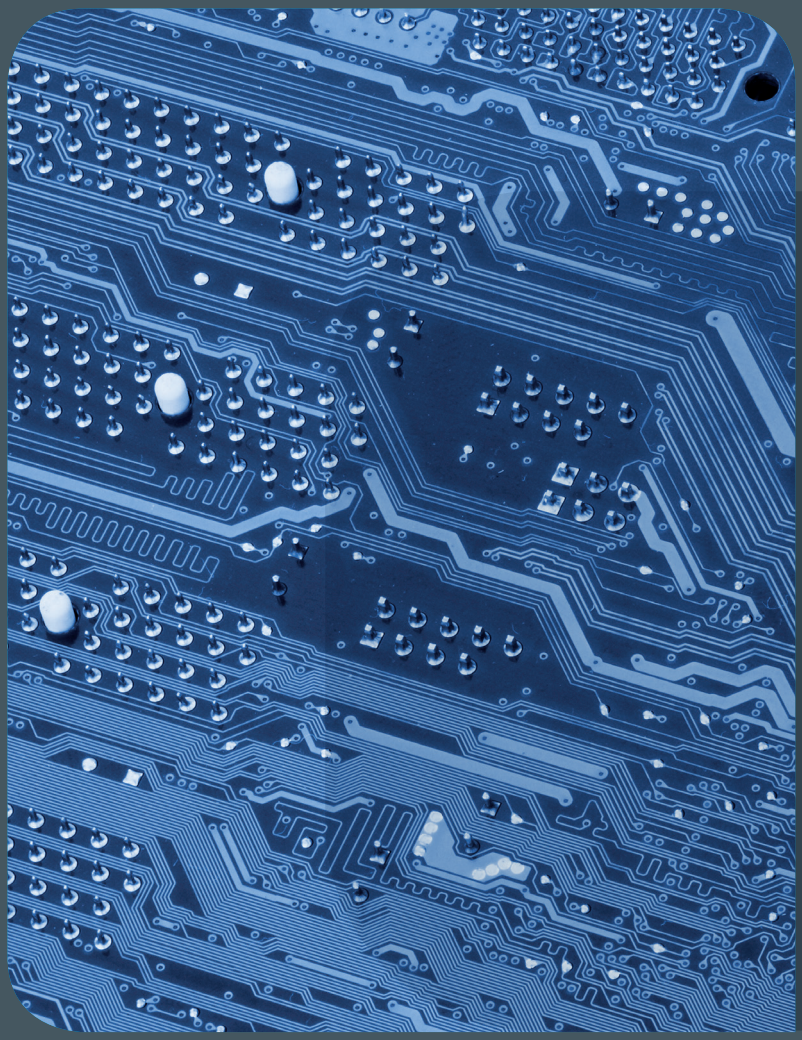
GWDG NACHRICHTEN 12|20

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG



GWDG NACHRICHTEN

12|20 Inhalt

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
43. Jahrgang
Ausgabe 12/2020

Erscheinungsweise:
10 Ausgaben pro Jahr

www.gwdg.de/gwdg-nr

Auflage:
550

Fotos:
© stokkete - stock.adobe.com (1)
© edelweiss - Fotolia.com (5)
© pineapple - Fotolia.com (19)
© pterwort - Fotolia.com (23)
© contrastwerkstatt - Fotolia.com (24)
© Robert Kneschke - Fotolia.com (26)
© MPIbpc-Medienservice (3, 25)
© GWDG (2)

Herausgeber:
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg 11
37077 Göttingen
Tel.: 0551 201-1510
Fax: 0551 201-2150

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,*

wir kommen zum Ende eines ungewöhnlichen Jahres mit diversen Herausforderungen. Normalerweise ist dies die passende Gelegenheit, um einen Blick zurückzuwerfen und das Jahr zusammenzufassen. Dieses Mal spare ich mir dies, da die Meisten sicherlich ausreichend Eindrücke von 2020 gesammelt haben und lieber in die Zukunft schauen. Natürlich hätte es für die GWDG in 2020 durchaus positive Berichtspunkte gegeben, wie das 50-jährige Bestehen der GWDG, die erfolgreiche Beteiligung an der Nationalen Forschungsdateninfrastruktur, die Auswahl als Nationales Hochleistungsrechenzentrum oder die Inbetriebnahme unseres Supercomputers „Emmy". Dennoch wird es auch Zeit, dass das Jahr zu Ende geht und wir den Blick nach vorne richten. Für 2021 stehen die Fertigstellung des ersten Bauabschnittes des Neubaus des gemeinsamen Rechenzentrums und der Umzug dorthin an. Daneben gibt es einige weitere Themen, auf die man gespannt sein kann. Somit schauen wir erwartungsvoll auf die Dinge, die vor uns liegen. Damit wünsche ich Ihnen und Ihren Familien schöne Feiertage und einen guten Start in ein erfolgreiches Jahr 2021 in allerbester Gesundheit.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Neuer Dienst „URL Shortener“

Text und Kontakt:
Stephan Hilker
stephan.hilker@gwdg.de
0551 201-2167
Ralph Krimmel
ralph.krimmel@gwdg.de
0551 201-1821

Auf vielfachen Wunsch bieten wir unseren Nutzer*innen ab sofort unter *https://url.gwdg.de* einen Dienst zur Erstellung von verkürzten Links (URLs) an. Diese dienen dann als Weiterleitung zu einem Internetdienst, einer Webseite oder einer Datei, die häufig einen sehr langen Original-URL besitzen, und lassen sich somit besser in Dokumentationen oder anderen Verweisen einsetzen.

ZIELSETZUNG UND FUNKTIONEN

Zentrales Ziel dieses neuen Dienstes ist es, die Sicherheit und Transparenz bei der Nutzung eines Weiterleitungsdienstes zu erhöhen. Das bedeutet, dass eine Nutzung des Dienstes nur nach Anmeldung mit einem GWDG-Account möglich ist. Außerdem bietet der Dienst die Möglichkeit, vor der Weiterleitung auf den Ziel-URL eine Zwischenseite einzublenden. Diese zeigt dem/der Besucher*in der Webseite den Ziel-URL vor der Weiterleitung an. So ist ein vorheriger Blick auf das Ziel möglich und eine eventuell unerwartete oder unerwünschte Webseite hinter dem Kurz-URL kann erkannt werden. Dies erhöht die Transparenz für jede*n Anwender*in.

Für den zukünftigen Betrieb des URL Shorteners sind bereits erweiterte Funktionen geplant, die durch die notwendige Anmeldung mit einem GWDG-Account möglich werden.

So wird sowohl die Anzeige einer Übersicht der eigenen Kurz-URLs folgen, als auch der Abruf der Anzahl von Besuchen dieser URLs möglich sein. Auch das Editieren von URLs und das Definieren eines Ablaufdatums für einen Kurz-URL sollen folgen.

Zudem ist die Unterstützung weiterer Domains für Kurz-URLs geplant. Dies wird es uns ermöglichen, den Dienst mandantenfähig zu gestalten und auf Domain-Wünsche einzugehen.

GÜLTIGKEIT DER KURZ-URLS

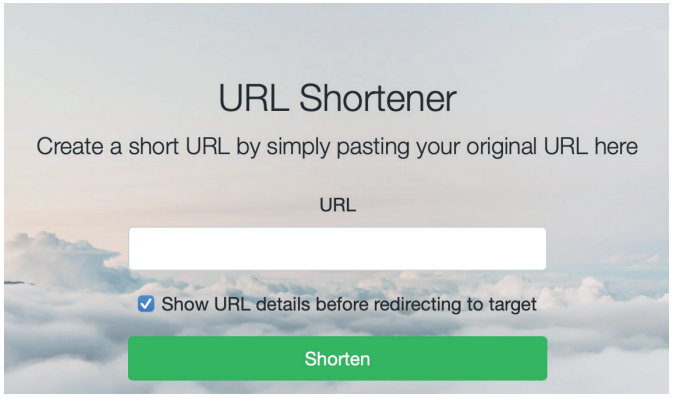
Wir streben eine langfristig gesicherte Auflösung der so erstellten Kurz-URLs an, können hier aber noch keine definierte Garantie abgeben. Wir sichern aktuell eine Auflösung für mindestens zwei Jahre zu und werden hierzu nähere Details kommunizieren, sobald mehr Erfahrungen mit der Softwarelösung vorliegen.

Liegt der Verwendungsbereich von URLs in der Langzeit-Referenzierung von Forschungsdaten oder Publikationen, bieten wir mit dem Dienst „Persistent Identifier“ PIDs nach EPIC oder DOIs bereits als passende Alternativen an.

NUTZUNG

Der neue Dienst „URL Shortener“ kann unter *https://url.gwdg.de* genutzt werden. .Nach der Anmeldung steht dort ein einfaches Web-Interface zur Erstellung eines Kurz-URLs zur Verfügung, das als Eingabe nur den Ziel-URL benötigt (siehe Abbildung 1).

Vor der Erstellung kann die vorausgewählte Einstellung zu Einblendung einer Zwischenseite auf Wunsch bearbeitet werden. Nach Absenden des Formulars wird ein für den Ziel-URL gültiger neuer Kurz-URL angezeigt, der dann entsprechend weiterverwendet werden kann.



1_Web-Interface für die Erstellung eines URLs

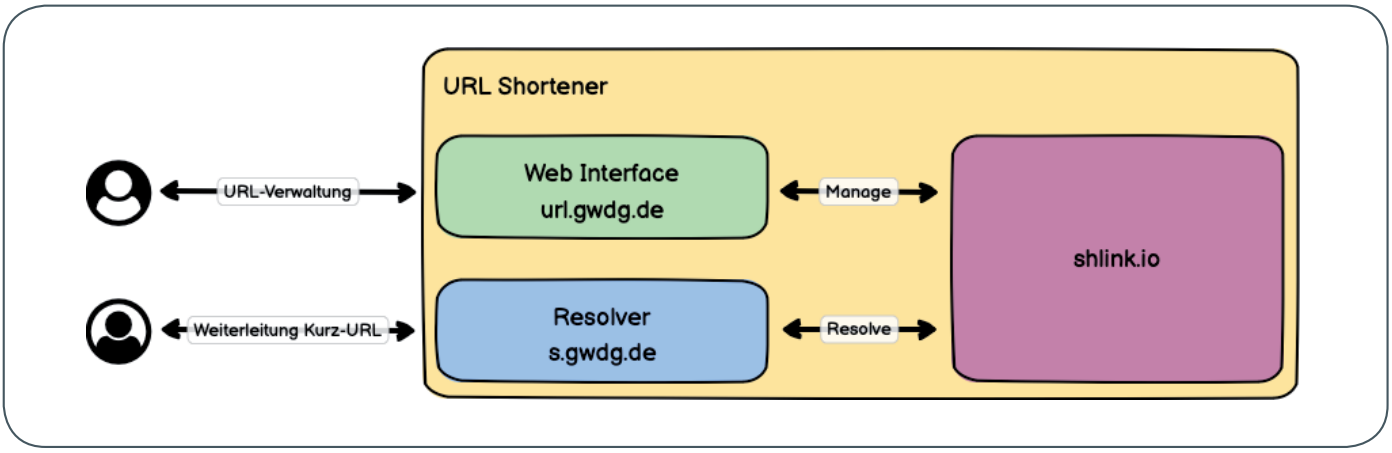
TECHNISCHE DETAILS

Die Architektur des Dienstes ist in Abbildung 2 dargestellt. Die Kurz-URLs und die verknüpften Metadaten werden mithilfe der Software shlink (*https://shlink.io*) gespeichert, die wir auf einem Server in unserem Rechenzentrum betreiben.

Da wir sowohl bei der Umsetzung von Anforderungen als auch bei der Wahl des speichernden Backends flexibel sein wollen, wurden auf Basis der REST-API von shlink die Verwaltung wie auch die Auflösung der URLs selbst in zwei kleinen Web-Applikationen umgesetzt.

New Service URL Shortener

By popular request, *https://url.gwdg.de* now offers our users a service for creating shortened links (URLs). The often very long URLs to a Internet service, website or document are thus available in a short notation. This can be better used in documentation or other references and serves as a redirection. The goal of this new service is to increase security and transparency when using a forwarding service.



2_Architektur des Dienstes „URL Shortener“

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

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?

Jeder Nutzer 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.

>> www.gwdg.de/virtuelle-server

Neue Speicherstrategie für die digitale Langzeitarchivierung mit koala

Text und Kontakt:
Björn Braunschweig
bjoern.braunschweig@gwdg.de
0551 201-2133

Die Speicherstrategie für den Langzeitarchivierungs-Dienst „koala“ hat sich in den letzten Monaten grundlegend verändert. Dieser Artikel stellt die wichtigsten Neuerungen vor, die zu einer verbesserten Leistungsfähigkeit des Dienstes führen.

BISHERIGER STAND

Bisher speicherte koala die Archivdaten klassisch mithilfe eines IBM Spectrum Protect-Servers (vormals TSM-Server) auf Bandspeicher (Tape) und lieferte sie von diesem auch wieder aus. Das Zurückholen von großen, zusammenhängenden Datenmengen ist über Bandlaufwerke effizient möglich. Allerdings ist die gesamte Transferzeit abhängig vom Suchen, Einlegen und Spulen des Bandes an die richtige Stelle, was bei beliebigem Zugriff verteilter Dateien die Transaktion erheblich verlangsamt. Beim Betrieb von koala hat sich gezeigt, dass sich dies erheblich auf die Nutzbarkeit des Dienstes auswirken kann. Eine weitere Schwierigkeit besteht in den vielen Zugriffen und dem dadurch resultierden erhöhten Verschleiss der Bandmedien.

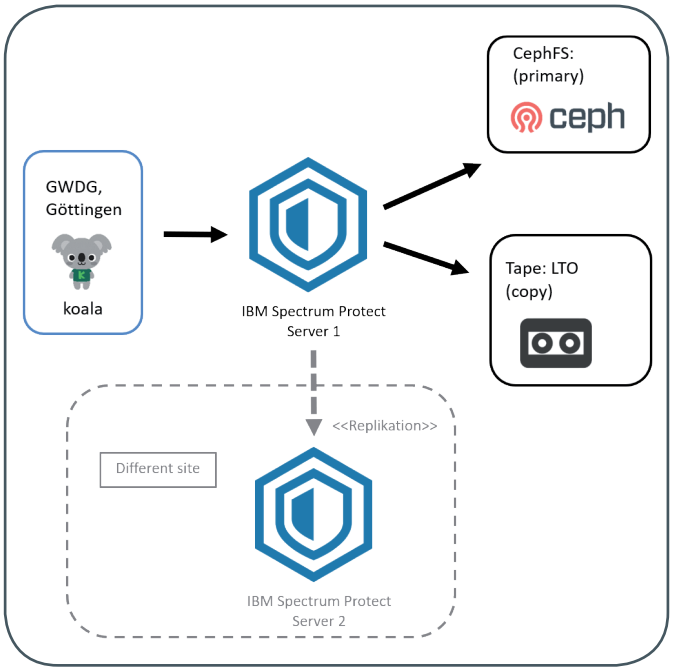
NEUERUNGEN

Mit dem Aufbau von Cloud Speicher in der Form von Ceph Object Storage im Rechenzentrum der GWDG ist ein weiteres, günstiges Massenspeichersystem verfügbar. Durch Kombination dieser Speicherart mit klassischem Tape Storage wird allen oben genannten Problemen wirksam entgegengetreten. Der Zugriff auf das CephFS-Dateisystem verhält sich aus Nutzersicht nicht anders als ein normales Dateisystem. Damit sind Zugriffe auf beliebige Objekte vom Zugriffsverhalten her schneller als beim Bandmedium.

Eine Kombination von CephFS und Bandspeicher ist die ideale Lösung für kostengünstigen und dennoch schnell zugreifbaren Langzeitspeicher mit hoher Datensicherheit durch standortgetrennte Kopien. Die Verwendung mehrerer physischer Medien, in diesem Fall Disk bei CephFS und Band bei IBM Spectrum Protect, ist aus Gesichtspunkten der Langzeitarchivierung (LZA) zusätzlich vorteilhaft.

ARCHITEKTUR

Die neue Architektur stellt sich wie folgt dar (siehe Abbildung 1): Beim „Ingest”, also der Aufnahme von Daten in das Archiv, werden diese zunächst vom Client an koala übergeben. koala spricht nativ mit dem IBM Spectrum Protect-Server (SP). Der



1_Neue koala-Architektur

IBM SP-Server nimmt die Daten entgegen und speichert sie in CephFS. Anschließend wird asynchron mindestens eine Kopie auf Band gesichert. Die Bandkopie liegt räumlich getrennt an einem anderen Standort, um für einen eventuellen Katastrophen-Fall wie z. B. Brandschäden gewappnet zu sein. Bei der Datenrückholung wird nun primär auf die Daten in CephFS zugegriffen, wodurch

New Storage Strategy for koala

In recent months, koala’s storage strategy has changed significantly. The data was saved on tape only. With the availability of a ceph object storage cluster in the GWDG data center, another inexpensive mass storage system is ready to use. Now koala is using ceph and tape in combination to get advantages of both systems: high random access bandwith of ceph and high storage capacity in combination with low cost of tape.

diese schneller als bisher ausgeliefert werden können. Nur im Fehlerfall, wenn beispielsweise die Checksumme einer Datei nicht stimmt (sehr unwahrscheinlich, da Ceph selbst mit Checksummen arbeitet), wird auf die Bandkopie zurückgegriffen.

SIMPLE BLOB STORAGE

Mit Verwendung des CephFS-Speichers ist koala nun in der Lage, Daten „live" auszuliefern, um sie beispielsweise direkt auf einer Webseite anzuzeigen. Außerdem kann das für leichtgewichtigere Anwendungsfälle als vorgeschaltete REST-API zum IBM SP-Server dienen, um die günstige CephFS/Tape-Infrastruktur und Standortredundanz zu nutzen.

Hierfür wurde der „Simple blob storage"-Modus (SBS) entwickelt, der eine einfache REST-API für den Up- und Download zur Verfügung stellt (siehe das Beispiel in Abbildung 2).

```
user@host ~: curl -X POST --data-binary @"myfile" \
--user user:pw https://koala.gwdg.de/api/sbs
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 61

{"internal_asset_id":
"63b54de9-dc2b-4bff-be28-e2ad92d02b5c"}
```

2_Beispiel für den Upload einer Datei bei Nutzung des SBS-Modus

AUSBLICK

Bisher noch nicht umgesetzt, aber in Planung, ist die zusätzliche „Replikation" in einen weiteren IBM SP-Server. Hierbei werden die komplette Inventardatenbank und jegliche Datenbestände des IBM SP-Servers in einem weiteren sogenannten „Repl-Server" abgelegt. koala ist in der Lage, bei Ausfall des primären IBM SP-Servers transparent auf diesen auszuweichen (vergleiche hierzu den ausgegrauten Bereich in Abbildung 1). Es erhöhen sich somit nochmals die Redundanz wie auch die Verfügbarkeit. Dies erhöht zudem die Datensicherheit noch über die reine Speicherung zusätzlicher Kopien hinaus, da neben den Rohdaten eine zweite Serverinstanz mit Inventar- und Metadaten des Archivs zur Verfügung steht und bei einem Ausfall die Annahme und Auslieferung von Daten direkt übernehmen kann.

WEITERE INFORMATIONEN

[1] GWDG-Projektseite: *https://www.gwdg.de/research-education/projects/koala*

[2] koala-Dokumentation: *https://koala-docs.gwdg.de/*

[3] Braunschweig, Björn: Digitale Langzeitarchivierung für die Deutsche Nationalbibliothek. In: GWDG-Nachrichten 9-10/2015, Seite 16 ff.; *https://www.gwdg.de/documents/20182/27257/GN_09-10-2015_www.pdf*

[4] Braunschweig, Björn: koala – neue Plattform zur Digitalen Langzeitarchivierung für die Deutsche Nationalbibliothek. In: GWDG-Nachrichten 7/2018, Seite 15 ff.; *https://www.gwdg.de/documents/20182/27257/GN_7-2018_www.pdf*

[5] DNB-LZA: *https://www.dnb.de/EN/Professionell/Erhalten/LZA-System/lza-system_node.html*

[6] Bildnachweis koala-Logo: © aratehortua - fotolia.com

[7] Bildnachweis Tape-Icon: *https://www.shareicon.net/author/ual-pharm*

Kurz & knapp

Erreichbarkeit der GWDG um Weihnachten und Neujahr 2020/2021

Die Service-Hotline der GWDG ist vom 24.12. bis zum 27.12.2020 sowie vom 31.12.2020 bis zum 03.01.2021 telefonisch nicht erreichbar. Vom 28.12. bis zum 30.12.2020 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://www.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

Kursprogramm der GWDG Academy für das erste Halbjahr 2021

Das Kursprogramm der GWDG Academy für das erste Halbjahr 2021 wurde jetzt unter *https://www.gwdg.de/academy/programme* veröffentlicht. Aufgrund der aktuellen Corona-Situation finden nahezu 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 01-02/2021 der GWDG-Nachrichten

Die nächsten GWDG-Nachrichten erscheinen wie gewohnt als Doppelausgabe 01-02/2021 Mitte Februar 2021.

Otto

Dotfiles per Git Repository

Text und Kontakt:
Kai Germershausen
kai.germershausen@gwdg.de
0551 201-1891

In diesem Artikel stellen wir eine elegante und effektive Möglichkeit vor, persönliche Konfigurationseinstellungen auf mehreren Systemen bereitzustellen. Die Anleitung richtet sich an Fortgeschrittene mit Grundkenntnissen in Git (Versionskontrolle) und der Linux-Kommandozeile (Shell).

AUSGANGSLAGE UND VORAUSSETZUNGEN

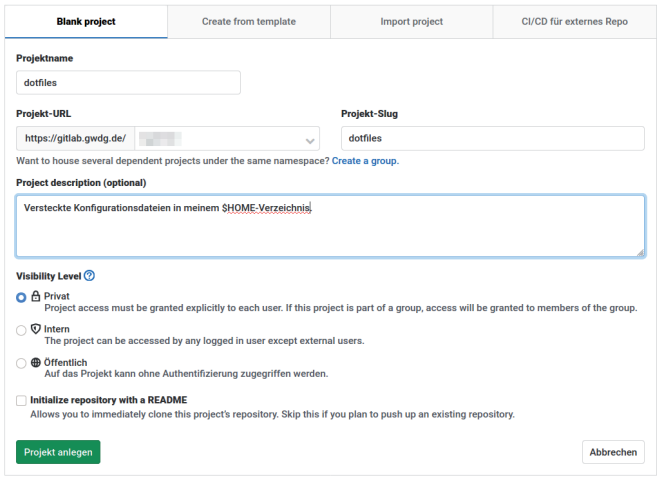
Als Nutzer*in kennen Sie vielleicht folgendes Problem: Sie haben auf Ihrem Host alle Konfigurationseinstellungen für ein bestimmtes Tool oder eine Anwendung vorgenommen und möchten diese Anpassungen nun ggfs. ohne große Umwege auch auf anderen Systemen nutzen. Um Ihnen das lästige Hin-und-Her-Kopieren zu ersparen und nebenbei noch das Problem unterschiedlicher Versionen zu vermeiden, greifen wir für diesen Zweck auf die Nutzung des GitLab-Dienstes der GWDG zurück. Hierbei gehen wir von folgenden Voraussetzungen aus:

- Es handelt sich um ein Linux/UNIX-System.
- OpenSSH und public/private keys liegen vor.
- Für die Versionskontrolle kommt Git zum Einsatz.

VORBEREITUNG

Als ersten Schritt benötigen wir für unsere „dotfiles" ein passendes Git Repository. Dies soll uns bei der verteilten Verwaltung der Konfigurationsdateien und deren Änderungen helfen.

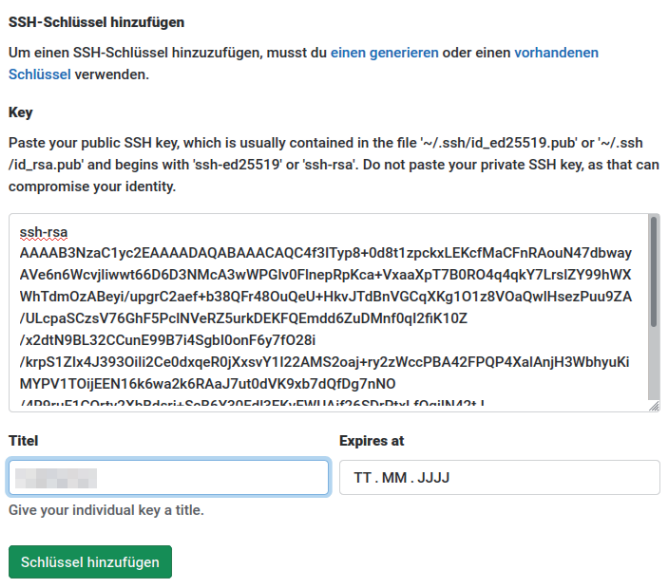
Melden Sie sich dazu bitte bei unserem GitLab-Dienst an (*https://gitlab.gwdg.de/*) und erstellen ein „Neues Projekt" mit dem treffenden Namen „dotfiles". Lassen Sie die Sicherheitseinstellungen auf „Privat" und legen ein leeres Repository ohne README an (siehe Abbildung 1).



1_Erstellen eines neuen GitLab-Projektes

Hinweis: Manche Konfigurationsdateien könnten vertrauliche Inhalte und Passwörter enthalten, weshalb nachdrücklich davon abgeraten wird, die Sichtbarkeit zu erhöhen oder solche Dateien zur Verteilung in der Versionskontrolle einzuchecken.

Falls Sie bislang noch keinen „public key" (SSH) in Ihrem GitLab-Profil hinterlegt haben, holen Sie dies jetzt bitte nach (siehe Abbildung 2): *https://gitlab.gwdg.de/-/profile/keys*



2_Hinzufügen eines SSH-Schlüssels

Damit sollten die Anforderungen erfüllt sein, per *ssh* auf Ihre Projekte zugreifen zu können.

Fahren Sie jetzt mit der Grundkonfiguration von Git auf Ihrem System fort, sofern dies noch nicht geschehen ist:

```
git config --global user.name "fmuster"
git config --global user.email "fred.mustermann@gwdg.de"
```

INITIALISIERUNG

Jetzt kann es endlich losgehen! Klonen Sie zuerst Ihr „dotfiles"-Projekt auf Ihr lokales System:

```
git clone --bare git@gitlab.gwdg.de:fmuster/dotfiles.git \
$HOME/.dotfiles
```

Dotfiles per Git Repository

Ever wondered how to manage and distribute your configuration files between several systems effectively? Well, we got you covered. This article has an efficient method for you.

Hinweis: Sie müssen hierzu den Beispielaccount *fmuster* durch Ihren eigenen Nutzernamen ersetzen. Wichtig ist hier der Parameter *--bare*, da wir eine besondere Art eines lokalen Repository erzeugen wollen.

Um komfortabel und exklusiv mit unseren „dotfiles" arbeiten zu können, hinterlegen wir nun einen gleichlautenden Alias für *git* zur Interaktion in unserem System:

```
alias dotfiles='/usr/bin/git --git-dir=$HOME/.dotfiles/ \
--work-tree=$HOME'
echo "alias dotfiles='/usr/bin/git --git-dir=$HOME/.dotfiles/ \
--work-tree=$HOME'" >> $HOME/.bashrc
```

Damit unser *git*-Alias *dotfiles* bei der Verwendung ausschließlich Dateien auflistet, die wir explizit festlegen, setzen wir hierfür einen entsprechenden Parameter mit folgendem Befehl:

```
dotfiles config --local status.showUntrackedFiles no
```

Außerdem möchten wir, dass unser neues Kommando das eigene lokale *.dotfiles*-Verzeichnis in unserem *$HOME* komplett ignoriert:

```
echo ".dotfiles" >> .gitignore
```

WORKFLOW

Ab hier können wir nun analog zu *git* mit dem Kommando *dotfiles <Parameter>* Dateien einchecken und committen:

```
dotfiles status
dotfiles add ~/.bashrc
dotfiles status
dotfiles commit
dotfiles status
```

Der wiederkehrende Aufruf von *status* dient hier nur dem besseren Verständnis der einzelnen Schritte.

Nun gilt es noch, einmalig das zentrale GitLab-„dotfiles"-Repository als Master zu deklarieren, damit anschließend der Up- und Download per *push* und *pull* gewährleistet ist:

```
dotfiles push --set-upstream origin master
```

```
dotfiles push
```

Was sind eigentlich Dotfiles?

Dotfiles nennt man die Dateien im *$HOME*-Verzeichnis des/der Nutzer*in, welche durch einem vorangestelltem Punkt (englisch: dot) als versteckt markiert sind. Meist handelt es sich dabei um Konfigurationsdateien, welche die persönlichen Einstellungen eingesetzter Kommandozeilentools beinhalten. Die *.bashrc* (Konfigurationseinstellungen der BASH) ist beispielsweise so eine Datei.

Von hier an können ab jetzt künftige Änderungen an den Master geschickt werden und somit lokale Anpassungen zentral gesichert wie auch bei Bedarf auf andere Systeme verteilt werden.

Um Ihre Konfigurationsdateien auch auf anderen Hosts nutzen zu können, wiederholen Sie bitte die entsprechenden Abschnitte dieser Anleitung auf dem neuen System. Denken Sie daran, dass dort ebenfalls passende SSH-Keys für Ihr GitLab-Profil hinterlegt sind.

Bei Versionskonflikten durch bereits bestehende Konfigurationsdateien auf dem neuen Zielsystem lösen Sie diese je nach Wunsch (*replace*, *diff* etc.) nach jeweiliger Git-Manier, aber mit dem Kommando *dotfiles* als unserem dediziertem *git*-Alias für diese Methode.

Hinweis: Sollten Sie unsicher im Umgang mit Git sein, machen Sie sich bitte zuerst ausreichend mit dieser Software vertraut. Stellen Sie grundsätzlich sicher, ein funktionierendes Backup Ihrer wichtigen Daten zu haben.

Das in diesem Artikel beschriebene Verfahren wird hauptsächlich zum Austausch von Konfigurationen unter ähnlichen, im Idealfall auch versionsgleichen Betriebssystemen empfohlen, da in einzelnen Fällen ggfs. manche darin enthaltene Parameter sonst nicht zu gleichen Ergebnissen führen können. Oft stellt dies aber kein Problem dar.

Weiterführende Informationen der vorgestellten Methode und zum Umgang mit Git finden Sie in den folgenden Quellenangaben.

QUELLEN

https://www.atlassian.com/git/tutorials/dotfiles
https://www.atlassian.com/git/tutorials
https://githowto.com/

Einsatzmöglichkeiten von X.509-Zertifikaten – Teil 2: Ein Blick hinter die Kulissen eines Teilnehmerservices

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

Dieser Artikel soll einen Einblick in die Tätigkeiten der Teilnehmerservice-Mitarbeiter*innen (TS-MA) geben und die Abläufe nach dem Eingang eines Zertifikatantrags bei der Registration Authority (RA) darstellen. Das ist das Kerngeschäft der TS-MA in den RAs. Zur Unterstützung dieser Aufgaben rund um den RA-Betrieb stellt der DFN-Verein den TS-MA das auf Java basierende Programm GUIRA zur Verfügung. Schauen wir also gemeinsam einmal hinter die Kulissen einer RA.

EINRICHTUNG EINER RA

Es gibt nur wenige Voraussetzungen, die für die Einrichtung einer RA erfüllt werden müssen. Als erstes braucht es mindestens zwei Kolleg*innen, optimal wären drei. So ist auf alle Fälle der Vertretungsfall im Urlaub und/oder Krankheit geregelt, so dass im besten Fall immer ein TS-MA da ist und aktiv werden kann. Jeder TS-MA verfügt über einen Rechner, auf dem Java installiert werden kann und darf.

Sind diese Voraussetzungen erfüllt, ist zu klären, ob es schon eine RA im Institut gibt. Ob das eigene Institut oder gar eine Fakultät eine RA hat, kann auf den Webseiten für die Universität Göttingen [1] und für die Max-Planck-Institute [2] nachgesehen werden.

Ist im eigenen Institut noch keine RA vorhanden, schreiben Sie bitte eine E-Mail an eine der E-Mail-Adressen *gwdg-ca@gwdg.de*, *gwdg-ca@uni-goettingen.de* oder *mpg-ca@mpg.de* mit der Anfrage, eine RA für Ihr Institut zu beantragen. Daraufhin wird der Autor dieses Artikels in seiner Funktion als sogenannte handlungsberechtigte Person im PKI-Bereich des DFN-Vereins und im Abwesenheitsfall seine Stellvertretung Kontakt mit Ihnen aufnehmen und die weiteren Schritte zur Einrichtung einer RA klären bzw. Sie auf den Weg hin zu einer RA für Ihr Institut begleiten. Aber auch nach Einrichtung der RA steht der Autor gerne bei weiteren Fragen zum RA-Betrieb und zu Zertifikaten zur Verfügung.

Im Folgenden werden die Schritte zu einer RA im eigenen Institut, wenn noch nicht vorhanden, beschrieben. Die zugehörigen Formulare werden vom Autor nach der entsprechenden Anfrage per E-Mail an die zukünftigen TS-MA gesendet. Es muss das Teilnahmeformular ausgefüllt und vom Geschäftsführenden Direktor des Instituts unterschrieben werden. Die zukünftigen TS-MA füllen, jeder einzeln für sich, ein Teilnehmerserviceformular aus und unterschreiben dieses. Diese Formulare am besten einscannen und als PDF-Datei an eine der oben genannten E-Mail-Adressen senden. Daraufhin findet eine persönliche Identifizierung per VideoIDent statt. Das Verfahren und der Vorgang werden an späterer Stelle genauer beschrieben. Der Autor dieses Artikels notiert noch Informationen auf die Formulare für den DFN-Verein und sendet die PDF-Dateien dorthin. Nach ca. drei Wochen ist dann die RA eingerichtet. Nun nimmt der Autor des Artikels wieder Kontakt mit den angehenden TS-MA auf und bitte diese, in der neu erstellten RA für das Institut einen Zertifikatantrag [3] zu stellen. Am Ende dieses Antragsverfahrens kommt eine PDF-Datei heraus. Diese bitte unterschreiben und wieder eingescannt als PDF-Datei an eine der oben angegebenen E-Mail-Adressen senden. Wichtig ist hierbei, dass im Namenfeld für das Zertifikat folgende Notation/Syntax eingehalten wird (siehe Abbildung 1):

PN: <Vorname> <Nachname> - Teilnehmerservice <Instituts-name oder gängige Abkürzung>

Nach dem Eintrag von Informationen für den DFN-Verein werden diese Anträge zum DFN-Verein gesendet und dort final

Possible Applications of X.509 Certificates – Part 2: The Tasks of a Registration Authority

This article is intended to give an insight into the activities of the participant service staff (TS-MA) and to describe the processes after a certificate application has been received by the Registration Authority (RA). This is the core business of the TS-MA in the RAs. To support these tasks around the RA operation, the DFN-Verein provides the TS-MA with the Java-based program GUIRA. So let's take a look behind the scenes of an RA.

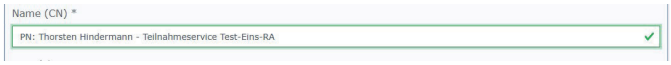


Abb. 1

bearbeitet und genehmigt. Eine E-Mail über die Ausstellung des TS-MA-Zertifikats erreicht den zukünftigen TS-MA. Dieses Zertifikat kann wie unter [4] beschrieben fertiggestellt werden. Die Datei, die das fertige Zertifikat enthält, hat in den allermeisten Fällen die Dateiendung *.p12*, in ganz seltenen Fällen *.pfx*. Inhaltlich sind beide Dateien gleich und sind im wahrsten Sinne des Wortes der Schlüssel für die zu verwaltende RA. Die RA wird mit dem Programm GUIRA verwaltet, dass im nächsten Abschnitt vorgestellt wird.

VERWALTUNG DER RA MIT GUIRA

Zur Bewältigung der Aufgaben des RA-Betriebs hat der DFN-Verein das auf Java basierende Programm GUIRA entwickelt. Dieses Programm wird vom DFN gepflegt und weiterentwickelt. Systemvoraussetzungen sind ein PC oder Laptop und die Installation von OpenJDK. OpenJDK kann z. B. unter [5] heruntergeladen werden. Die Informationen zum Herunterladen des Programms GUIRA für RA-Tätigkeiten finden Sie unter [6].

Es ist wichtig, das OpenJDK installiert wird. Der DFN-Verein hat aufgrund der Schwierigkeiten mit der Lizenzierung von Oracle Java das Programm GUIRA OpenJDK-kompatibel gemacht.

Nach dem Herunterladen und Aufruf durch das entsprechenden Start-Skript, das für Windows, Linux und macOS im Installationsordner zur Verfügung steht, wird das Programm GUIRA gestartet.

Beim allerersten Start wird nach einem TS-MA-Zertifikat (siehe oben) gefragt, damit die RA des Instituts im Programm angezeigt und verwaltet werden kann. Die Ermittlung der entsprechenden RA erfolgt aus den Angaben im TS-MA-Zertifikat des zugehörigen TS-MA. Nach diesem initialen Einrichtungsschritt können die RA und der TS-MA ihren Betrieb bzw. ihre Tätigkeit aufnehmen und die RA verwalten sowie eingegangene Zertifikatanträge bearbeiten und, wenn die Voraussetzungen erfüllt sind, genehmigen (siehe Abbildung 2; da der Autor dieses Artikels Hauptverwalter von mehreren RAs ist, sind im linken Navigationsbereich mehrere Einträge zu sehen). Diese Tätigkeiten werden wir nun genauer betrachten.

TÄTIGKEITEN EINER RA

Persönliche Identifizierung

Voraussetzungen

Seit dem 24.04.2020 hat der DFN-Verein das Video-Identifizierungverfahren freigegeben. Somit können die MPG-, Uni-Göttingen- und GWDG-CA (Zertifizierungs-Autoritäten, engl. Certificate Authorities, kurz CAs) sowie deren RAs (Registrierungs-Autoritäten, engl. Registration Authorities, kurz RAs) in Zeiten der Corona-Pandemie die persönliche Identifizierung von Antragsteller*innen von Nutzerzertifikaten durchführen – das Ganze im Sinne der sozialen Distanzierung per Video-Chat oder -Konferenzsystem. Voraussetzung ist, dass die TS-MA sich selbst geschult haben. Dies ist entsprechend zu dokumentieren.

Weiterhin sollten sich die TS-MA im DFNconf [7] einen Meetingraum anlegen, um eine mögliche Video-Identifizierung mit einem Zertifikatnehmer durchführen zu können. Darüber hinaus können Video-Chat oder -Konferenzsysteme, die innerhalb der Einrichtung dienstlich bereitgestellt werden, zum Einsatz kommen. Weitere Details dazu sind in der Richtlinie „Video-Identifizierung in der DFN-PKI“ zu finden [8]. Die benötigten Informationen für die Selbstschulung liegen in Form von PDF-Dateien und einem Schulungsvideo unter [9] vor.

Durchführung

Wenn eine Video-Identifizierung durchgeführt werden soll, muss als erstes die vom Zertifikatnehmer nach der Beantragung des Zertifikats ausgedruckte Antrags-PDF-Datei unterschrieben und dem TS-MA zugesendet werden. Hat der TS-MA dieses Formular erhalten, nimmt er Kontakt mit dem Zertifikatnehmer auf, fragt, mit welchem Ausweisdokument sich der Zertifikatnehmer identifizieren möchte, und vereinbart dann einen Termin für die Video-Identifizierung mit ihm. Praktischerweise enthält der angelegte Meetingraum Textvorlagen in Deutsch und in Englisch mit Informationen, wie der Zertifikatnehmer dieser Video-Identifizierung beitreten kann.

Wenn diese Identifizierung per DFNconf zustande kommt, sollten sich sowohl der TS-MA als auch der Zertifikatnehmer jeweils alleine in einem möglichst geschlossenen Raum befinden. Der Identifizierungsvorgang muss dann in einem Stück durchgeführt werden und darf nicht unterbrochen werden. Wird die Identifizierung unterbrochen, muss sie zu einem neuen Termin unterbrechungsfrei wiederholt werden. Während der persönlichen

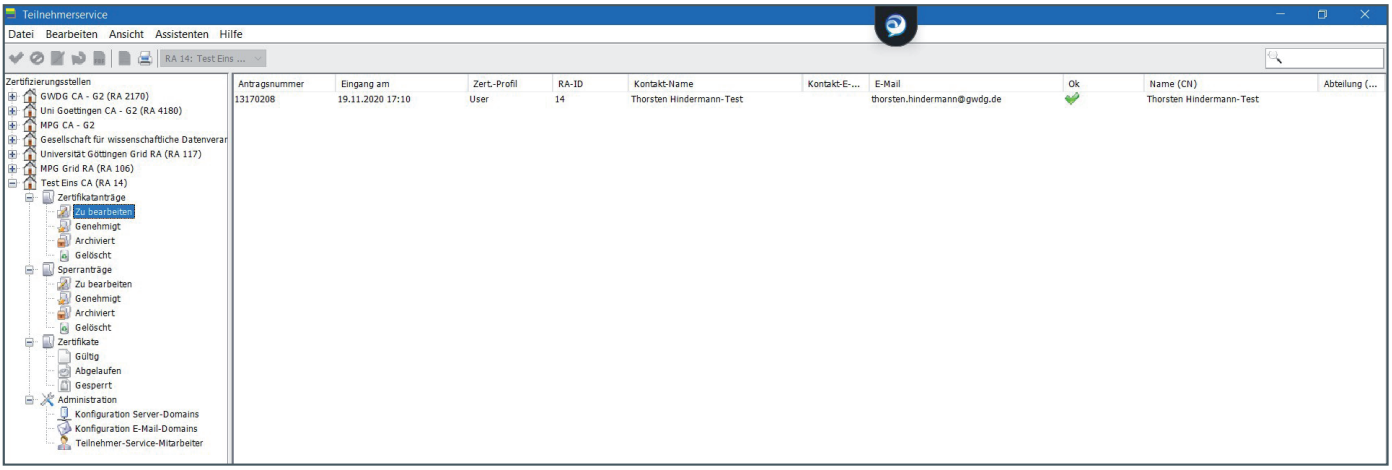


Abb. 2

Identifizierung werden vom TS-MA folgende Fragen und Anweisungen an den Zertifikatnehmer gestellt und Merkmale auf dem Ausweisdokument überprüft:

- Der Antragsteller wurde in diesem Wortlaut über den Zweck des Verfahrens informiert: Diese Videokonferenz dient dazu, Sie für die Ausstellung des von Ihnen beantragten Zertifikats zu identifizieren. Wie lautet die Antragsnummer des von Ihnen gestellten Antrags?
- Der Antragsteller hat die folgende Antragsnummer genannt: ____; diese Antragsnummer passt zum vorliegenden Antrag.
- Herkunft und Art des Ausweisdokuments sind auf dem Videobild klar erkennbar und passen zu den im Voraus gemachten Angaben.
- Das Lichtbild auf dem Ausweisdokument ist klar erkennbar und passt zum Antragsteller.
- Der Antragsteller ist mit dem Finger vor dem Lichtbild auf dem Ausweisdokument entlanggefahren.
- Das Lichtbild wurde dabei vollständig überstrichen, aber trotzdem stabil und ohne Auffälligkeiten angezeigt.
- Der Name auf dem Ausweisdokument ist klar lesbar und passt zum vorliegenden Antrag.
- Die Unterschrift auf dem Ausweisdokument ist klar erkennbar und passt zum vorliegenden Antrag.
- Das Gültigkeitsdatum des Ausweisdokuments ist klar lesbar; der Ausweis ist gültig.
- Die Nummer des Ausweisdokuments ist klar lesbar; die letzten fünf Stellen lauten: ____
- Die folgenden Sicherheitsmerkmale des Ausweisdokuments sind klar erkennbar (hier müssen mindestens drei von fünf Merkmalen erkannt werden): ____
- Es sind insgesamt mindestens drei Sicherheitsmerkmale zweifelsfrei erkannt worden.
- Die Angaben auf der Vorder- und Rückseite des Ausweisdokuments sind konsistent.

Nachdem diese Punkte alle abgearbeitet worden sind und der TS-MA zum Ergebnis gelangt ist, dass es sich bei dem Zertifikatnehmer um die Person handelt, die das Nutzerzertifikat beantragt hat, werden dieses Ergebnis und ein paar weitere Informationen auf dem Dokumentationsbogen notiert und zusammen mit den Zertifikatantrag abgelegt bzw. archiviert. Ab diesem Zeitpunkt kann der TS-MA den Zertifikatantrag bearbeiten und anschließend genehmigen.

Hinweise für TS-MA

Wichtig wäre noch zu erwähnen, dass für die Identifizierung der Ausweismerkmale durch den TS-MA mittels der Videoübertragung im Raum des Zertifikatnehmers genügend Tageslicht vorhanden sein sollte. Sonst können unter Umständen die Sicherheitsmerkmale der Ausweisdokumente nicht einwandfrei erkannt werden.

Wird die Pexip Infinity Connect App unter Android- oder iOS-Geräten genutzt, hat es sich bewährt, dass der Zertifikatnehmer in der App von der Front-Kamera auf die rückseitige Hauptkamera umschaltet, da sich die Hauptkameras der mobilen Geräte besser eignen, um die Sicherheitsmerkmale der Ausweisdokumente gut sichtbar darstellen zu können.

Die Video-Identifizierung dauert ca. fünf Minuten. Am längsten dauert dabei die Erkennung der Sicherheitsmerkmale bei diesem Vorgang.

Eine weitere Empfehlung ist, Termine für die Video-Identifizierung zu vereinbaren und darin den DFNconf-Meetingraum Vorlagentext einzufügen, damit der Zertifikatnehmer weiß, mit welchem Kommunikationsmedium er sich für diesen Vorgang verbinden kann. Weiterhin empfiehlt es sich, in Abständen die Gast-PIN für den DFNconf-Meetingraum zu ändern.

In der Praxis haben sich aber auch Identifizierungen mittels anderer gängiger Video-Konferenzprogramme bewährt, wie z. B. BBB [10] oder Zoom.

Falls der Zertifikatnehmer über keinen deutschen Personalausweis oder Reisepass verfügt, kann sich der TS-MA über eine Webseite der EU [11] – PRADO - Öffentliches Online-Register echter Identitäts- und Reisedokumente – über alle weltweit gültigen Ausweise und deren Sicherheitsmerkmale für den Identifizierungsvorgang informieren. Dazu dient die Abfrage des TS-MA im Vorfeld der Identifizierung, z. B. bei der Terminvergabe, mit welchem Ausweisdokument sich der Zertifikatnehmer ausweisen möchte.

Nutzer/E-Mail-Zertifikate

Hat ein*e Anwender*in ein Nutzerzertifikat beantragt, muss die Antrags-PDF-Datei von ihm/ihr ausgedruckt, unterschrieben und wieder eingescannt werden oder aber ein gutes Handyfoto gemacht werden. Diese PDF- oder JPEG-Datei muss dann dem Teilnehmerservice zugehen.

Vor der COVID-19-Pandemie konnte der Antrag beim Teilnehmerservice im eigenen Institut abgegeben werden. Dies kann in der COVID-19-Zeit sicherlich auch erfolgen, wenn das Institut schon wieder teilweise oder komplett in Präsenzarbeit vertreten ist – in diesem Fall dann aber unter Einhaltung der Hygienemaßnahmen des betreffenden Instituts.

Im anderen Fall, wenn die meisten Anwender*innen im Homeoffice arbeiten, muss dem Teilnehmerservice die unterschriebene PDF-Datei oder das Foto des unterschriebenen Antrags z. B. als JPEG-Datei per E-Mail zugesendet werden. Dort wird der Antrag vom TS-MA ausgedruckt und ein Termin für eine persönliche Identifizierung per Video-Identifizierung vereinbart.

Nachdem die persönliche Identifizierung per Video-Identifizierung erfolgreich absolviert worden ist, kann der TS-MA die Angaben des Papierantrags mit den Angaben des elektronisch vorliegenden Antrags mit Hilfe des Programms GUIRA prüfen

Beim Nutzer- bzw. E-Mail-Zertifikat, das vom Nutzer in den allermeisten Fällen zum Signieren und in seltenen Fällen auch zum Verschlüsseln von E-Mails verwendet wird, sind die wichtigsten Felder das „Name (CN)"-Feld und die „Alternative Namen"-Felder.

Dem „Name (CN)"-Feld (siehe Abbildung 3) und in der Zertifikatantrags-Ansicht in der Gruppe „Subject DN" dem Feld „CN" (siehe Abbildung 4) kommt eine wichtige Rolle zu. In diesem Feld stehen im Normalfall die Angaben Vorname und Nachname sowie, wenn im Ausweisdokument wie z. B. Personalausweis, Reisepass oder Aufenthaltstitel vorhanden, der Dr.-Titel. Beispiele sind. „CN=Erika Mustermann" oder „CN=Dr. Erika Mustermann".

Weichen die Angaben in diesem Feld ab, muss mit dem Zertifikatnehmer geklärt werden, um was für ein Zertifikat es sich handelt. Für diese Fälle sieht die Richtlinie des DFN-Verein die Präfixe „PN:" (Pseudonym-Zertifikat), „GRP:" (Gruppenzertifikat) oder „EXT:" (externer Zertifikatnehmer) vor.

Ein Beispiel für einen Pseudonym-Zertifikatantrag ist in den Abbildungen 4 und 5 zu sehen. Hier ist der „CN=PN: Thorsten Hindermann-Test" zu lesen. Wegen der Endung „-Test" im

Antragsnummer	Eingang am	Zert.-Profil	RA-ID	Kontakt-Name	Kontakt-E-Mail	E-Mail	Ok	Name (CN)
70674976	23.11.2020 15:38	Web Server	2170	Thorsten Hindermann	thorsten.hindermann@gwdg.de		✔	example.gwdg.de

Abb. 3

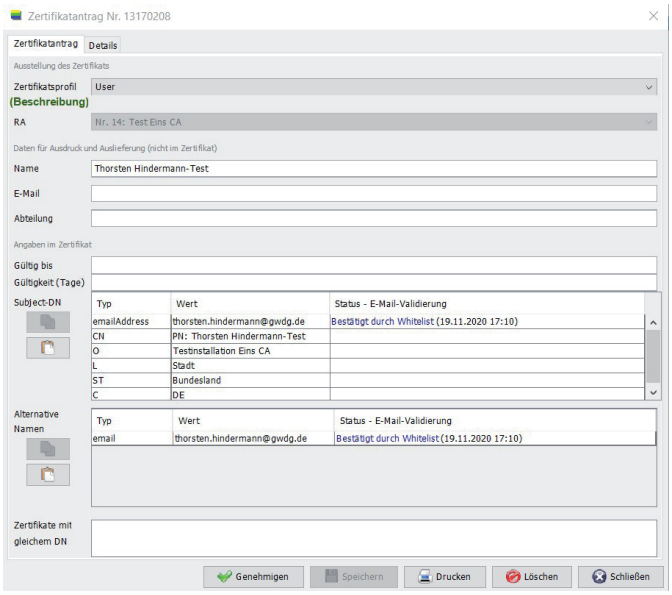


Abb. 4

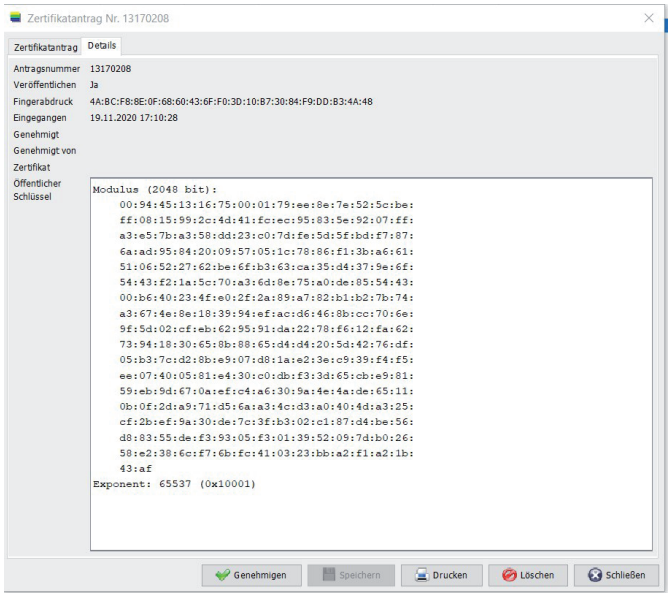


Abb. 5

Nachnamen muss diesem Zertifikat das Präfix „PN:“ vorangestellt werden (siehe Abbildung 4). Ein weiteres Praxisbeispiel für ein Pseudonym-Zertifikat wäre „CN=PN: Prof. Dr. Erika Mustermann“. Der Grund für das „PN:“ in diesem Beispiel ist, dass der Titel „Prof.“ kein Namensbestandteil ist und somit auch nicht in Ausweisdokumenten steht.

Bei einem Gruppenzertifikat handelt es sich um ein Zertifikat, das von mehreren Personen genutzt werden kann. Das „Name (CN)-Feld“ sieht dann z. B. so aus: „CN=GRP: Datenschutzbeauftragte“. Im Bereich der „Alternative Namen“-Felder sind dann entweder alle einzelnen E-Mail-Adressen der Datenschutzbeauftragten des Instituts aufgelistet oder nur die zentrale E-Mail-Adresse des Postfachs für die Datenschutzbeauftragten des Instituts. Hier muss der Antragsteller des Gruppenzertifikats entscheiden, welche E-Mail-Adresse(n) aufgenommen werden sollen.

Bei einem Zertifikat mit dem Präfix „EXT:“ im „Name (CN)“-Feld wird kenntlich gemacht, dass eine externe Person im Namen des Instituts Aufgaben verrichtet und somit berechtigt ist, E-Mails zu versenden. Ein Beispiel wäre ein externer Dienstleister, dessen Mitarbeiter*innen im Institut Aufgaben erledigen und mit Kund*innen kommunizieren müssen. Diese externen Mitarbeiter*innen können Zertifikate mit dem Präfix „EXT:“ erhalten um anzuzeigen, dass diese keinen direkten Arbeitsvertrag mit dem Institut abgeschlossen haben, aber für das Institut Dienstleistungen erbringen und mit dessen Kund*innen und Mitarbeiter*innen kommunizieren müssen. Ein Beispiel wäre „CN=EXT: Erika Mustermann“.

In den „Alternative Namen“-Felder sollten, wenn möglich, alle dem/der Nutzer*in vom Institut zugeordneten E-Mail-Adressen eingetragen werden. Somit kann der/die Nutzer*in seine/ihre primäre E-Mail-Adresse zum Absenden ändern, ohne das der E-Mal-Client, z. B. Microsoft Outlook, moniert, dass die Absender-E-Mail-Adresse nicht im Nutzerzertifikat vorhanden ist (siehe Abbildung 4).

In der Registerkarte „Details“ ist der Fingerabdruck vorhanden. Dieser sollte mit dem Fingerabdruck auf dem Papierantrag verglichen werden (siehe Abbildung 5).

Wenn alle Angaben überprüft und korrekt sind, steht der Genehmigung des Zertifikatantrags nichts mehr im Wege. Mit einem Klick auf „Genehmigen“ wird der Antrag genehmigt. Nach ein paar Minuten ist das Zertifikat dann von der zuständigen CA ausgestellt und der/die Antragsteller*in erhält eine Bestätigungs-E-Mail mit dem Zertifikat im Anhang. Technisch gesehen ist der Anhang der signierte öffentliche Schlüssel, der zum bei der Beantragung erzeugten privaten Schlüssel des Zertifikats passt. In mehreren GWDG-Nachrichten-Artikeln wird diese ganze Prozedur für die Nutzer*innen ausführlich beschrieben:

1. GWDG-Nachrichten 12/2019: E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 1: Beantragung und Sicherung von Zertifikaten (ab Seite 9)
2. GWDG-Nachrichten 1-2/2020: E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 2: Installation und Verteilung von Zertifikaten (ab Seite 14)
3. GWDG-Nachrichten 3/2020: E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 3: Outlook-E-Mail-Anwendungen (ab Seite 6)
4. GWDG-Nachrichten 4-5/2020 – Überarbeitung des neuen Beantragungsweges für Nutzerzertifikate in der DFN-PKI (ab Seite 26)
5. GWDG-Nachrichten 7-8/2020: E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 4: Apple E-Mail-Anwendungen (ab Seite 8)
6. GWDG-Nachrichten 11/2020: E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 5: Thunderbird, Notes und Mutt (ab Seite 12)

Serverzertifikate

Erzeugung von Serverzertifikaten durch den Server-Administrator

Die Bearbeitung, Prüfung und Genehmigung eines Serverzertifikats erfolgt ähnlich wie bei einem Nutzerzertifikat. Ein Serverzertifikat ist daran zu erkennen, dass das Zertifikatprofil z. B. „Web-Server“, „VPN-Server“, „Mail-Server“ oder „Radius-Server“ heißt.

Weiterhin steht im „Name (CN)"-Feld ein voll qualifizierter Domänenname, kurz FQDN (siehe Abbildung 3).

Wenn der Server-Administrator den PDF-Antrag an den Teilnehmerservice gesendet hat, sollte der TS-MA folgende Aktionen durchführen:

Ist der unterschriebene Antrag per Post oder Fax eingegangen, sollte zunächst per Video-Identifizierung der Antragsteller identifiziert werden.

Ist der Antrag in einer signierten E-Mail des Antragstellers eingegangen, sollte das Zertifikat auf Gültigkeit geprüft werden. Ist dies der Fall, ersetzt das Zertifikat die Unterschrift in der angehängten Zertifikatantrag-PDF-Datei. Die E-Mail mit der Antrags-PDF-Datei sollte auf alle Fälle in einem Dateisystem gespeichert werden. Die Archvierungsfrist der E-Mail beträgt, genau wie die Papieranträgen, sieben Jahre.

Nach diesen Prüfschritten können nun die Angaben in der PDF-Datei mit denen im Programm GUIRA geprüft werden. Die Zertifikatantragsdaten können mit einem Doppelklick auf den elektronischen Antrag aufgerufen werden (siehe Abbildung 6). Alle Angaben können überprüft werden und auch vor dem Genehmigen

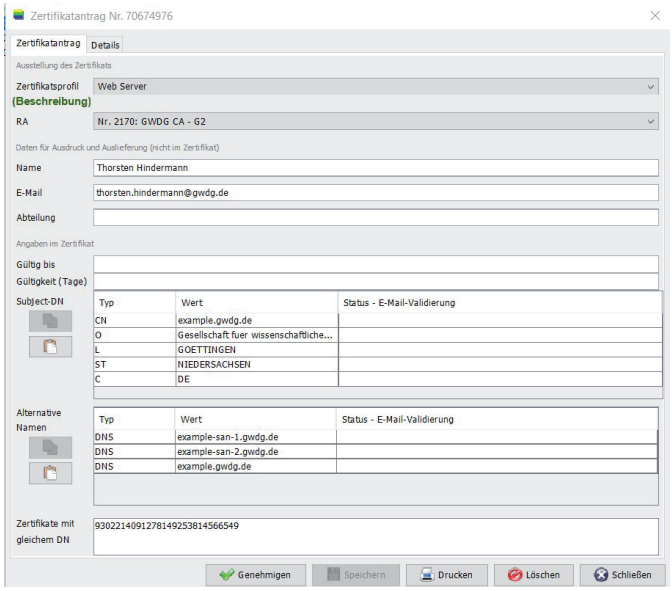


Abb. 6

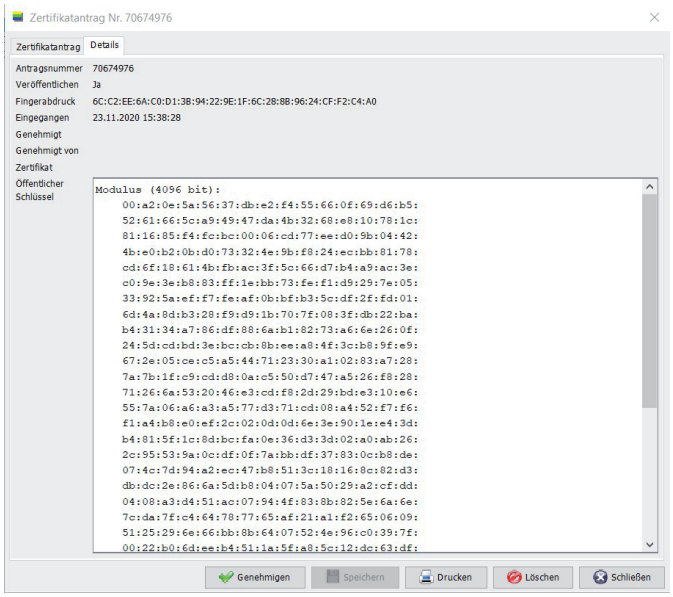


Abb. 7

bearbeitet werden. In der Registerkarte „Details" kann noch der Fingerprint angesehen und mit der Antrags-PDF-Datei verglichen werden (siehe Abbildung 7).

Sind die Angaben geprüft und alles ist in Ordnung, steht einer Genehmigung des Zertifikatantrags nichts mehr im Wege. Dieser Vorgang wird mit Klick auf die Schaltfläche „Genehmigen" ausgeführt. Nach ein paar Minuten ist das Zertifikat dann von der zuständigen CA ausgestellt und der Antragsteller erhält eine Bestätigungs-E-Mail mit dem Zertifikat, technisch der signierte öffentliche Schlüssel, der zum bei der Beantragung erzeugten privaten Schlüssel des Zertifikats passt. Beide Teile zusammen ergeben das Zertifikat und können nun vom Server-Administrator in den entsprechenden Server bzw. Dienst zur Absicherung der Übertragungswege und Informationen konfiguriert werden.

In dem Artikel „Einsatzmöglichkeiten von X.509-Zertifikaten – Teil 1: Serverzertifikate" in den GWDG-Nachrichten 9-10/2020 werden die Tätigkeiten eines Server-Administrators bei der Beantragung und Weiterverarbeitung eines Serverzertifikats ausführlicher beschrieben.

Erzeugung von Serverzertifikaten durch den TS-MA

Bei Serverzertifikaten tritt die Einrichtung als juristische Person als Antragsteller auf und nicht der TS-MA als natürliche Person. Deshalb ist es möglich, dass der TS-MA Serverzertifikate selbst beantragen und genehmigen kann.

Im Programm GUIRA befindet sich im Menü „Assistenten" der Punkt „Serverzertifikat erstellen", der die Erzeugung von privatem Schlüssel und Antrag und dessen Genehmigung automatisiert (siehe Abbildung 8).

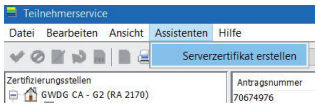


Abb. 8

Erfüllt der Teilnehmerservice die Rolle eines Administrators, z. B. weil dieser direkt im Rechenzentrum angesiedelt ist, kann diese Möglichkeit eingesetzt werden.

Das Formular des Serverzertifikat-Assistenten sieht wie in Abbildung 9 dargestellt aus. Die Felder mit dem Sternchen (*) sind Pflichtfelder, die ausgefüllt werden müssen. Abbildung 9 zeigt exemplarisch das ausgefüllte Formular, so wie es sich in der Praxis bewährt. Mit einem Klick auf die Schaltfläche „Weiter" erscheint eine Hinweis-Dialogbox (siehe Abbildung 10) mit weiteren Anweisungen, die mit einem Klick auf die Schaltfläche „OK" bestätigt wird. Jetzt muss das Verzeichnis ausgewählt werden, in dem alle Dateien des Serverzertifikat-Assistenten gespeichert werden können (siehe Abbildung 11). Mit einem Klick auf die Schaltfläche „Öffnen" wird die Auswahl des Verzeichnisses abgeschlossen.

Als nächstes beginnt der Assistent mit der Erzeugung des privaten Schlüssels (siehe Abbildung 12). Wenn dieser Schlüssel erzeugt wurde, wird der elektronische Zertifikatantrag, engl. Certificate Signing Request, kurz CSR, in der RA eingereicht. Dieser Vorgang findet im Hintergrund bei der Ausführung des Assistenten statt. Wenn er abgeschlossen ist, erscheint ein weiteres Formular (siehe Abbildung 13). Parallel dazu wird der Zertifikatantrag in PDF-Form vom Assistenten heruntergeladen und im Standardansichtsprogramm für PDF-Dateien angezeigt (siehe Abbildung 14).

Die PDF-Datei kann nun entweder ausgedruckt und im unteren Bereich mit der Überschrift „Wird vom Teilnehmerservice ausgefüllt" vom TS-MA entsprechend ausgefüllt und unterschrieben

Abb. 9

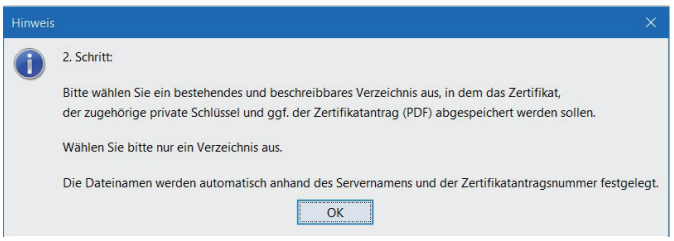


Abb. 10

Abb. 12

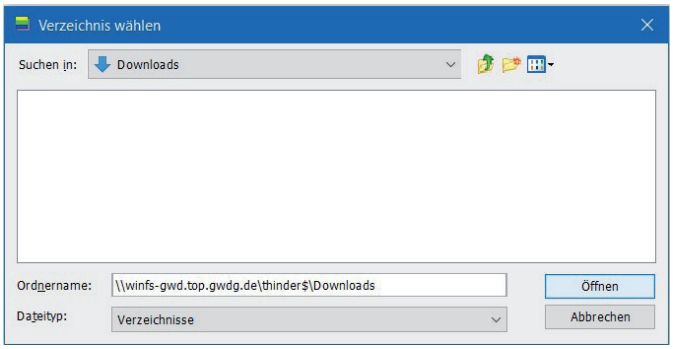


Abb. 11

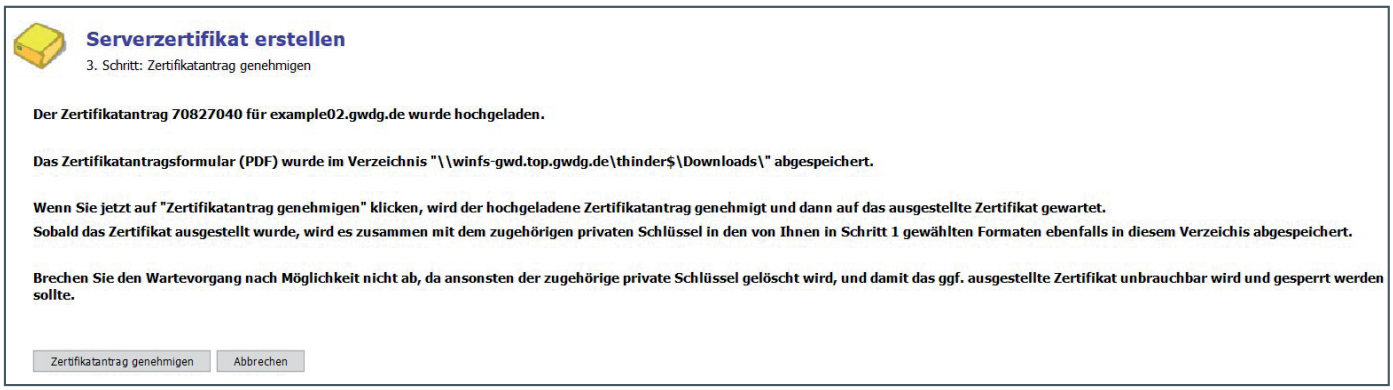


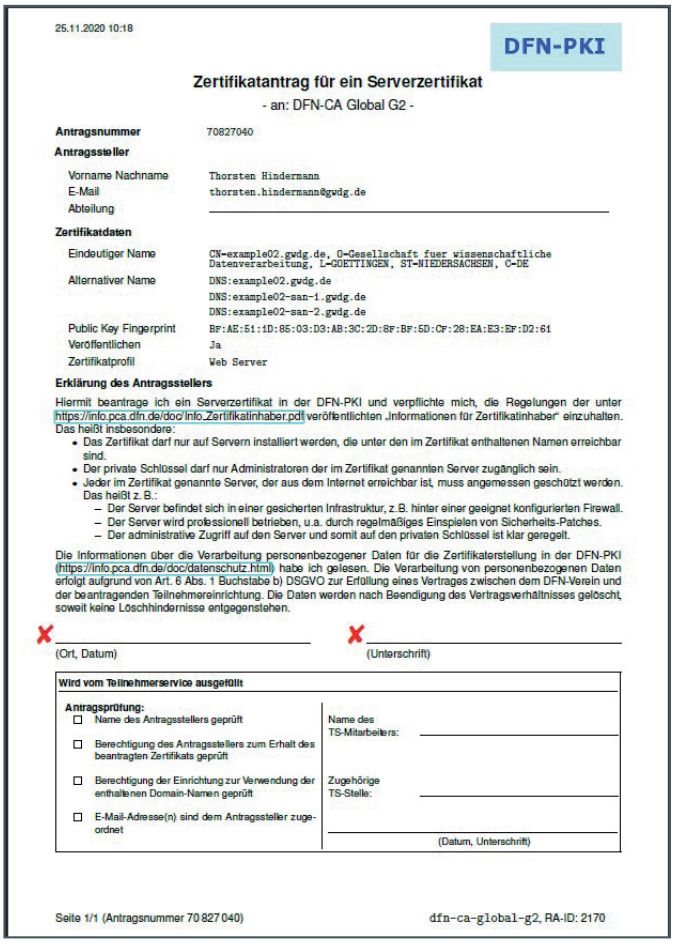
Abb. 13

werden oder aber mit einem PDF-Bearbeitungsprogramm ausgefüllt und unterschrieben werden (siehe Abbildung 15).

Abschließend wird im Programm GUIRA noch auf die Schaltfläche „Zertifikatantrag genehmigen“ geklickt (siehe Abbildung 13). Eine Statusmeldung erscheint, die den Vorgang der Bearbeitung anzeigt (siehe Abbildung 16). Ist der Vorgang abgeschlossen, zeigt der Assistent die letzte finale Seite an, die Auskunft über die erfolgreiche Ausstellung des Serverzertifikats gibt (siehe Abbildung 17).

Domänenverwaltung

In einer RA können nach der Erstellung nur Zertifikate für den zum Institut zugehörigen Domänennamen ausgestellt werden. Im



25.11.2020 10:18

DFN-PKI

Zertifikatantrag für ein Serverzertifikat

- an: DFN-CA Global G2 -

Antragsnummer 70827040

Antragssteller

Vorname Nachname	Thorsten Hindermann
E-Mail	thorsten.hindermann@gwdg.de
Abteilung	

Zertifikatdaten

Eindeutiger Name	CN=example02.gwdg.de, O=Gesellschaft fuer wissenschaftliche Datenverarbeitung, L=GOETTINGEN, ST=NIEDERSACHSEN, C=DE
Alternativer Name	DNS:example02.gwdg.de DNS:example02-san-1.gwdg.de DNS:example02-san-2.gwdg.de
Public Key Fingerprint	BF:AE:51:1D:85:03:D3:AB:3C:2D:8F:BF:5D:CF:28:EA:E3:EF:D2:61
Veröffentlichen	Ja
Zertifikatprofil	Web Server

Erklärung des Antragsstellers

Hiermit beantrage ich ein Serverzertifikat in der DFN-PKI und verpflichte mich, die Regelungen der unter https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf veröffentlichten „Informationen für Zertifikatinhaber" einzuhalten. Das heißt insbesondere:

- Das Zertifikat darf nur auf Servern installiert werden, die unter den im Zertifikat enthaltenen Namen erreichbar sind.
- Der private Schlüssel darf nur Administratoren der im Zertifikat genannten Server zugänglich sein.
- Jeder im Zertifikat genannte Server, der aus dem Internet erreichbar ist, muss angemessen geschützt werden. Das heißt z. B.:
  - Der Server befindet sich in einer gesicherten Infrastruktur, z. B. hinter einer geeignet konfigurierten Firewall.
  - Der Server wird professionell betrieben, u.a. durch regelmäßiges Einspielen von Sicherheits-Patches.
  - Der administrative Zugriff auf den Server und somit auf den privaten Schlüssel ist klar geregelt.

Die Informationen über die Verarbeitung personenbezogener Daten für die Zertifikatserstellung in der DFN-PKI (https://info.pca.dfn.de/doc/datenschutz.html) habe ich gelesen. Die Verarbeitung von personenbezogenen Daten erfolgt aufgrund von Art. 6 Abs. 1 Buchstabe b) DSGVO zur Erfüllung eines Vertrages zwischen dem DFN-Verein und der beantragenden Teilnehmereinrichtung. Die Daten werden nach Beendigung des Vertragsverhältnisses gelöscht, soweit keine Löschhindernisse entgegenstehen.

✗ _____ (Ort, Datum)

✗ _____ (Unterschrift)

Wird vom Teilnehmerservice ausgefüllt

Antragsprüfung:

- ☐ Name des Antragsstellers geprüft
- ☐ Berechtigung des Antragstellers zum Erhalt des beantragten Zertifikats geprüft
- ☐ Berechtigung der Einrichtung zur Verwendung der enthaltenen Domain-Namen geprüft
- ☐ E-Mail-Adresse(n) sind dem Antragssteller zugeordnet

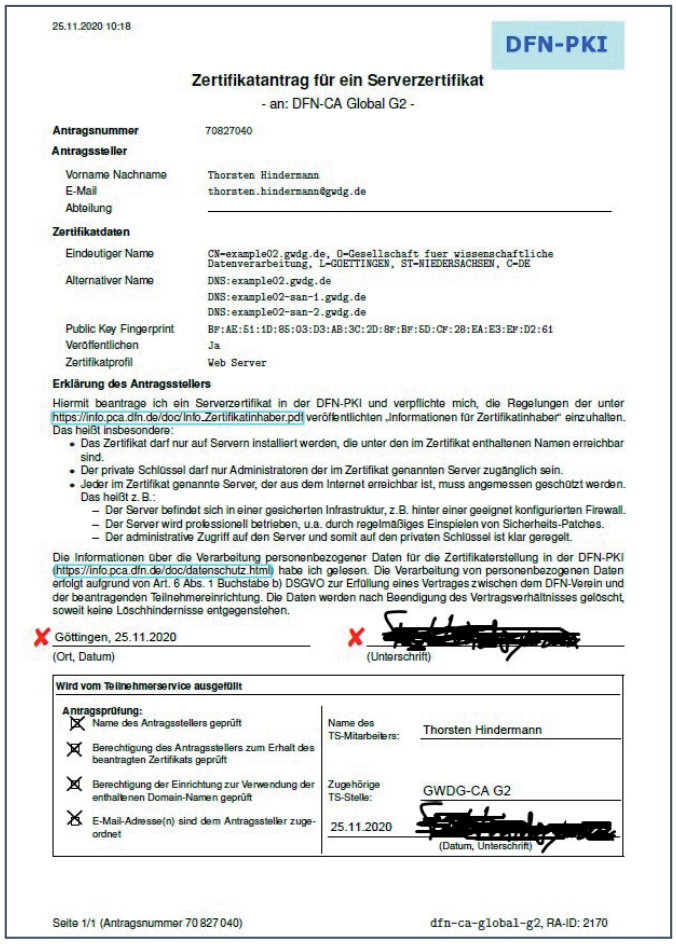
Name des TS-Mitarbeiters: _____

Zugehörige TS-Stelle: _____

(Datum, Unterschrift)

Seite 1/1 (Antragsnummer 70827040) dfn-ca-global-g2, RA-ID: 2170

Abb. 14



25.11.2020 10:18

DFN-PKI

Zertifikatantrag für ein Serverzertifikat

- an: DFN-CA Global G2 -

Antragsnummer 70827040

Antragssteller

Vorname Nachname	Thorsten Hindermann
E-Mail	thorsten.hindermann@gwdg.de
Abteilung	

Zertifikatdaten

Eindeutiger Name	CN=example02.gwdg.de, O=Gesellschaft fuer wissenschaftliche Datenverarbeitung, L=GOETTINGEN, ST=NIEDERSACHSEN, C=DE
Alternativer Name	DNS:example02.gwdg.de DNS:example02-san-1.gwdg.de DNS:example02-san-2.gwdg.de
Public Key Fingerprint	BF:AE:51:1D:85:03:D3:AB:3C:2D:8F:BF:5D:CF:28:EA:E3:EF:D2:61
Veröffentlichen	Ja
Zertifikatprofil	Web Server

Erklärung des Antragsstellers

Hiermit beantrage ich ein Serverzertifikat in der DFN-PKI und verpflichte mich, die Regelungen der unter https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf veröffentlichten „Informationen für Zertifikatinhaber" einzuhalten. Das heißt insbesondere:

- Das Zertifikat darf nur auf Servern installiert werden, die unter den im Zertifikat enthaltenen Namen erreichbar sind.
- Der private Schlüssel darf nur Administratoren der im Zertifikat genannten Server zugänglich sein.
- Jeder im Zertifikat genannte Server, der aus dem Internet erreichbar ist, muss angemessen geschützt werden. Das heißt z. B.:
  - Der Server befindet sich in einer gesicherten Infrastruktur, z. B. hinter einer geeignet konfigurierten Firewall.
  - Der Server wird professionell betrieben, u.a. durch regelmäßiges Einspielen von Sicherheits-Patches.
  - Der administrative Zugriff auf den Server und somit auf den privaten Schlüssel ist klar geregelt.

Die Informationen über die Verarbeitung personenbezogener Daten für die Zertifikatserstellung in der DFN-PKI (https://info.pca.dfn.de/doc/datenschutz.html) habe ich gelesen. Die Verarbeitung von personenbezogenen Daten erfolgt aufgrund von Art. 6 Abs. 1 Buchstabe b) DSGVO zur Erfüllung eines Vertrages zwischen dem DFN-Verein und der beantragenden Teilnehmereinrichtung. Die Daten werden nach Beendigung des Vertragsverhältnisses gelöscht, soweit keine Löschhindernisse entgegenstehen.

✗ Göttingen, 25.11.2020 (Ort, Datum)

✗ [redacted] (Unterschrift)

Wird vom Teilnehmerservice ausgefüllt

Antragsprüfung:

- ☒ Name des Antragsstellers geprüft
- ☒ Berechtigung des Antragstellers zum Erhalt des beantragten Zertifikats geprüft
- ☒ Berechtigung der Einrichtung zur Verwendung der enthaltenen Domain-Namen geprüft
- ☒ E-Mail-Adresse(n) sind dem Antragssteller zugeordnet

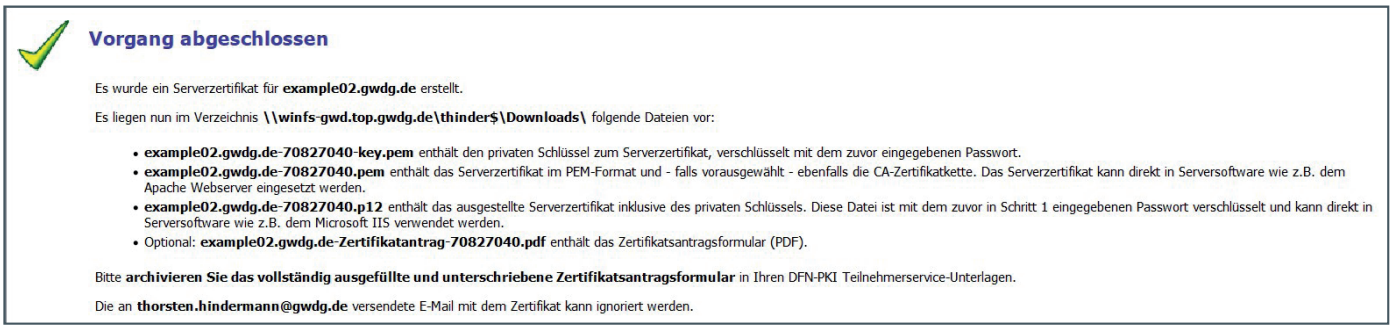
Name des TS-Mitarbeiters: Thorsten Hindermann

Zugehörige TS-Stelle: GWDG-CA G2

25.11.2020 [redacted] (Datum, Unterschrift)

Seite 1/1 (Antragsnummer 70827040) dfn-ca-global-g2, RA-ID: 2170

Abb. 15



Vorgang abgeschlossen

Es wurde ein Serverzertifikat für **example02.gwdg.de** erstellt.

Es liegen nun im Verzeichnis **\\winfs-gwd.top.gwdg.de\thinder$\Downloads** folgende Dateien vor:

- **example02.gwdg.de-70827040-key.pem** enthält den privaten Schlüssel zum Serverzertifikat, verschlüsselt mit dem zuvor eingegebenen Passwort.
- **example02.gwdg.de-70827040.pem** enthält das Serverzertifikat im PEM-Format und - falls vorausgewählt - ebenfalls die CA-Zertifikatkette. Das Serverzertifikat kann direkt in Serversoftware wie z.B. dem Apache Webserver eingesetzt werden.
- **example02.gwdg.de-70827040.p12** enthält das ausgestellte Serverzertifikat inklusive des privaten Schlüssels. Diese Datei ist mit dem zuvor in Schritt 1 eingegebenen Passwort verschlüsselt und kann direkt in Serversoftware wie z.B. dem Microsoft IIS verwendet werden.
- Optional: **example02.gwdg.de-Zertifikatantrag-70827040.pdf** enthält das Zertifikatsantragsformular (PDF).

Bitte **archivieren Sie das vollständig ausgefüllte und unterschriebene Zertifikatsantragsformular** in Ihren DFN-PKI Teilnehmerservice-Unterlagen.

Die an **thorsten.hindermann@gwdg.de** versendete E-Mail mit dem Zertifikat kann ignoriert werden.

Abb. 17

Abb. 16

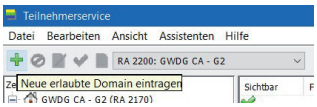


Abb. 18

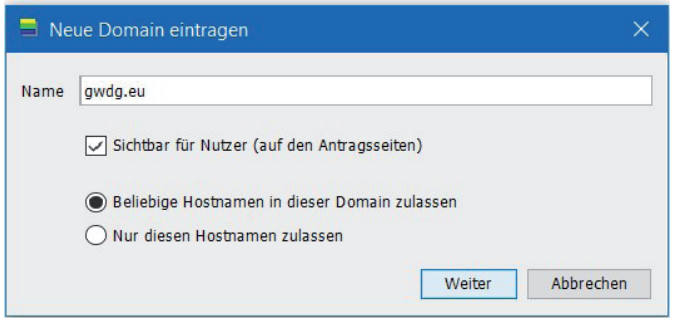


Abb. 19

Laufe der Zeit können und werden noch weitere Domänennamen dazukommen. Im folgenden Beispiel wird das Hinzufügen einer Domäne zur RA veranschaulicht. Es soll die Domäne *gwdg.eu* der RA hinzugefügt werden. Dazu in GUIRA oben links in der Werkzeugleiste auf die Schaltfläche mit dem grünen „+" klicken (siehe Abbildung 18). Den Namen der Domäne eintragen, die der RA hinzugefügt werden soll (siehe Abbildung 19). Gewählt werden kann noch die Sichtbarkeit für Beantragende auf den Antragsseiten und ob beliebige Hostnamen für den neuen Domänennamen zugelassen sind oder nur der im Eingabefeld genau eingegebene Domänennamen zulässig ist. Auf die Schaltfläche „Weiter" klicken. In dem zweiten Schritt nun am besten den Zonen-Kontakt anwählen und auf die Schaltfläche „Speichern" klicken (siehe Abbildung 20). An die angezeigte E-Mail-Adresse wird nach initialer Überprüfung durch den DFN-Verein dann eine Validierungs-E-Mail gesendet. Diesen abschließenden Dialog mit Klick auf die Schaltfläche „OK" beenden (siehe Abbildung 21). Nachdem der Empfänger der E-Mail der Domänenvalidierung zugestimmt hat, können ab diesem Zeitpunkt in dieser RA Zertifikate beantragt und genehmigt werden, deren im Zertifikatantrag enthaltene Domänennamen mit der Domänenendung *gwdg.eu* enden (z. B. *www.gwdg.eu)*.

Eine weitere Tätigkeit der Domänenverwaltung ist die Revalidierung. Die Domänen sind nur für eine bestimmte Zeit in der RA gültig. Danach muss erneut eine Validierungs-E-Mail versendet werden. Dazu eine Domäne auswählen und auf die Auswahl mit der rechten Maustaste klicken. Im Kontext-Menü den Menüpunkt „Domain validieren" anklicken (siehe Abbildung 22). Im Dialogfeld am besten wieder den Zonen-Kontakt auswählen. An diese E-Mail-Adresse wird die Validierungs-E-Mail gesendet (siehe Abbildung 23). Bestätigt der Empfänger der E-Mail die Domäne, ist diese revalidierte Domäne für den nächsten Zeitraum gültig und steht in der RA wieder für Zertifikatanträge zur Verfügung. Abbildung 24 zeigt den Benachrichtigungstext für die Domänenvalidierung, in diesem Beispiel in englischer Sprache. Abbildung 25 zeigt den relevanten Ausschnitt der Validierungswebseite, wenn der URL in der Adresszeile eines Webbrowers aufgerufen wurde, und Abbildung 26 schließlich den relevanten Teil der Webseite, nachdem auf die Schaltfläche „Bestätigen" geklickt worden ist.

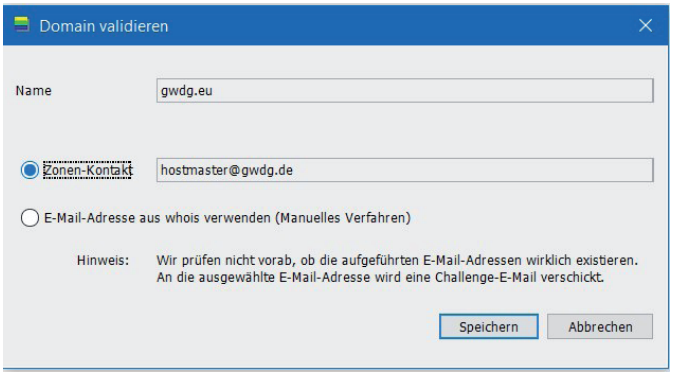


Abb. 20

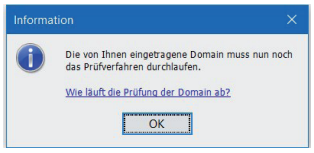


Abb. 21

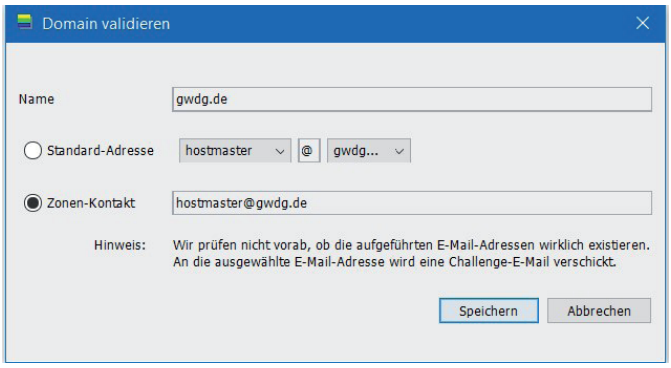


Abb. 23

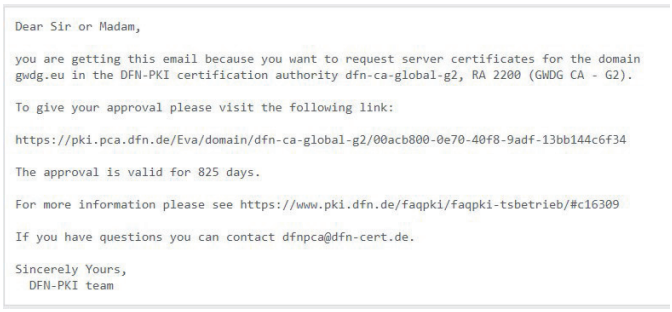


Abb. 24

Sperrung

Wenn ein Zertifikatinhaber über das Formular zum Sperren des Zertifikats einen entsprechenden Sperrantrag erstellt hat oder dem TS-MA mitteilt, dass das Zertifikat gesperrt werden soll, sollte der TS-MA diesen Antrag zeitnah genehmigen bzw. das Zertifikat direkt sperren (siehe Abbildung 27). Bei der Direktsperrung sowie der Sperrung mittels des Webformulars wird jeweils noch nach einem Sperrgrund gefragt (siehe Abbildungen 28 und 29). Nachdem der Sperrantrag durch den TS-MA genehmigt wurde oder der TS-MA das Zertifikat direkt gesperrt hat, wird im Hintergrund das gesperrte Zertifikat in die Sperrliste eingetragen und die neue Liste wird zum Abruf veröffentlicht. Die URLs zum Abruf der Sperrlisten können in den Informationen jedes Zertifikats eingesehen werden (siehe Abbildung 30).

Beratung

Wie in dem Zertifizierungsrichtlinien-Dokument des DFN-Vereins [12] unter „Aufgabe der Rolle" der Rolle „Teilnehmerservice-Mitarbeiter" zu lesen, ist der TS-MA auch für die Beratung der Zertifikat-inhaber zuständig. Aus eigener langjähriger Erfahrung ergeben sich zumeist immer wieder dieselben Fragen. Das Ergebnis der Fragen und Antworten ist in die oben genannten GWDG-Nachrichten-Artikel eingeflossen und sie sind damit für neue aber auch schon länger amtierende TS-MA sicherlich ein gutes Fundament für ihre Beratungstätigkeit. Diese Artikel können auch unter [13], Thema „E-Mail-Verschlüsselung mit X.509-Zertifikaten", und [14], Thema „Einsatzmöglichkeiten von X.509-Zertifikaten", als PDFs abgerufen werden.

Ausblick

Nachdem Sie nun diesen Artikel gelesen haben und sich vielleicht zutrauen, eine RA für Ihr Institut, dass noch keine RA hat, zu verwalten, zögern Sie nicht, eine E-Mail an die weiter oben genannten E-Mail-Adressen zu schreiben. Sollten Sie noch Fragen in Bezug auf die TS-MA-Tätigkeit und Verwaltung einer RA sowie Zertifikaten haben, die dieser Artikel nicht beantwortet, dann schreiben Sie einfach an die genannten E-Mail-Adressen eine E-Mail mit Ihren Fragen, die der Autor diese Artikels gerne beantwortet.

In einem nächsten GWDG-Nachrichten-Artikel soll dann das auf Java basierende RA-Verwaltungsprogramm GUIRA, das in

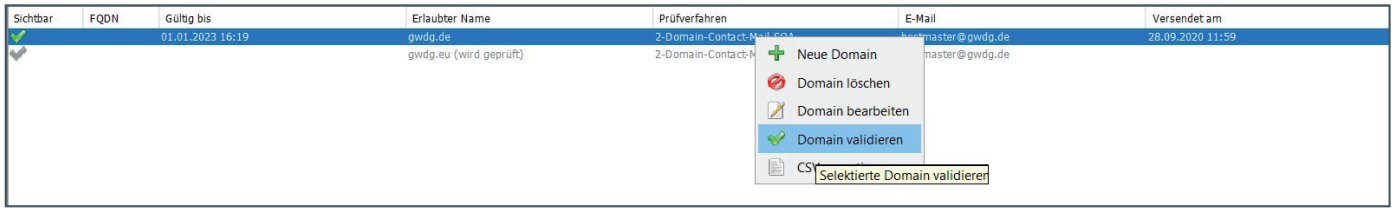


Abb. 22

Abb. 25

Abb. 26

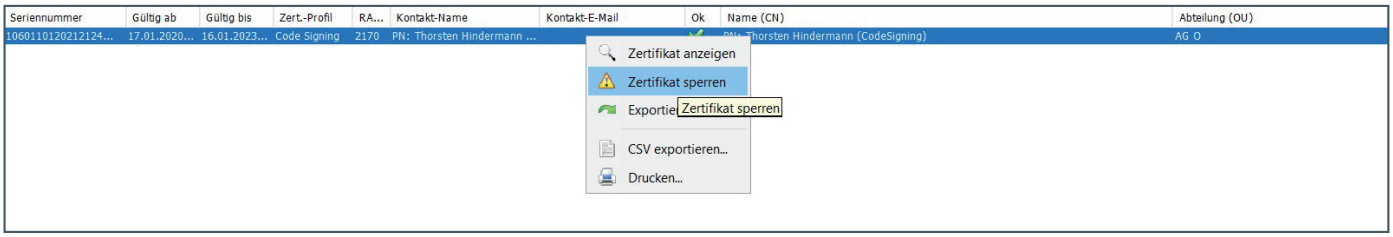


Abb. 27

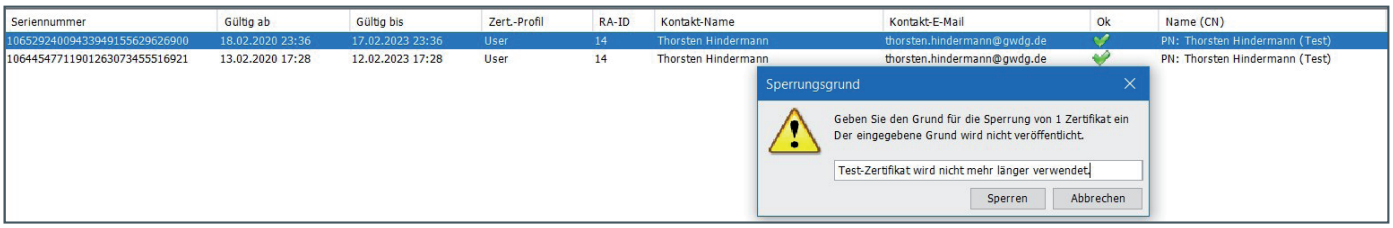


Abb. 28

Abb. 29

diesem Artikel nur kurz vorgestellt wurde, noch einmal genauer beleuchtet werden.

LINKS

[1] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:uniras*

[2] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:mpgras*

[3] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start#zertifikat_beantragen*

[4] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start#zertifikat_abholen*

[5] *https://adoptopenjdk.net/*

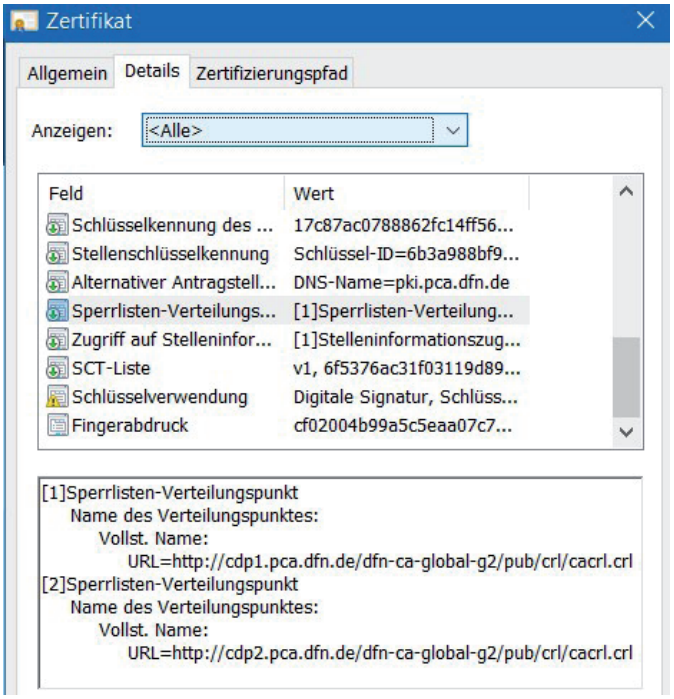
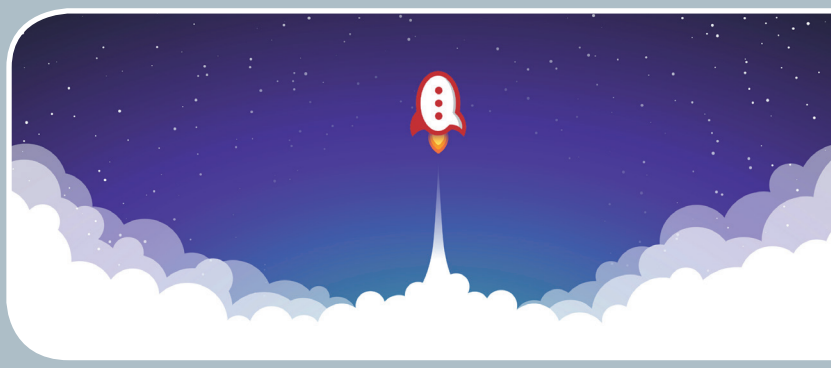


Abb. 30

[6] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:raoperator*
[7] *https://www.conf.dfn.de*
[8] *https://www.pki.dfn.de/fileadmin/PKI/VideoIdent/Richtlinien-Video-Identifizierung-DFN-PKI.pdf*
[9] *https://www.pki.dfn.de/policies/videoident/*
[10] *https://meet.gwdg.de*
[11] *https://www.consilium.europa.eu/prado/de/prado-start-page.html*
[12] *https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP.pdf#page=18*
[13] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start#detaillierte_beschreibung_der_e-mail-verschluesselung_mit_x509-zertifikaten*
[14] *https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start#detaillierte_beschreibung_der_einsatzmoeglichkeiten_von_x509-zertifikaten*

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



Rocket.Chat

Kommunikation leicht gemacht!

Ihre Anforderung

Sie benötigen einen professionellen Chat-Dienst, der eine einfache, persistente Kommunikation mit Kollegen ermöglicht – sowohl in Einzel- als auch in Gruppenunterhaltungen, die komfortabel durchsuchbar sind. Sie wollen Bilder und Dateien mit Kollegen austauschen..

Unser Angebot

Wir betreiben den Messaging-Dienst „Rocket.Chat“, der es Ihnen ermöglicht, sich in Teams, Gruppen oder auch einzeln auszutauschen. Der Dienst unterstützt zusätzlich Emojis, das Versenden von Dateien, Bildern und Videos sowie die Integration von Benachrichtigungen verschiedener Dienste wie z. B. GitLab. Aufgrund einer breiten Palette von Clients, auch für mobile Geräte, sowie einer übersichtlichen Weboberfläche bieten wir komfortablen Zugriff vom Arbeitsplatz und von unterwegs..

Ihre Vorteile

> Einfache Kommunikation im Team
> Persistente, durchsuchbare Chat-Verläufe
> Einfaches Teilen von Dateien und Bildern
> Unterhaltungen mit allen Nutzern, die einen Account bei der GWDG besitzen
> Integrierte Bots und APIs für die Anbindung von GitLab oder die Einbindung von RSS-Feeds

Interessiert?

Jeder Nutzer mit einem gültigen Account bei der GWDG und einem aktuellen Webbrowser oder Client kann den Dienst „Rocket.Chat“ nutzen. Für die Benutzung rufen Sie einfach *https://chat.gwdg.de* auf. Nutzer ohne GWDG-Account können einen Account auf https://www.gwdg.de/registration registrieren.

>> www.gwdg.de/rocket.chat

Entwicklung eines Microservices zur Beantragung von E-Mail-Zertifikaten – ein IHK-Abschlussprojekt

Text und Kontakt:
Nils Buczior
nils.buczior@gwdg.de
0551 201-2190

Herr Nils Buczior hat im Juli seine Ausbildung zum Fachinformatiker für Anwendungsentwicklung bei der GWDG erfolgreich abgeschlossen. Der praktische Teil seiner Abschlussprüfung bestand aus der Durchführung einer 70-stündigen Projektarbeit. Hierfür wurde von ihm ein Microservice für die Beantragung von E-Mail-Zertifikaten implementiert.

AUSBILDUNG BEI DER GWDG

Die GWDG bildet schon seit Jahren Fachinformatiker*innen für Anwendungsentwicklung wie auch für Systemintegration aus. Den angehenden Fachinformatiker*innen werden Techniken und Fähigkeiten vermittelt, die sie für ihren weiteren beruflichen Werdegang benötigen. Für die Anwendungsentwickler*innen ist dies unter anderem der Umgang mit Programmiersprachen, Entwicklungsumgebungen, Bibliotheken und Frameworks. Zusätzlich werden auch die Architektur von Software sowie die Kommunikation zwischen Netzteilnehmern gelehrt.

Der Fokus bei den Programmiersprachen liegt auf C# und Java. C# findet Verwendung bei der Entwicklung des Identity-Management-Portals (IdM) der GWDG (*https://idm.gwdg.de*), während Java die gewählte Programmiersprache für die Web-Entwicklung im Kundenportal der GWDG (*https://www.gwdg.de*) ist.

Während der Ausbildung besuchen die Auszubildenden die Berufsschule. Dies geschieht entweder einen Tag die Woche oder in Blockform. Der Besuch der Berufsschule ist verpflichtend im dualen System der Ausbildung. In der Berufsschule lernen deie-Auszubildenden in den Fächern Netzwerktechnik, Politik, Deutsch, Englisch, Elektrotechnik und Wirtschaft Wissen abseits des Programmierens. Dieses Wissen ist Bestandteil der schriftlichen Abschlussprüfung.

VERLAUF

Ich begann meine Ausbildung zum Fachinformatiker für Anwendungsentwicklung im August 2018. Zuvor hatte ich mein Informatikstudium mit dem Wunsch abgebrochen, praxisnaher zu arbeiten. Auch wenn ich das Studium nicht abgeschlossen habe, konnte ich dennoch viele der dabei erworbenen Fähigkeiten und Erkenntnisse mitnehmen, was zum einen positiv bei meinen Vorstellungsgesprächen bewertet wurde, zum anderen mir auch beim Einstieg in die Ausbildung half.

Trotz meines Vorwissens war es kein leichter Einstieg. Früh kommt man als Auszubildender in den Kontakt mit großen Softwareprojekten. Es dauerte eine Weile, bis ich ein gutes Vorgehen fand, das für mich funktionierte, um beim Einstieg in große Projekte nicht die Übersicht zu verlieren oder sich in den Tiefen des Programmcodes zu verlaufen.

Beim Erlernen neuer Fähigkeiten werden die Auszubildenden von Ausbilder*innen unterstützt und geleitet. Weitere Kolleg*innen teilen ebenfalls ihre Expertise mit den Auszubildenden; sei es Wissen über die Entwicklung von Benutzeroberflächen, Aufbau von Datenmodellen oder die Verwendung bestimmter Frameworks.

Die Auszubildenden und die Ausbilder*innen treffen sich

Graduation Project for an Apprenticeship at the GWDG

In July Mr. Nils Buczior finished his apprenticeship as a Software Developer at the GWDG. The final exam consisted of three parts. A written exam, the development of a 70 hours software project and a presentation of that project. Together with his instructor and two colleagues he decided to implement a microservice to request e-mail certificates. The GWDG already offers certificates to its users, but the current work flow has its flaws and needs to be replaced. For the development he needed to learn how to work with frameworks and libraries involving microservices and handling of certificates and keys. Also, the microservice needed to be connected to the infrastructure of the GWDG, including the Identity Provider for user information. The application used Spring Boot for the back end and Java Server Faces combined with Bootstrap for the front end, while Bouncy Castle was used for most of the key and certificate operations.

wöchentlich, um den Lernfortschritt der Auszubildenden festzustellen, Fragen und Schwierigkeiten zu klären und um einen Plan für die Woche zu erstellen. Hierbei wird auch entschieden, an welchen produktiven Projekten die Auszubildenden teilnehmen werden. Auf diese Weise können die Auszubildenden bereits während ihrer Ausbildung Erfahrungen im produktiven Arbeiten sammeln und ihre zukünftigen Kolleg*innen kennenlernen.

Ein mögliches Projekt ist beispielsweise das IdM-Portal der GWDG. Nach einer Einarbeitungsphase werden den Auszubildenden zunächst kleine Aufgaben gegeben, wie das Überarbeiten eines Algorithmus oder das Erstellen eines Tests für bereits bestehenden Code. Dies geschieht über die Zuweisung eines Issues in GitLab. Im Laufe der Ausbildung werden den Auszubildenden immer größere und komplexere Aufgaben zugeteilt. Bei Fragen und Problemen ist das IdM-Team stets mit Hilfe und Rat zur Stelle.

Um den Auszubildenden einen Einblick in möglichst viele Techniken zu ermöglichen findet jede Woche eine Programmierübung mit einem erfahrenen Kollegen statt. Die gelehrten Techniken reichen von der Programmierung in Assembler und C bis zur Entwicklung im ASP.NET-Framework. Hierbei wird weniger in die Tiefe gegangen, sondern vielmehr steht der Kontakt mit möglichst vielen verschiedenen Bereichen im Vordergrund.

ABSCHLUSSPROJEKT

Am 31. Juli 2020 beendete ich erfolgreich meine Ausbildung. Die IHK-Abschlussprüfung bestand neben einer schriftlichen Prüfung auch aus einem 70-stündigem Projekt und der Dokumentation zu diesem Projekt. Zudem ist eine mündliche Prüfung zum Thema des Projektes Teil der Abschlussprüfung. Zusammen mit meinem Ausbilder, dem Projektleiter für das Kundenportal und dem bei der GWDG zuständigen Registration-Authority-Mitarbeiter erstellten wir eine Liste mit möglichen Themen. Wir entschieden uns für das Projekt, einen Microservice zur Beantragung von E-Mail-Zertifikaten zu entwickeln. Ich begann die Arbeit an dem Projekt im Februar 2020.

.Das Kundenportal der GWDG *https://www.gwdg.de* enthält Informationen für Nutzer*innen zum Beantragungsweg von Zertifikaten. Zudem werden Links zu den Certification Authorities (CAs) der GWDG, der Max-Planck-Gesellschaft und der Universität Göttingen bereitgestellt, sodass sich Kund*innen direkt an die richtige CA wenden können. Die Zertifikate dienen der eindeutigen Identitätsbestimmung der Kommunikationspartner sowie der Signierung und/oder Verschlüsselung von E-Mails und werden erst nach persönlicher Identifikation ausgestellt.

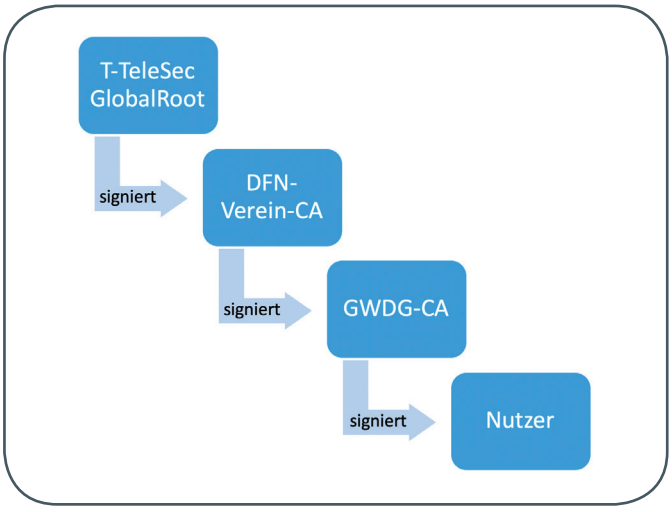
Der Anlass für die Suche nach einer neuen Lösung ist die Fehleranfälligkeit des aktuellen Systems. Unklarheiten bei der Bedienung und menschliche Fehler wie Fehleingabe des Namens der Nutzer*innen trotz ausführlicher Anleitungen im GWDG-Kundenportal führen dazu, dass Teilnehmerservice-Mitarbeiter*innen, kurz TS-MA, Kontakt zum/zur Antragsteller*in aufnehmen müssen, um fehlerhafte Daten zu korrigieren. Die Bedienung ist nicht immer intuitiv und führt zu einer schlechten Benutzererfahrung. Zudem findet eine Weiterleitung zum Webauftritt des DFN statt, was bei manchen Nutzer*innen Sicherheitsbedenken hervorruft. Durch die neue Lösung sollte die Fehleranfälligkeit reduziert werden und der daraus resultierende Arbeitsaufwand für Mitarbeiter*innen ebenfalls verringert werden.

AUFGABENSTELLUNG

Ziel des Projektes war es, einen Microservice für das Kundenportal der GWDG zu implementieren, der die Beantragung von E-Mail-Zertifikaten übernimmt und den aktuellen Ablauf ablöst. Die Bedienung für Nutzer*innen und Administrator*innen sollte vereinfacht werden. Prozesse sollten, soweit möglich, automatisiert werden und der Ablauf sollte nur auf dem Webauftritt der GWDG stattfinden. Nutzerinformationen sollten vom Identity Provider (IdP) der GWDG geliefert werden. Die Verantwortung für die Sicherheit des Zertifikats bzw. des generierten privaten Schlüssels sollte bei dem/der Nutzer*in liegen. Die Benutzeroberfläche wurde während des Projekts aus Zeitgründen lediglich als Proof of Concept erstellt und wird zu einem späteren Zeitpunkt überarbeitet.

Ein digitales Zertifikat ist ein elektronisches Dokument, das verwendet wird, um zu beweisen, dass man Eigentümer*in eines öffentlichen Schlüssels ist. Das Zertifikat enthält Informationen über die Identität des/der Eigentümer*in und die digitale Signatur einer Entität, die die Identität des/der Eigentümer*in bestätigt. Das Projekt verwendet den Standard X.509. Dieser ist der meistverwendete Standard für E-Mail-Zertifikate. Ein X.509-Zertifikat setzt sich zusammen aus einem signierten öffentlichen Schlüssel und einem privaten Schlüssel.

Das Zertifikat wird von der Certification Authority (CA) der GWDG ausgestellt. Die CA ist Teil einer Public Key Infrastructure (PKI; siehe Abbildung 1). Dies ist eine hierarchische Struktur. Jedes Zertifikat, das von einer CA innerhalb einer PKI ausgestellt wird, beinhaltet eine Vertrauenskette. Diese Vertrauenskette repräsentiert den Aufbau der PKI und hat ihren Ursprung im Wurzelzertifikat. In Falle der GWDG liegt dies bei der Deutschen Telekom. Von hier verläuft die Vertrauenskette über die CA des DFN, die CA der GWDG und endet bei dem/der Nutzer*in.



1_Public Key Infrastructure

UMSETZUNG

Die Beantragung eines Zertifikats gliedert sich in drei Schritte. Im ersten Schritt wählt der Benutzer den entsprechenden Punkt im Kundenportal aus.

Seine Daten werden vom Identity Provider der GWDG als JSON-Web-Token geliefert (siehe Abbildung 2). Die Nutzerinformationen werden aus dem Token extrahiert und dem Zertifikatantrag beigelegt. Dieses Vorgehen hat den Vorteil, dass die menschliche

Fehlerquelle entfernt wird.

Mit Hilfe der Bibliothek Bouncy Castle wird ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, erzeugt. Der private Schlüssel wird kodiert bei dem/der Nutzer*in abgelegt. Der öffentliche Schlüssel wird über eine Simple Object Access Protocol (SOAP)-Schnittstelle an die GWDG-Test-CA geschickt und dort signiert. Über dieselbe Schnittstelle schickt die GWDG-Test-CA eine PDF-Datei an den Microservice, welcher die PDF-Datei per E-Mail an den/die Nutzer*in weiterleitet. Diese PDF-Datei muss von dem/der Nutzer*in unterschrieben und dann der Registration Authority (RA) vorgelegt werden.

Dies ist der zweite Schritt des Vorgangs – die persönliche Identifikation. Hier werden die Informationen des ausgedruckten PDFs mit den Informationen auf dem Personalausweis des/der Nutzer*in verglichen. Wenn die Informationen übereinstimmen, gibt der/die Teilnehmerservice-Mitarbeiter*in den Antrag frei.

Nach erfolgreicher Identifikation beginnt der letzte Schritt. Der/die Nutzer*in kann nun im Kundenportal mit einem Klick auf den entsprechenden Menüpunkt sein/ihr Zertifikat erhalten. Hierbei wird der kodierte private Schlüssel des Nutzers mit dem signierten öffentlichen Schlüssel von der CA zu einem X.509-E-Mail-Zertifikat im *pkcs12*-Format zusammengefügt. Dieses wird über das JSF-Framework und das Liferay-Framework dem/der Nutzer*in zum Download angeboten.

TECHNIKEN

Für die Entwicklung des Microservices wurde die Integrated Development Environment (IDE) IntelliJ IDEA von JetBrains verwendet. Das Projekt wurde mithilfe des Spring Boot Frameworks in Java entwickelt. Spring Boot ist ein Open-Source-Framework, das den Java-Entwickler dabei unterstützt, eine produktionsfertige, eigenständige Anwendung zu erstellen. Spring Boot zeichnet sich durch seine hohe Flexibilität und seine einfache Konfiguration aus.

Der Prototyp der Benutzeroberfläche wurde mit den Frameworks Java Server Faces (JSF) und Bootstrap erstellt. JSF ist ein Framework-Standard, der zur Entwicklung von Benutzeroberflächen für Web-Anwendungen verwendet wird. Bootstrap ist ein Open-Source-Framework, das Cascading Style Sheets (CSS)- und Java Script-Vorlagen liefert. Diese erleichtern die Implementierung von Grundfunktionen einer Webseite.

Tomcat von Apache Software Foundation dient als Servlet-Container für die Anwendung.

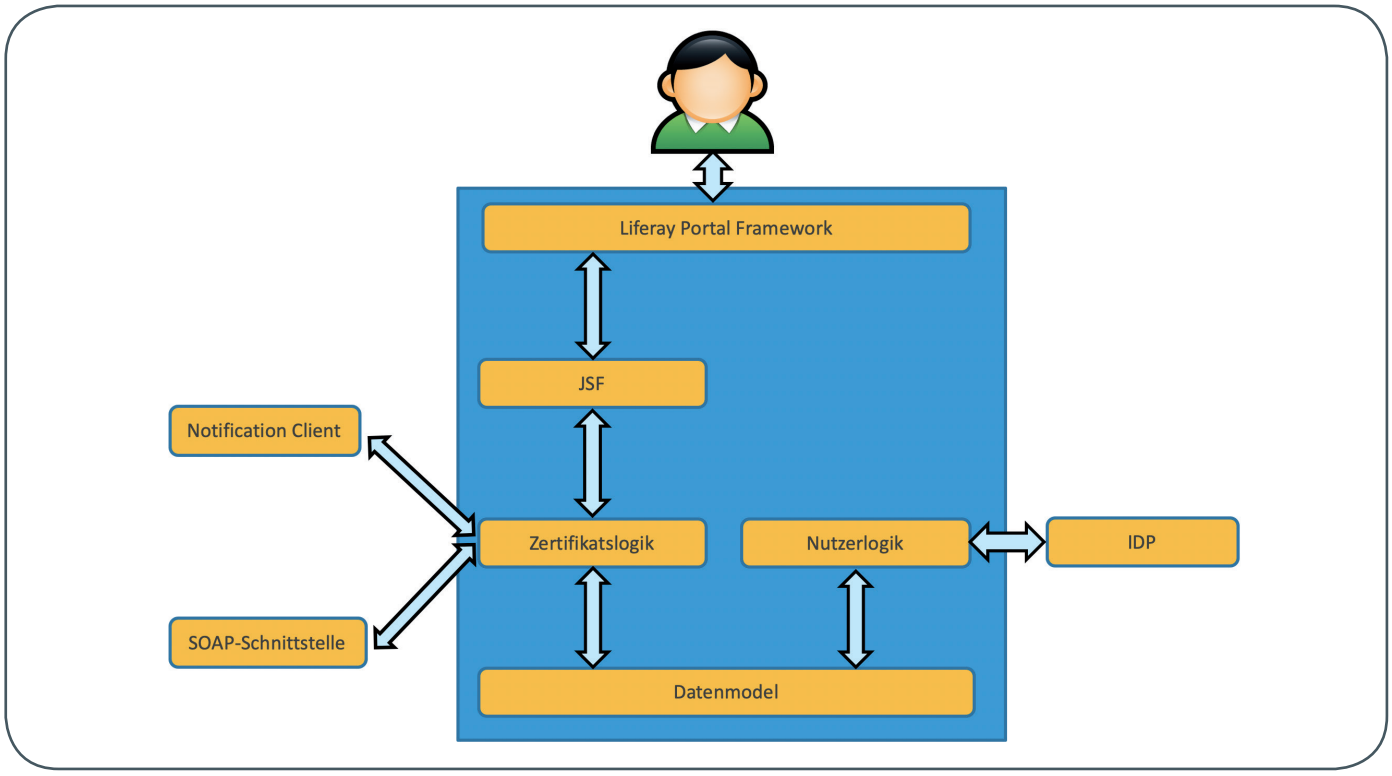
Die Kommunikation zwischen dem Microservice und der GWDG-Test-CA findet über den SOAP-Client statt. Dieser setzt die Bibliothek Bouncy Castle für seine Verwendung voraus. Bouncy Castle vervollständigt die standardmäßige Java-Erweiterung Java Cryptographic Extension (JCE) mit weiteren Verschlüsselungsalgorithmen und Komponenten für diverse Zertifikatprotokolle. Bouncy Castle wurde im Projekt für den Großteil der Schlüssel- und Zertifikatsoperationen verwendet.

Um die Wartbarkeit zu maximieren, wurde das Build-Management-Tool Maven eingesetzt. Maven erlaubt dem Entwickler, Versionen von eingebundenen Bibliotheken und Frameworks mit der Änderung eines Wertes in der Konfigurationsdatei *pom.xml* zentral vorzunehmen, ohne dass der Programmcode durchgesehen werden muss.

HERAUSFORDERUNGEN

Für die Durchführung des Projektes war die Arbeit mit Frameworks und Bibliotheken essenziell. Teilweise hatte ich bereits Erfahrung mit ihrer Verwendung, aber mit vielen hatte ich noch nicht gearbeitet. Diese Herausforderung und die Einarbeitung nahmen einen beachtlichen Teil der 70 Stunden ein.

Die Arbeit mit Zertifikaten war für mich Neuland. Ich hatte zwar ein Grundwissen über deren Funktionsweise, aber für die



2_Programmarchitektur

Projektarbeit war ein deutlich fundierteres Wissen erforderlich. Der Registration-Authority-Mitarbeiter unterstützte mich hierbei tatkräftig. Er half mir, die Zertifikatoperationen zu implementieren und erklärte mir die Abläufe bei der Beantragung. Zudem unterstützte er mich bei der Erstellung und Installation von Testzertifikaten.

Die Projektarbeit war mein erstes selbstgeplantes und durchgeführtes Projekt, daher war mein vorher erstellter Zeitplan an einigen Stellen nicht realistisch. Einige Projektphasen waren deutlich schneller abzuschließen und andere benötigten mehr Zeit als zuvor geplant.

Die angefertigte Projektdokumentation über die geleistete Arbeit ist der Teil, der am Ende von der Industrie- und Handelskammer (IHK) bewertet wird. Sie umfasst rund 15 Seiten und beinhaltet neben einer Beschreibung der einzelnen Projektphasen auch Ist- und Soll-Analysen, Abbildungen und Diagramme.

FAZIT

Die Projektarbeit war eine interessante Erfahrung, die mir auch viel Spaß gemacht hat. Das Thema war gut gewählt, da es Wissen aus vielen Bereichen erforderte und ich so in den Kontakt mit vielen Bereichen kam. Gleichzeitig konnte ich aber auch mein gelerntes Wissen und Techniken einsetzen, was mir meine Fortschritte als Softwareentwickler verdeutlichte. Zudem fand ich die Themen Verschlüsselung und Sicherheit sehr spannend. Es gab auch schwierige und mitunter frustrierende Phasen, aber dank der Unterstützung meiner Kolleg*innen, die mir mit Rat und Tat zur Seite standen, waren auch diese zu bewältigen.

Das Projekt war zudem eine gute Erfahrung, wie es ist, nach Kundenwunsch genaue Anforderungen zu erfüllen. Hierfür wurden Lasten- und Pflichtenhefte angefertigt, die der Dokumentation beiliegen.

Ich bin sehr zufrieden und stolz auf meine Arbeit und die Bewertung der IHK bestätigte dies. Es war eine Erfahrung, an die ich mich gerne zurückerinnere. Nach meiner Ausbildung bei der GWDG fühle ich mich gut für meinen weiteren beruflichen Werdegang vorbereitet. Ich denke, dass ich viele essenzielle Techniken gelernt habe und mir die nötigen Werkzeuge zur Verfügung stehen. Besonders positiv für mich war die Kombination aus produktivem Arbeiten und geleitetem Lernen.

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

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 Nutzern.

>> www.gwdg.de/software

Stellenangebot
Nr. 20201126

Die GWDG sucht ab sofort zur Verstärkung des High-Performance-Computing-Teams der Arbeitsgruppe „eScience" (AG E) zwei

IT-Systembetreuer *innen (m/w/d)

mit 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 E11 vorgesehen. Die Stelle ist grundsätzlich auch für Teilzeitkräfte geeignet und zunächst auf zwei Jahre befristet. Eine Verlängerung nach Ablauf der zwei Jahre ist möglich.
Die Bereitstellung von leistungsfähigen HPC-Systemen gehört seit über 40 Jahren zu unseren Aufgaben. Seit 2018 betreiben wir im Auftrag der Universität Göttingen den HLRN-IV, den schnellsten Superrechner Norddeutschlands und Platz 5 in Deutschland. Ab 2021 wird die GWDG einen weiteren Superrechner für das Deutsche Zentrum für Luft- und Raumfahrt e. V. (DLR) betreiben und sucht dafür Ihre Unterstützung im Team!

Aufgabenbereiche

- Einarbeitung in neues Fachwissen
- Vorbereitung und Überwachung der Rechnerrauminfrastruktur
- Bauseitige Begleitung der Aufbauarbeiten
- Begleitung der technischen Abnahmetests
- Technische Systemüberwachung und -betreuung
- Übernahme von Wartungs- und Pflegearbeiten
- Zusammenarbeit mit dem Hersteller und der Gebäudetechnik

Anforderungen

- Erfolgreich abgeschlossene Ausbildung, ein abgeschlossenes Studium oder gleichwertige Fähigkeiten und Erfahrungen im IT-Bereich
- Erfahrung mit der Administration von Linux-Servern
- Gutes analytisches Denkvermögen
- Selbstständige, strukturierte und systematische Arbeitsweise
- Ausgeprägte Team- und Kommunikationsfähigkeit
- Gute Deutsch- und Englischkenntnisse in Wort und Schrift

Wünschenswert

- Erfahrung mit der Arbeit in einem Rechenzentrum
- Interesse an Computerhardware und Elektronik
- Interesse an IT-Sicherheit
- Supporterfahrung

Unser Angebot

- Flexible Arbeitszeiten und Möglichkeit zum mobilen Arbeiten
- Mitarbeit in einem engagierten Team
- Außergewöhnliches Arbeitsumfeld mit großer Nähe zu Wissenschaft und Forschung
- Eine interessante, vielseitige Tätigkeit in einem großen, international agierenden IT- Kompetenzzentrum
- Qualifizierung und Weiterentwicklung Ihrer Fähigkeiten
- Im öffentlichen Dienst übliche Sozialleistungen, wie z. B. Betriebsrente mit zusätzlicher Erwerbsminderungs- und Hinterbliebenenversorgung

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 bis zum **31.01.2021** über unser Online-Formular unter *https://s-lotus.gwdg.de/gwdgdb/age/20201126.nsf/bewerbung*.

Fragen zur ausgeschriebenen Stelle beantwortet Ihnen:

Herr Dr. Christian Boehme
Tel.: 0551 201-1839
E-Mail: *christian.boehme@gwdg.de*

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Personalia

NEUE MITARBEITERIN JASMIN OSTER

Seit dem 15. August 2020 unterstützt Jasmin Oster die Arbeitsgruppe „Basisdienste und Organisation“ (AG O) und übernimmt vor allem Aufgaben im Rahmen des PIM-Projektes übernehmen. Ziel ist der Aufbau einer Plattform zur Unterstützung der internationalen Studierendenmobilität. Als Teil des Entwicklungs-Teams liegt der Schwerpunkt ihrer Aufgaben im Bereich der Softwareentwicklung und der Weiterentwicklung von CI/CD. Jasmin Oster ist per E-Mail unter *jasmin.oster@gwdg.de* zu erreichen.

Hilker

NEUER MITARBEITER DANIEL ELKELES

Seit dem 1. Oktober 2020 verstärkt Herr Daniel Elkeles die Arbeitsgruppe „Anwendungs- und Informationssysteme“ (AG A) als wissenschaftlicher Mitarbeiter. Er hat an der Georg-August-Universität Göttingen Physik mit Schwerpunkt Astrophysik studiert und in seiner Masterarbeit die Entwicklung von Sternen in Galaxien in einem „Fuzzy Dark Matter“-Modell untersucht. Seine Aufgabenschwerpunkte liegen sowohl im Bereich der Systemadministration für das Max-Planck-Institut für Wissenschaftsgeschichte (MPI-WG) in Berlin als auch im Bereich der Anwendungssysteme BigBlueButton und GitLab. Herr Elkeles ist per E-Mail unter *daniel.elkeles@gwdg.de* zu erreichen.

Krimmel

NEUER MITARBEITER PASCAL UPHAUS

Seit dem 15. Oktober 2020 verstärkt Herr Pascal Uphaus die Arbeitsgruppe „Anwendungs- und Informationssysteme“ (AG A) als studentische Hilfskraft. Er studiert zurzeit Wirtschaftsinformatik an der Georg-August-Universität Göttingen. Sein Aufgabenschwerpunkt liegt im Aufbau und Betrieb des Bibliothekssystems Koha. Herr Uphaus ist per E-Mail unter *pascal.uphaus@gwdg.de* zu erreichen.

Krimmel

NEUER MITARBEITER GREGOR THIEM

Seit dem 1. November 2020 ist Herr Gregor Thiem als studentische Hilfskraft in der Arbeitsgruppe „Anwendungs- und Informationssysteme“ (AG A) tätig. Herr Thiem studiert zurzeit Wirtschaftsinformatik an der Georg-August-Universität Göttingen. Dort unterstützt er bereits verschiedene Abteilungen bei der Systemadministration und als Netzwerkbeauftragter. Sein Aufgabenschwerpunkt liegt bei der Unterstützung der Teams für die beiden Dienste „Webhosting“ und „GWDG Pad“. Herr Thiem ist per E-Mail unter *gregor.thiem@gwdg.de* zu erreichen.

Krimmel

INFORMATIONEN:
support@gwdg.de
0551 201-1523

Januar bis Juli 2021

Academy

KURS	DOZENT*IN	TERMIN	ANMELDEN BIS	AE
GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP	Töpfer	16.02. – 17.02.2021 9:30 – 16:00 Uhr	09.02.2021	8
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	23.02. – 24.02.2021 9:00 – 12:00 und 13:00 – 15:30 Uhr	16.02.2021	8
ADMINISTRATION VON WINDOWS-PCS IM ACTIVE DIRECTORY DER GWDG	Quentin	11.03.2021 9:00 – 12:30 und 13:30 – 15:30 Uhr	04.03.2021	4
STATISTIK MIT R FÜR TEILNEHMER MIT VORKENNTNISSEN – VON DER ANALYSE ZUM BERICHT	Cordes	16.03. – 17.03.2021 9:00 – 12:00 und 13:00 – 15:30 Uhr	09.03.2021	8
INDESIGN – GRUNDLAGEN	Töpfer	23.03. – 24.03.2021 9:30 – 16:00 Uhr	16.03.2021	8
EINFÜHRUNG IN DIE PROGRAMMIERUNG MIT PYTHON	Sommer	13.04. – 15.04.2021 9:30 – 16:00 Uhr	06.04.2021	12
USING THE GWDG SCIENTIFIC COMPUTE CLUSTER – AN INTRODUCTION	Boden, Khuziyakhmetov	19.04.2021 9:30 – 16:00 Uhr	12.04.2021	4
PARALLEL PROGRAMMING WITH MPI	Prof. Haan	20.04. – 21.04.2021 9:15 – 17:00 Uhr	13.04.2021	8
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	21.04. – 22.04.2021 9:00 – 12:00 und 13:00 – 15:30 Uhr	14.04.2021	8

KURS	DOZENT*IN	TERMIN	ANMELDEN BIS	AE
PROGRAMMING WITH CUDA – AN INTRODUCTION	Prof. Haan	27.04.2021 9:15 – 17:00 Uhr	20.04.2021	4
XUBUNTU-LINUX: XFCE-DESKTOP ALS ALTERNATIVE ZU POPULÄREN KOMMERZIELLEN BETRIEBSSYSTEMEN	Dr. Heuer	29.04.2021 9:00 – 12:00 und 13:30 – 15:30 Uhr	22.04.2021	4
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	05.05. – 06.05.2021 9:00 – 12:00 und 13:00 – 15:30 Uhr	28.04.2021	8
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	18.05. – 19.05.2021 9:30 – 16:00 Uhr	11.05.2021	8
INDESIGN GRUNDKURS – SCHWERPUNKT POSTERGESTALTUNG	Töpfer	02.06. – 03.06.2021 9:30 – 16:00 Uhr	26.05.2021	8
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	09.06. – 10.06.2021 9:00 – 12:00 und 13:00 – 15:30 Uhr	02.06.2021	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	24.06.2021 9:15 – 12:00 und 13:00 – 16:00 Uhr	17.06.2021	4
INDESIGN – AUFBAUKURS	Töpfer	29.06. – 30.06.2021 9:30 – 16:00 Uhr	22.06.2021	8
STATISTIK MIT R FÜR TEILNEHMER MIT VORKENNTNISSEN – VON DER ANALYSE ZUM BERICHT	Cordes	07.07. – 08.07.2021 9:00 – 12:00 und 13:00 – 15:30 Uhr	30.06.2021	8

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
Alle Kurse finden in geeigneten Räumlichkeiten am Göttingen Campus statt. Den genauen Ort entnehmen Sie bitte der jeweiligen Kursbeschreibung. 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.


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen