sie Fragen zum aktuellen Academy-Kursangebot, zur Kursplanung oder Wünsche nach weiteren Kursthemen haben, schicken Sie bitte eine E-Mail an support@gwdg.de. Falls bei einer ausreichend großen Gruppe Interesse besteht, könnten u. U. auch Kurse angeboten werden, die nicht im aktuellen Kursprogramm enthalten sind.



Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen