


GWDG NACHRICHTEN 12|19

FAIR Digital Objects und
Data Type Registries

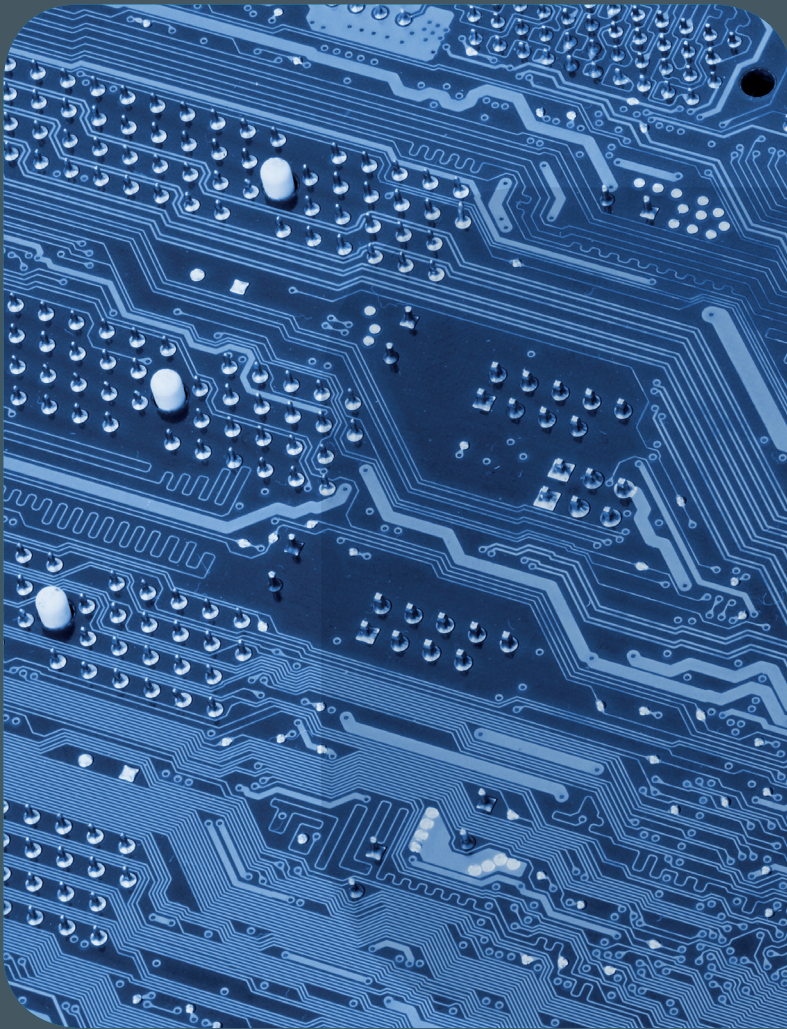
E-Mail-Verschlüsselung

Cryptomator

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG



*Frohe Weihnachten
und einen guten
Rutsch ins neue Jahr!*



GWDG NACHRICHTEN

12|19 Inhalt

.....

4 FAIR Digital Objects und Data Type Registries
9 E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 1: Beantragung und Sicherung von Zertifikaten **16 Tipps & Tricks** **20 Kurz & knapp**
22 Stellenangebot **23 Personalia**

Impressum

.....

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
42. Jahrgang
Ausgabe 12/2019

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
550

Fotos:

© Angelov - stock.adobe.com (1)
© fotogestoerber - Fotolia.com (8)
© pineapple - Fotolia.com (15)
© edelweiss - Fotolia.com (19)
© momius - Fotolia.com (21)
© contrastwerkstatts - Fotolia.com (22)
© MPLbpc-Medienservice (3, 23)
© GWDG (2, 20)

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:

Franziska Schimek
E-Mail: franziska.schimek@gwdg.de

Druck:

Kreationszeit GmbH, Rosdorf



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

Liebe Kunden und Freunde der GWDG,

vor einigen Tagen ist die erste Ausschreibung zum Aufbau einer Nationalen Forschungsdateninfrastruktur (NFDI) zu Ende gegangen. Ich hatte hierzu bereits im letzten Jahr einige Zeilen geschrieben. Die Ausschreibung geht insbesondere auf eine Empfehlung des Rates für Informationsinfrastrukturen (RfII) zurück, der im Auftrag der Gemeinsamen Wissenschaftskonferenz (GWK) eine systemische Betrachtung des deutschen Wissenschaftssystems vornimmt.

In seinen Empfehlungen „Leistung aus Vielfalt“ aus dem Jahr 2016 wurde unter anderem festgehalten, dass die Ausprägung von Infrastrukturen zum Forschungsdatenmanagement eine komplexe Gemeinschaftsaufgabe ist, die neue Förderinstrumente mit dem Ausblick auf eine dauerhafte Finanzierung benötigt. Mit der Ausschreibung wird eine wissenschaftsgetriebene Entwicklung von fachdisziplinären Communities angestoßen, da generische Dienste bisher nur eine begrenzte Verbreitung gefunden haben. Damit ist nicht verbunden, dass solche Communities neue Datenzentren ausprägen sollen, sondern Partnerschaften zu bestehenden Dienstleistungseinrichtungen finden, um Synergien zu vorhandenen Infrastrukturen zu nutzen und diese bedarfsorientiert anzupassen. Mit dem Ende der ersten Ausschreibungsrunde gehen nun die ersten NFDI-Konsortien in die Begutachtung. Im kommenden Jahr werden diese ihre Arbeit aufnehmen können und man darf gespannt sein, wie sich dieses Format entwickeln wird.

Bis dahin wünsche Ihnen und Ihren Familien schöne Feiertage und einen erfolgreichen Start in das neue Jahr.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

FAIR Digital Objects und Data Type Registries

Text und Kontakt:

Dr. Ulrich Schwardmann
ulrich.schwardmann@gwdg.de
0551 201-1542

Die FAIR-Prinzipien haben in letzter Zeit viel Aufmerksamkeit als Rahmenstruktur für die Nachhaltigkeit von Daten, insbesondere wissenschaftlicher Daten, bekommen. Für die Prozesse, Daten zu finden (Find), auf sie zuzugreifen (Access), sie über verschiedene Bereiche hinweg zu nutzen (Interoperate) und sie wiederzuverwenden (Reuse), spielte Maschinentauglichkeit bei FAIR immer schon eine wichtige Rolle. Aber die gegebenen Policies selbst können nicht viel über die Automatisierung von Prozessen sagen. Ein eher technischer Ansatz einiger früher Research Data Alliance [1] (RDA) Arbeitsgruppen führte allerdings zum Begriff des Digitalen Objektes (DO) und es stellte sich heraus, dass die vorgesehene Struktur dieser Digitalen Objekte eine komplementäre Sicht aus dem eher technischen Blickwinkel auf viele Aspekte von FAIR erlaubt. Nach einer tieferen Analyse und Intergration dieser Konzepte intensivierte eine Gruppe, genannt GEDE, von ca. 150 europäischen Datenexperten aus etwa 50 Forschungsinfrastrukturen die Diskussion um die sogenannten FAIR Digital Objects. Die Komponenten dieser FAIR-DOs und ihre Potenziale sollen hier beschrieben werden. Welche Services innerhalb dieses Rahmens von der GWDG bereitgestellt werden und wie die deutsche wissenschaftliche Community daran partizipieren kann, wird hier ebenfalls gezeigt.

PIDS ALS NOTWENDIGE ABSTRAKTION IN DER DATEN-DOMÄNE

An Automatisierung führt kein Weg vorbei

Verschiedene Studien in relevanten Datenanalyseprojekten, zum Beispiel eine Erhebung von RDA Europe von 2013, kommen zu dem Ergebnis, dass bis zu 80 % der Zeit, die Experten mit Daten verbringen, mit Daten-Hickhack, insbesondere bei der Aufbereitung der Daten für Analytics, verschwendet werden. Dies deutet darauf hin, dass nur ein hoher Automatisierungsgrad auf Basis einfacher Strukturen eine Alternative zu dieser hochineffizienten und fehleranfälligen Art der Datenverarbeitung darstellen kann.

Das Haupthindernis für die Automatisierung ist die Heterogenität und Komplexität der Daten und Abstraktion ist ein generischer Weg, diese Heterogenität und Komplexität durch Kapselung und Virtualisierung zu verbergen.

Kapselung und Virtualisierung

Durch die **Kapselung** werden Details ausgeblendet, die auf einer bestimmten Ebene nicht benötigt werden. Zum Beispiel auf der Ebene der Dateninfrastruktur gibt es keinen Unterschied zwischen Daten, Metadaten, Software, semantischen Behauptungen usw. Alle können als eine Art von Daten angesehen werden, zum Beispiel als Dateien in einem Dateisystem, die kopiert, geändert oder gelöscht werden. Auf dieser Ebene unterscheiden die

Operationen nicht zwischen Metadaten und Daten, während auf einer Datenverwaltungs- und Wiederverwendungsschicht eine Unterscheidung erforderlich ist. Hier müssen Metadaten verwendet

FAIR Principles and Digital Objects

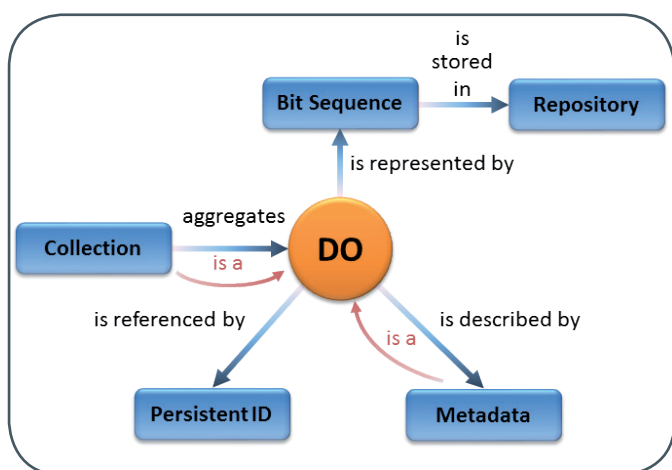
The FAIR principles gained a lot of attention as a framework for the sustainability of data, in particular scientific data. Machine actionability, the capability of computational systems to find, access, interoperate and reuse data and services without human intervention, was always in the focus of FAIR. But the policy framework itself cannot say much about automated processes. However a more technical approach of some of the Research Data Alliance (RDA) working groups lead to the notion of digital objects and it turned out that their intended structure has a complementary view on several aspects of FAIR from a technical perspective. After a deeper analysis and integration of these concepts a group involving 150 of European data experts from about 50 research infrastructures intensified the discussion on so called FAIR DOs. We will describe the components of this framework and its potential here, and also which services inside this framework are provided by GWDG and how the German scientific community can participate.

werden, um die Verwaltungsvorgänge für Daten zu steuern.

Durch **Virtualisierung** ersetzt man Objekte durch ihre logische Darstellung. Die abstrakteste Art der logischen Repräsentation ist der Pointer, der auf das Objekt zeigt, ein klassischer und in der Informatik häufig verwendeter Ansatz, der alle Komplexität hinter einem reinen Bezug zum Objekt verbirgt. Bei Virtual Machines als weiteres Virtualisierungsbeispiel verbirgt man nur die Hardware in der logischen Darstellung, zeigt aber dennoch den größten Teil der internen Struktur.

Digital Objects

Ein erster Schritt der Abstraktion, also der Virtualisierung und Kapselung von Daten, ist die Identifizierung von minimalen Elementen, die aus Sicht der Datenverwaltung und -wiederverwendung als atomar angesehen werden können. Bereits vor fünf Jahren wurden diese Elemente von der RDA-Arbeitsgruppe „Datengrundlagen und Terminologie“ als Digitale Objekte (DO) bezeichnet. Sie können als eine gewisse Verallgemeinerung von Dateien in lokalen Dateisystemen oder Streams von Streaming-Providern betrachtet werden, und sie sind in eine Struktur anderer wichtiger Datenkonzepte eingebettet, wie man in Abbildung 1 sehen kann.



1_Das Digitale Objekt (DO), eingebettet in eine Struktur anderer wichtiger Datenelemente und Konzepte.

Wie man jedoch die logische Struktur Digitaler Objekte mit der richtigen Abstraktionsebene abbildet, ist in ihren Details noch Gegenstand der Diskussion. Wie wir bereits gesehen haben, hängt es sicherlich davon ab, wie viel von der logischen Struktur durch die Kapselung hinter einer bestimmten Schicht verborgen ist. Und es wird auch teilweise von den Daten selbst, spezifischen Workflows und Anwendungsfällen der Datenverwaltung und -wiederverwendung abhängen.

Aber auf jeden Fall spielt der Pointer als abstrakteste logische Repräsentation eine herausragende Rolle, und da Daten domänen- und standortübergreifend verfügbar sind und sein müssen, muss der Pointer eine weltweit eindeutige Referenz sein.

Eine globale Referenz als URL könnte als die einfachste Option angesehen werden, aber URLs sind unvorhersehbare instabile Referenzen, da sie sich ändern, wenn sich der Standort der Daten ändert. Siehe auch [2] für eine tiefere Analyse dieses Problems und seiner Folgen für die wissenschaftliche Reproduzierbarkeit. Dieses Problem ist den Bibliothekaren seit vielen Jahren bekannt und wird gleichsam im Begriff „Shelfmark“ dokumentiert, der ursprünglich von der Marke für die Position eines Buches im Regal stammt.

Nach kurzer Zeit stellte sich heraus, dass es keinen Sinn macht, das Buch immer am gleichen Ort zu platzieren. Eine Ebene der Redirektion wurde eingeführt und Regalmarken wurden zu symbolischen Einträgen in einem Katalog.

Diese zusätzliche Ebene der Redirektion ist im Wesentlichen die Begründung für persistente Identifikatoren (PIDs, englisch Persistent Identifiers). Vordergründig sind sie lediglich global eindeutige Zeichenketten ohne Semantik, aber jede dieser Zeichenketten hat einen Datensatz in einer Datenbank, der zum Objekt führt, z. B. über den URL. Wenn dieser sich ändert, kann und muss der Datenbankeintrag geändert werden. Diese PIDs gelten als der richtige Weg, um Objekte zu referenzieren. Um den Pfad zum Objekt aus der Identifizierungs-Zeichenkette als Referenz zu erhalten, spricht man von Auflösung. Und da es sich um globale Referenzen handelt, müssen sie global auflösbar sein, d. h. es muss einen einfachen, global organisierten Weg geben, der zum verwiesenen Objekt führt. Andernfalls wären diese Referenzen keine Pointer im Sinne einer logischen Repräsentation in der Informatik.

Glücklicherweise sind solche persistenten Identifikatoren bereits weit verbreitet als globale Referenzen in mehreren Bereichen der Datenverwaltung und -veröffentlichung und verschiedene hochzuverlässige, globale Infrastrukturen sind seit vielen Jahren verfügbar. Die meisten dieser PID-Infrastrukturen bieten selbst keine globale Auflösung, aber eines dieser bewährten Systeme, das Handle-System [3], verfügt über einen eigenen, hochskalierbaren globalen Auflösungsmechanismus. Somit sind die PIDs des Handle-Systems in der Lage, die Rolle des Pointers als logische Darstellung digitaler Objekte tatsächlich zu erfüllen.

DAS FAIR DIGITAL OBJECT FRAMEWORK

Die FAIR-Prinzipien

Der FAIR-Ansatz wurde später, vor etwa drei Jahren, als „Daten und Dienstleistungen, die sowohl für Maschinen als auch für Menschen auffindbar, zugänglich, interoperabel und wiederverwendbar sind“ definiert. Dies wurde in fünfzehn Prinzipien [4] (siehe auch [5]) formuliert und diese FAIR-Grundsätze sind bereits Teil der Roadmap der European Open Source Cloud (EOSC) geworden, wie man in [6] sehen kann. Die meisten dieser Prinzipien wiederholen als Regelwerk erneut die starke Beziehung zwischen Metadaten, den Daten oder Digitalen Objekten selbst und dem persistenten Identifikator, wie bereits in Abbildung 1 beschrieben. Aber sie gehen noch weiter, indem sie beispielsweise erklären, dass Metadaten den Datenidentifikator (siehe F4 der FAIR-Prinzipien) angeben müssen und dass (Meta-)Daten durch ihren Identifikator über ein standardisiertes Kommunikationsprotokoll (siehe A1 der FAIR-Prinzipien) abrufbar sind.

Dies zeigt einerseits die starke Kopplung zwischen Digitalen Objekten und den FAIR-Prinzipien, andererseits sind die Ansätze aber konzeptionell auf ganz unterschiedlichen Ebenen: Die FAIR-Prinzipien sind Richtlinien, während die Digitalen Objekte technische Abstraktionen sind. Dies deutet darauf hin, dass eine tiefe Vernetzung beider Ansätze äußerst fruchtbar sein kann, da konkrete Implementierungen von Digitalen Objekten automatisch zu Datenstrukturen führen werden, die zumindest teilweise den Richtlinien entsprechen. Die Idee, diese Kopplung zu vertiefen und FAIR Digital Objects (FAIR-DOs) als Digitale Objekte zu beschreiben, die alle FAIR-Prinzipien erfüllen, wurde unter anderem von der GEDE Digital Object Topic Group [7] durchgeführt und ist auch in [8] beschrieben.

Persistent Identifier, Handles und DOIs

Wie bereits erwähnt, spielt der persistente Identifikator als Zeiger eine herausragende Rolle im Abstraktionsprozess sowie in den FAIR-Prinzipien und damit im Framework für die Digitalen Objekte im Zusammenhang mit FAIR. Zusätzlich gibt es klare Vorteile, das Handle-System als PID-Technologie zur Beschreibung von FAIR-DOs einzusetzen. Die sogenannten Digital Object Identifier (DOI), die hauptsächlich für die Veröffentlichung von Artikeln oder Daten verwendet werden, sind übrigens ebenfalls Handles mit bestimmten zusätzlichen Richtlinien. Aber Handles können einen viel breiteren Anwendungsbereich haben, und die Richtlinien, die für Veröffentlichungen notwendig sind, sind nicht immer flexibel genug, um die Bedürfnisse der Datenverwaltung oder des Datenaustausches zwischen Forschern zu erfüllen.

Daher gibt es den Bedarf nach anderen Governance-Strukturen für Handles, um zuverlässige PID-Dienste mit einer viel höheren Flexibilität bei der PID-Nutzung und bei den Richtlinien zu gewährleisten. Die GWDG ist Gründungsmitglied von ePIC, dem PID-Consortium for eResearch, einem internationalen Konsortium aus leistungsstarken Rechenzentren und Communities, um zuverlässige PID-Dienste für die internationale Forschungsgemeinschaft auf Basis des Handle-Systems anzubieten. Die GWDG besitzt zusätzlich den Identifikator-Präfixraum 21. für PIDs im Namen von ePIC als Mitglied von DONA, einer Schweizer Stiftung, die das Global Handle Registry, den Root-Service für die Handle-Auflösung, überwacht. Auf diese Weise kann die GWDG im Auftrag von ePIC eine beliebige Anzahl von Präfixen verwalten und jeder von ihnen kann für eine beliebige Anzahl von PIDs verwendet werden. In diesem Rahmen bietet die GWDG PID-Dienste für stabile wissenschaftliche Datenreferenzen für die deutschen Forscher an.

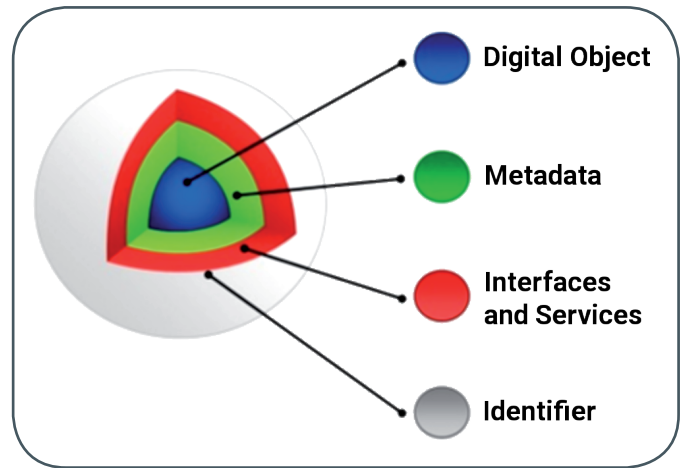
Data Types

Neben der Virtualisierung durch Referenz ist es entscheidend, eine auch für Maschinen verständliche Beschreibung des Objekts zu liefern, um die derzeit sehr ineffiziente Art des Daten-Handlings zu überwinden und flexible Dienste für DOs in wissenschaftlichen Workflows auszuwählen und vorzubereiten. Und es wäre hilfreich, wenn dies bereits auf der Referenzebene möglich wäre.

Man kennt dieses Prinzip bereits aus der einfachen Charakterisierung Digitaler Objekte über MIME-Typen, bei denen das Ende einer Referenz-URL die notwendige Information liefert. Für die Wiederverwendbarkeit von Daten sind jedoch viele andere und verfeinerte Parameter notwendig. Diese Metadaten-Erweiterungen des DO werden als Datentypen bezeichnet.

Wie bereits erwähnt, betonen die FAIR-Prinzipien sowie der Begriff des digitalen Objekts eine enge Verbindung zwischen Metadaten, Daten und dem persistenten Identifikator als Zeiger. Mit den abstrakten Strukturen der FAIR-DOs wird dies noch deutlicher. Bereits in den frühen RDA-Arbeitsgruppen „PID Information Types“ und „Data Type Register“ wurde die Kopplung noch enger gestaltet, indem bestimmte Arten von Metadaten Teil des Identifier-Records in der Auflösungsdatenbank werden konnten. Solche Metadaten werden als „PID-Information-Type“ bezeichnet und stellen eine wesentliche Kapselung der Komplexität in einer generischen Struktur dar (siehe auch Abbildung 2).

Allerdings muss man diese zusätzlichen Metadatenelemente im PID-Datensatz sorgfältig auswählen, da eine umfangreiche Verwendung zusätzlicher Felder die Auflösungsinfrastruktur verlangsamen könnte. So entwickelte eine zusätzliche RDA-Arbeitsgruppe



2_Kapselung der digitalen Objekt-, Metadaten- und Serviceschnittstellen in ein einziges logisches Element, das durch einen persistenten Identifikator (PID) referenziert wird.

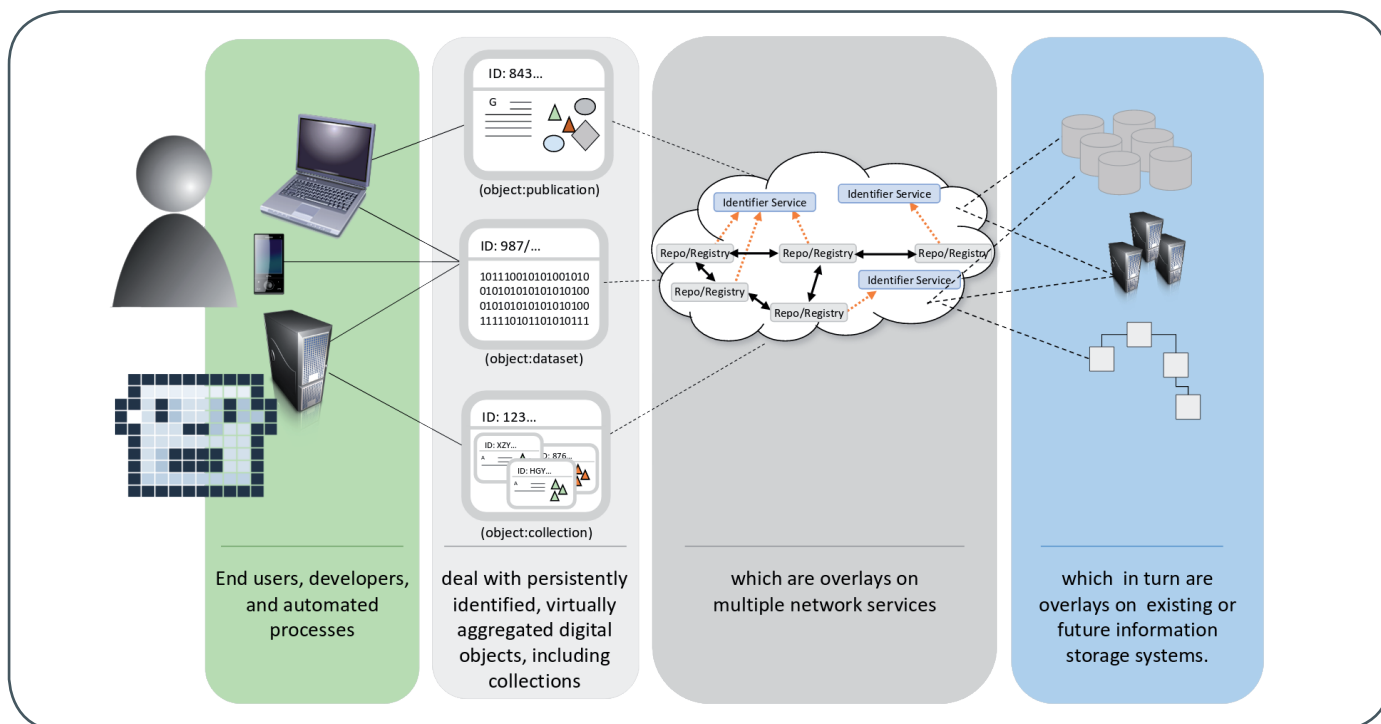
„Kernel Information Types“ Regeln und ein Profil [9] für eine Reihe von einfachen und am häufigsten benötigten Metadatenelementen, die zusammen mit dem PID gespeichert werden sollten. Das Profil kann beispielsweise für die speziellen Bedürfnisse von Wissenschaftsgemeinschaften erweitert werden und die Regeln sind Richtlinien für diese Erweiterungen. Derzeit wird diese leistungsstarke Technologie von den DOI-Anbietern für Papier- und Datenpublikation nicht unterstützt. Für die wissenschaftliche Datenverwaltung ist es nur mit dem allgemeineren Handle-System verfügbar, wie es beispielsweise von ePIC oder für Deutschland von der GWDG bereitgestellt wird.

Data Type Registries

Auf jeden Fall benötigen diese Typen aber eine Art Standardisierung, um ein Mindestmaß an Interoperabilität zu erreichen, ein weiteres wichtiges Ziel der FAIR-Prinzipien. Der klassische Weg entlang der Verfahren internationaler Normungsgremien ist entweder zu spezifisch oder nicht flexibel und schnell genug, um die Bedürfnisse der verschiedenen Forschungs- und Wirtschaftsbereiche in diesem schnell wachsenden Bereich des Datenmanagements zu decken.

Ein vielversprechenderer Ansatz ist es, community-getriebene, zuverlässige Register bereitzustellen, die überprüfte Typdefinitionen in maschinenlesbarer und interpretierbarer Form enthalten, die durch PIDs eindeutig referenziert und disambiguiert definiert werden. Die PIDs der Typdefinitionen können als Schlüssel für die Metadaten als Wert verwendet werden, die für die Digitalen Objekte relevant sind, entweder im PID-Eintrag oder in einem speziellen Metadatensatz.

Solche Register mit Typdefinitionen werden als Data Type Registries (DTRs) bezeichnet und sind auch für die Research Data Alliance (RDA) seit ihren ersten Tagen ein Thema. Zwei Arbeitsgruppen gaben Empfehlungen ab, die den prototypischen Einsatz einer funktionierenden DTR-Implementierung namens CORDRA ermöglichten. CORDRA ist eine Open-Source-Software, die mittlerweile in der Version 2.0 verfügbar ist. Die GWDG betreibt im Auftrag von ePIC zwei Instanzen von CORDRA als DTRs, eine für produktive Datentypen und eine für die Vorbereitung von Datentypen und Tests. Die Typdefinitionen sind frei verfügbar. Um Typen anzulegen oder zu ändern, wird ein Nutzerkonto benötigt. Eine Besonderheit der ePIC-DTRs ist die Möglichkeit, Typen



3_Verschiedene Abstraktionsebenen in der Daten-Domäne, mit der FAIR Digital Objects beim Daten-Interface für die Endverbraucher präsentiert werden (basierend auf „Global Digital Object Cloud“; Larry Lannom, RDA 2016).

hierarchisch zu definieren, so dass auch komplexe Datentypen einfach definiert werden können und beispielsweise Schemata für die Wertedomäne aus der Definition [10] abgeleitet werden können. Als Ausgangspunkt findet sich auf den ePIC-Webseiten [11] eine kurze Übersicht mit Links zu diesen DTRs.

Da DTRs die Disambiguierung und korrekte Zuordnung von Typen für Mensch und Maschine ermöglichen, sind sie integraler Bestandteil des FAIR-DO-Frameworks. Eine einheitliche Sicht auf die Daten, die durch ihre Referenzen dargestellt werden, ergänzt durch Typen, die die notwendigen Informationen für die weitere Verarbeitung liefern, ist in Abbildung 3 dargestellt. Mit der richtigen Wahl der PID-Information-Typen, je nach Bedarf einer wissenschaftlichen Community, ermöglichen solche FAIR-DOs schnelle Entscheidungen über die Relevanz von Daten für bestimmte wissenschaftliche Fragestellungen bereits auf der Referenzebene, erlauben die Identifizierung der Lokation und bereiten die automatisierte Bereitstellung von nicht-lokalen Daten für die Verarbeitung in einem wissenschaftlichen Workflow, z. B. mit Hochleistungsrechnern vor, oder sogar die automatisierte Entscheidung, dass eine nicht-lokale Berechnung weniger Aufwand erfordern würde.

FAIR DIGITAL OBJECTS BEI DER GWGD

Wie bereits erwähnt, bietet die GWGD zuverlässige PID-Dienste für stabile Referenzen wissenschaftlicher Daten für die deutsche Forschungslandschaft. Institutionen, Rechenzentren oder Forschungsgruppen können solche Dienste bei der Service-Hotline der GWGD per E-Mail an support@gwdg.de anfordern. Kunden der GWGD können PID-Dienste auch direkt als Selfservice im Kundenportal nutzen (siehe [12]). Die Typdefinitionen in der ePIC-Datatype-Registry sind öffentlich. Wenn Forschungsgemeinschaften daran interessiert sind, ihre eigenen Typen zu definieren, sollte auch ein Antrag über die Service-Hotline der GWGD gestellt werden.

REFERENZEN

- [1] <https://rd-alliance.org>
- [2] Klein, Van De Sompel, et al.: „Scholarly Context Not Found: One in Five Articles Suffers from Reference Rot (2014)“, DOI: 10.1371/journal.pone.0115253
- [3] <http://www.handle.net/>
- [4] <https://www.force11.org/group/fairgroup/fairprinciples>
- [5] Wilkinson, M.D., et al.: The FAIR Guiding Principles for scientific data management and stewardship, Scientific Data 3 (2016), DOI: 10.1038/sdata.2016.18
- [6] Turning FAIR into reality: Final report and action plan from the European Commission expert group on FAIR data, DOI: 10.2777/1524
- [7] <https://rd-alliance.org/group/gede-group-european-data-experts-rda/wiki/gede-digital-object-topic-group>
- [8] Schultes, E., Wittenburg, P.: FAIR Principles and Digital Objects: Accelerating Convergence on a Data Infrastructure. In: Manolopoulos, Y., Stupnikov, S. (Eds): Data Analytics and Management in Data Intensive Domains. DAMDID/RCDL 2018. Communications in Computer and Information Science, Vol. 1003, Springer, Cham, DOI: 10.1007/978-3-030-23584-0
- [9] <https://www.rd-alliance.org/group/pid-kernel-information-wg/outcomes/recommendation-pid-kernel-information>
- [10] Schwarzmann, U.: Automated schema extraction for PID information types, 2016 IEEE International Conference on Big Data, DOI: 10.1109/BigData.2016.7840957, PID: 21.11101/0000-0002-A987-7
- [11] <http://dtr.pidconsortium.net/>
- [12] Bingert, S.: Neue Funktion im Kundenportal der GWGD: Persistent Identifier, GWGD-Nachrichten 04/2017



Mailinglisten

MAILVERSAND LEICHT GEMACHT!

Ihre Anforderung

Sie möchten per E-Mail zu oder mit einer Gruppe ausgewählter Empfänger kommunizieren, auch außerhalb Ihres Instituts. Sie möchten selbstständig eine Mailingliste verwalten, z. B. Empfänger hinzufügen oder entfernen. Bei Bedarf sollen sich auch einzelne Personen in diese Mailingliste einschreiben dürfen.

Unser Angebot

Wir bieten Ihnen einen Listserver, der zuverlässig dafür sorgt, dass Ihre E-Mails an alle in die Mailingliste eingetragenen Mitglieder versendet werden. Die E-Mails werden automatisch archiviert. Das Archiv kann von allen Mitgliedern der Liste nach Schlagwörtern durchsucht werden. Die Anzahl Ihrer Mailinglisten ist unbegrenzt.

Ihre Vorteile

- > Leistungsfähiges ausfallsicheres System zum Versenden von vielen E-Mails
- > Sie senden Ihre E-Mail lediglich an eine Mailinglisten-Adresse, die Verteilung an die Mitglieder der Mailingliste übernimmt der Listserver.

- > Listenmitglieder können an diese E-Mail-Adresse antworten. Eine Moderationsfunktionalität ist verfügbar, mit der Sie die Verteilung einer E-Mail genehmigen können.
- > Voller administrativer Zugriff auf die Einstellungen der Mailingliste und der Listenmitglieder
- > Obsolete E-Mail-Adressen werden vom System erkannt und automatisch entfernt.
- > Wenn Ihre E-Mail-Domäne bei uns gehostet wird, können Sie auch die Adresse der Mailingliste über diese Domäne einrichten lassen.

Interessiert?

Für die Einrichtung einer Mailingliste gibt es zwei Möglichkeiten: Zum einen als registrierter Benutzer der GWDG im Selfservice über das Kundenportal der GWDG und zum anderen, indem Sie bitte eine entsprechende E-Mail an support@gwdg.de senden, die die Wunsch-E-Mail-Adresse der Liste sowie die E-Mail-Adresse der Person, die die Liste bei Ihnen administrieren soll, enthalten sollte. Die administrativen Aufgaben sind leicht zu erlernen.

E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 1: Beantragung und Sicherung von Zertifikaten

Text und Kontakt:

Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

In den GWDG-Nachrichten 9-12/2013 wurde eine vierteilige Artikelserie „E-Mail-Verschlüsselung mit X.509-Zertifikaten“ veröffentlicht, die dann zusammengefasst auch als Special 1/2014 erschienen ist. Aufgrund von zwei bedeutenden diesjährigen Ereignissen in der DFN-PKI ist nun eine komplette Überarbeitung der Artikelserie angebracht. Das erste Ereignis war im Juli der Ablauf des Wurzelzertifikats der DFN-PKI der Generation 1 und das zweite die Veröffentlichung der Firefox-Version 69 Anfang September, die durch den Wegfall des KEYGEN-Tag einen komplett überarbeiteten Beantragungsweg für Nutzerzertifikate von Seiten der DFN-PKI erforderlich machte. In loser Folge werden die aktualisierten und an die neuen Gegebenheiten angepassten vier Artikel der Serie aus dem Jahr 2013, beginnend mit dieser Ausgabe, erscheinen.

BEGRIFFSERKLÄRUNGEN

Die zwei Hauptbegriffe, die im Zusammenhang mit dem Umgang von E-Mail-Verschlüsselung fallen, sind **X.509-Zertifikate** und **Public Key Infrastructure**, im Weiteren kurz **PKI** genannt.

Die PKI ist ein hierarchisch organisierter Aufbau von Zertifikatsautoritäten, engl. **Certification Authority** (im Weiteren kurz **CA** genannt), beginnend mit einer Wurzel, über Zwischenstationen hin zur ausstellenden Autorität für Zertifikate. Diese Kette der Autoritäten bildet die Grundlage einer PKI.

Die Zertifikate wiederum sind eine digitale Repräsentation von Benutzern, Diensten, Netzwerkgeräten oder Computern, die durch eine CA ausgestellt wurden. Diese Zertifikate sind zusammen mit jeweils einem privaten Schlüssel (engl. private key) und einem öffentlichen Schlüssel (engl. public key) miteinander verbunden.

Technisch betrachtet ist das Zertifikat eine digital signierte Ansammlung von Informationen, u. a. Informationen über den Benutzer, den Dienst, das Netzwerkgerät oder den Computer, die ausstellende CA, die verwendeten Signier-/Verschlüsselungsverfahren, Informationen über die Abruf-URLs von Sperrlisten für gesperrte Zertifikate usw.

X.509 wiederum ist ein ITU-T-Standard (Internationale Fernmeldeunion) für eine PKI zum Er-/Ausstellen digitaler Zertifikate.

ZERTIFIKAT BEANTRAGEN

Um nun ein Zertifikat zu beantragen, ist es als erstes wichtig zu wissen, welche ausstellende Registrierungsautorität, engl. **Registration Authority** (im Weiteren kurz **RA** genannt), für

Antragsteller zuständig ist. Unter dem URL https://info.gwdg.de/dokuwiki/doku.php?id=de:services:it_security:пки:start finden Sie die jeweiligen Einstiegspunkte für die RAs der Max-Planck-Gesellschaft, der Universität Göttingen und der GWDG.

Bedingt durch die technische Änderung im Webbrowser Firefox ab der Version 69 gibt es seit diesem Zeitpunkt keinen gängigen Webbrowser mehr, der noch über das KEYGEN-Tag verfügt. Das KEYGEN-Tag war bisher der technisch „traditionelle“ Weg der Schlüsselerzeugung im Browser für Nutzerzertifikate in der MPG-CA, Uni-Göttingen-CA und GWDG-CA.

E-Mail Encryption Using X.509 Certificates – Part 1: Application and Securing of Certificates

In the GWDG News 9-12/2013 a four-part article series „E-Mail Encryption Using X.509 Certificates“ was published, which was then also summarized as Special 1/2014. Due to two significant events in the DFN-PKI this year, a complete revision of the article series is now necessary. The first event was the expiration of the root certificate of the DFN-PKI Generation 1 in July and the second was the release of Firefox Version 69 in the beginning of September, which required a completely revised application procedure for user certificates from DFN-PKI due to the omission of the KEYGEN tag. In loose succession, the updated and adapted to the new circumstances four articles of the series from the year 2013, starting with this issue, will appear.

Seit dem 2. September 2019 steht in der DFN-PKI, also auch für die soeben genannten CAs, ein neuer Beantragungsweg für Nutzerzertifikate für die bekannten Webbrowser Firefox, Chrome, Opera und Safari sowie deren mobile Gegenparts auf Android- und iOS-Geräten zur Verfügung.

Die Anleitung für den neuen Beantragungsweg finden Sie hier: https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start#neuer_weg

Der neue Beantragungsweg wurde bereits in einem Artikel in den GWDG-Nachrichten 8-9/2019 ausführlich beschrieben und soll daher hier nicht weiter behandelt werden, sondern im Weiteren nur der „Sonderfall“ des Microsoft Internet Explorer.

Aufgrund seines Alters wird es für diesen Browser aus Kompatibilitätsgründen weiterhin noch den bisherigen Beantragungsweg geben, der nachfolgend näher erläutert werden soll.

Die Anleitung für den bisherigen Beantragungsweg finden Sie hier: https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start#bisheriger_weg

Für weiterführende Schritte und eine detaillierte Anweisung zur Installation des Zertifikats in verschiedenen E-Mail-Clients lesen Sie bitte die Informationen im „GWDG-Nachrichten Special 1/2014“ ab Seite 7, das Sie unter folgendem URL abrufen können: https://www.gwdg.de/documents/20182/27257/GN_Special_01-2014_www.pdf. Bis zur geplanten Veröffentlichung des aktualisierten Teils 2 der Artikelserie können diese Informationen größtenteils noch genutzt werden.

BEANTRAGUNG VON ZERTIFIKATEN MIT DEM INTERNET EXPLORER

Nach dem Klick auf „Zertifikatantrag im Webformular für Benutzer ...“ bei der ausgewählten jeweiligen Einrichtung für die MPG-RAs https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:mpgras
 Universität-Göttingen-RAs https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:uniras
 GWDG-RAs https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:gwdgras

[it_security:pki:gwdgras](https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:gwdgras)

erscheint bei Erkennung des Microsoft Internet Explorer 11 (getestet unter Windows 10) ein entsprechendes Formular (siehe Abbildung 1).

Bei diesem Webformular ist es wichtig, dass die mit * gekennzeichneten Felder ausgefüllt werden müssen. Eine Abteilung kann wahlweise angegeben werden. Nun muss noch eine PIN eingegeben werden. Diese wird verwendet, wenn der Anwender selbst sein Zertifikat sperren möchte. Auch hier wird dann die PIN abgefragt, bevor das Zertifikat gesperrt wird. Bitte diese Angabe gut merken! Da in einer PKI der öffentliche Schlüssel ohne Bedenken weitergegeben werden kann, kann auch das Häkchen bei „Veröffentlichung des Zertifikats“ bedenkenlos gesetzt werden. Diese Möglichkeit kann sich sogar als vorteilhaft erweisen, wie in einem späteren Artikel noch beschrieben wird. Die „Informationen für Zertifikatinhaber“ müssen auf alle Fälle durch Setzen des Häkchens anerkannt werden. Jetzt auf „Weiter“ klicken.

In der dann erscheinenden Übersichtsseite über die eingegebenen Angaben können diese noch einmal auf ihre Richtigkeit hin geprüft werden und mit einem Klick auf „Ändern“ korrigiert werden. Andernfalls nun auf „Bestätigen“ klicken.

Wurde auf „Bestätigen“ geklickt, wird im Microsoft Internet Explorer 11, im Weiteren kurz IE genannt, der private Schlüssel generiert und im Windows-Zertifikatspeicher für den angemeldeten Benutzer abgelegt. Weiterhin wird der Zertifikatantrag (engl. certificate signing request; im Weiteren kurz CSR) in der ausgewählten RA hochgeladen.

Es wird eine Bestätigungsseite angezeigt. Mit einem Klick auf „Zertifikatantrag anzeigen“ wird der generierte Antrag im PDF-Format entweder gleich angezeigt oder heruntergeladen und kann dann mit einem PDF-Anzeigeprogramm angezeigt und ausgedruckt werden. Welche Variante angewendet wird, hängt vom genutzten Betriebssystem und/oder installierten PDF-Anzeigeprogramm ab. Den ausgedruckten Antrag muss der Zertifikatnehmer eigenhändig unterschreiben.

Mit diesem Formular muss er dann zum RA-Operator der ausgewählten RA gehen. Dort wird die persönliche Identifizierung

Nutzerzertifikat beantragen

Bitte geben Sie Ihre Daten ein. Felder mit einem Stern (*) müssen ausgefüllt werden.

Zertifikatdaten

E-Mail *

Name *

Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate stellen Sie das Kürzel "GRP:" voran. Verwenden Sie keine Umlaute.

Abteilung

Wenn Sie hier eine Abteilung angeben, wird diese in den Zertifikatnamen aufgenommen.

Weitere Angaben

Diese Angaben werden nicht in das Zertifikat übernommen.

PIN (Mindestens 8 beliebige Zeichen) *

Nochmalige Eingabe der PIN zur Bestätigung *

Die PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen oder um dieses einzulesen, wenn Sie einer Veröffentlichung nicht zustimmen. Bitte notieren Sie sich die PIN.

Ich verpflichte mich, die in den [Informationen für Zertifikatinhaber](#) aufgeführten Regelungen einzuhalten. *

Ich stimme der [Veröffentlichung des Zertifikats](#) mit meinem darin enthaltenen Namen und der E-Mail-Adresse zu.

Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft durch eine E-Mail an pki@dfn.de widerrufen.

Abb. 1



Abb. 2

vor- genommen, d. h. mittels des Personalausweises des Zertifikatnehmers überprüft und vergleicht der RA-Operator (im neuen Sprachgebrauch DFN-Teilnehmerservice-Mitarbeiter, kurz TS-Mitarbeiter) die Angaben auf dem Zertifikatantrag mit dem Ausweis. Wenn alles in Ordnung ist, wird der RA-Operator das Zertifikat dann zeitnah ausstellen. Per Bestätigungs-E-Mail an den Zertifikatnehmer wird dieser über die Ausstellung des Zertifikats unterrichtet. Korrekterweise muss hier von der Signierung des öffentlichen Schlüssels, des hochgeladenen CSR, durch die entsprechende CA gesprochen werden.

In der Bestätigungs-E-Mail kopiert der Zertifikatnehmer den zweiten URL – das ist wichtig(!) – aus der E-Mail und fügt diesen in die Adresszeile des IE ein. Ist auf dem System des Zertifikatnehmers der IE der Standardbrowser, genügt ein Klick auf diesen Link.

Nun werden im IE der private und signierte öffentliche Schlüssel zusammengeführt und beide ergeben zusammen das Zertifikat (siehe Abbildung 2). Ist dieser Vorgang durch Klick auf die Schaltfläche „Zertifikat importieren“ erfolgreich abgeschlossen, wird ein entsprechender Hinweis präsentiert (siehe Abbildung 3). Diesen Dialog mit einem Klick auf die Schaltfläche „Ja“ bestätigen. Eine sehr einfache Erfolgsmeldung wird im Anschluss präsentiert (siehe Abbildung 4).

Mit dieser Aktion ist das Zertifikat im Windows-Zertifikatspeicher des angemeldeten Benutzers erfolgreich erstellt worden und kann z. B. nun in Outlook als Signier- oder Verschlüsselungszertifikat verwendet werden. Darauf wird in einem späteren Teil dieser Artikelserie eingegangen (siehe dazu auch am Schluss dieses Artikels das Kapitel „Ausblick“).

Anmerkung: Es kann beim IE vorkommen, dass, abhängig von der eingesetzten Windows-Version, ein wichtiger betriebssystemseitiger Bestandteil noch nicht installiert ist, so dass es zu Fehlermeldungen kommen kann und die Beantragung scheitert. Hier müssen dann die Vor-Ort-Administratoren erst noch das fehlende Programmteil installieren, bevor die Beantragung gelingt. Die Erzeugung eines CSR ist auch mittels des Kommandozeilenprogramms

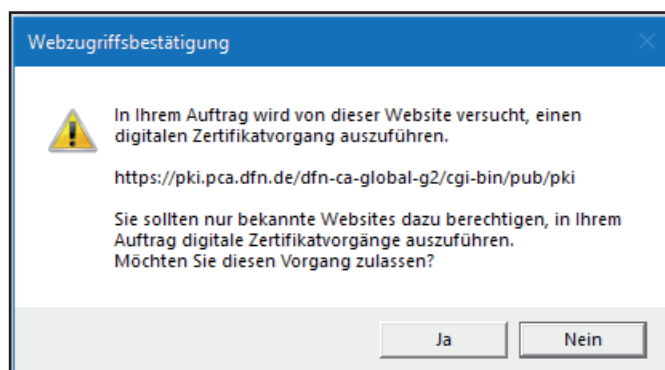


Abb. 3

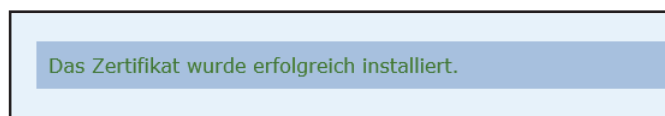


Abb. 4

OpenSSL möglich. Allerdings werden hier dann schon erweiterte Kenntnisse zu Zertifikaten und der Umgang mit der Kommandozeile vorausgesetzt – ein weiterer Grund, Firefox oder Chrome zu verwenden, die sich im Laufe der Jahre als am praktikabelsten erwiesen haben.

SICHERUNG VON ZERTIFIKATEN AUS DEM INTERNET EXPLORER

Eine der wichtigsten Handlungen ist es, eine Sicherheitskopie des gerade erstellten Zertifikats anzufertigen. Diese Aktion ist mit dem IE möglich und wird im Folgenden beschrieben.

Mit einem Klick auf das Zahnrad, das sich oben rechts in der Ecke des IE befindet, wird ein Menü aufgerufen. In diesem Menü bitte den Menüpunkt „Internetoptionen“ anklicken (siehe Abbildung 5).

In dem sich öffnenden Dialogfenster „Internetoptionen“ auf den Registerreiter „Inhalte“ klicken (siehe Abbildung 6).



Abb. 5

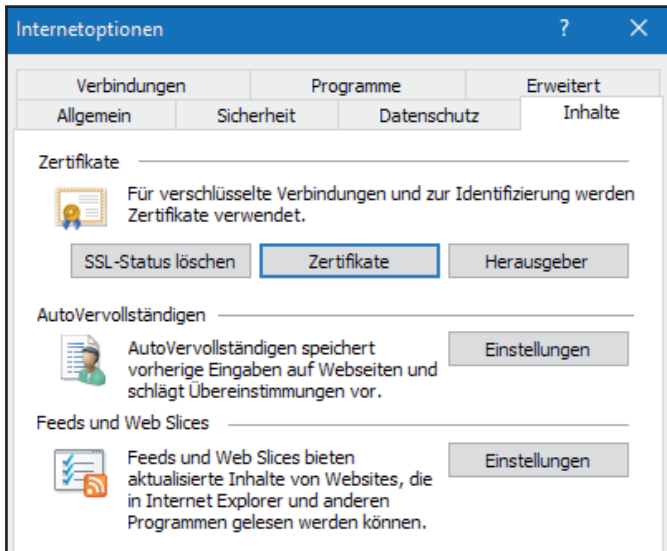


Abb. 6

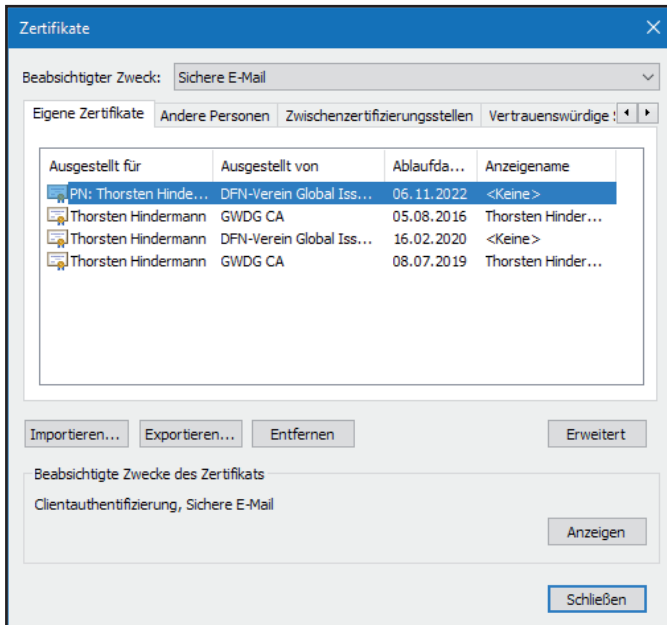


Abb. 7

Jetzt auf die Schaltfläche „Zertifikate“ klicken, woraufhin sich das Dialogfenster „Zertifikate“ öffnet. Der Registerreiter „Eigene Zertifikate“ ist schon als erster Reiter vorausgewählt. In der ausklappbaren Liste „Beabsichtigter Zweck:“ die Auswahl „Sichere E-Mail“ auswählen und jetzt das Zertifikat auswählen, das exportiert werden soll (siehe Abbildung 7).

Mit einem Klick auf die Schaltfläche „Exportieren...“ wird der „Zertifikatexport-Assistent“ gestartet (siehe Abbildung 8).

Mit einem Klick auf die Schaltfläche „Weiter“ startet der Exportvorgang. Im nächsten Schritt „Ja, privaten Schlüssel exportieren“ anklicken und auf die Schaltfläche „Weiter“ klicken (siehe Abbildung 9).

Anschließend die drei Möglichkeiten anklicken, wie in Abbildung 10 zu sehen, und auf „Weiter“ klicken.

Im nächsten Schritt die Möglichkeit „Kennwort“ durch Klick anhaken und aktivieren. Es wird nach einem Kennwort gefragt, mit dem die Container-Datei im PKCS#12-Format verschlüsselt wird. Der Grund dafür ist, dass diese Datei sowohl den privaten als auch den öffentlichen Schlüssel enthält, also das gesamte Zertifikat. Gerade wegen des privaten Schlüssels ist es wichtig, dass diese

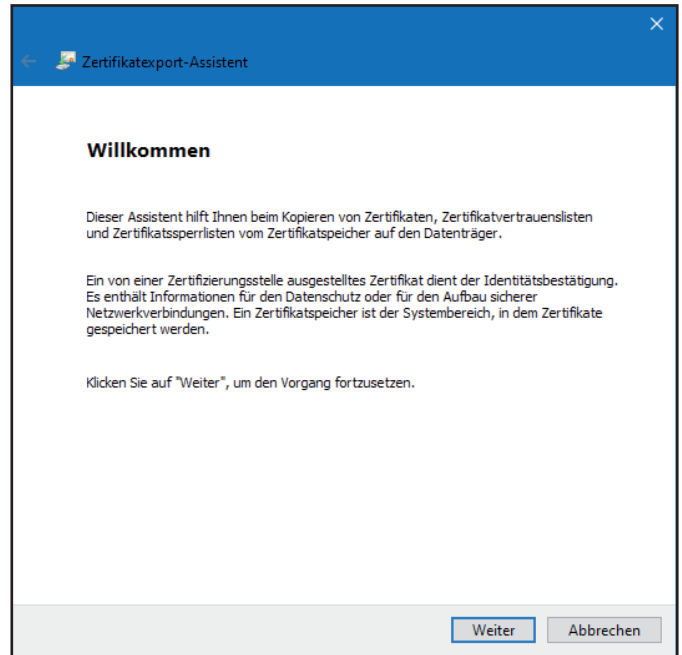


Abb. 8

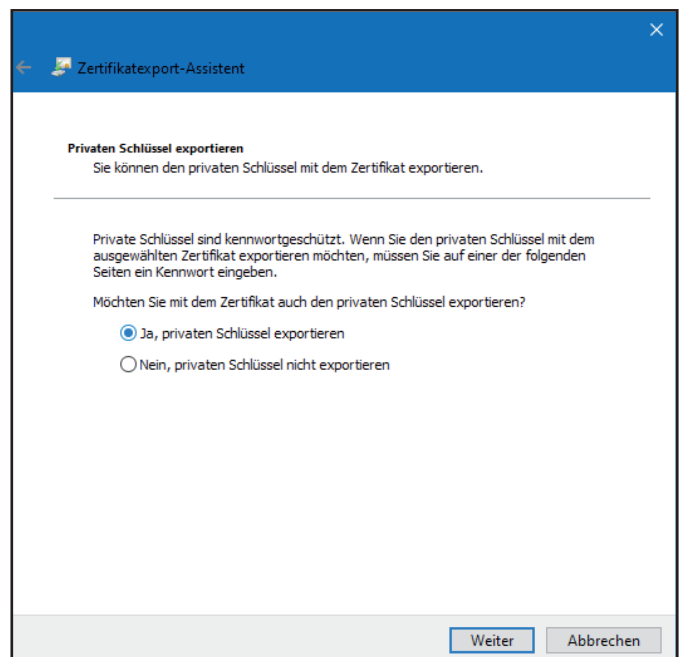


Abb. 9

Datei entsprechend gesichert ist (siehe Abbildung 11). Weiter geht es mit dem Klick auf die Schaltfläche „Weiter“.

Im entsprechenden Speicherdialog muss ein Datenträger/Verzeichnis angegeben werden, wo die Datei mit der Dateierdung .PFX gespeichert werden soll (siehe Abbildung 12). Es empfiehlt sich ein externer Datenträger. Praktischer Hintergrund: Wenn der Rechner, auf dem das Zertifikat einmal beantragt wurde, ausgetauscht wird, die Festplatte formatiert wird oder defekt ist, ist das Zertifikat unwiderruflich verloren. Dann ist ein Entschlüsseln von E-Mails, die mit diesem Zertifikat verschlüsselt worden sind, für immer unmöglich!

Durch Klick auf die Schaltfläche „Speichern“ werden der Pfad und der Dateiname in den Dialog übernommen (siehe Abbildung 13).

Mit dem Klick auf die Schaltfläche „Weiter“ wird eine Zusammenfassung angezeigt (siehe Abbildung 14).

Wird abschließend auf die Schaltfläche „Fertig stellen“

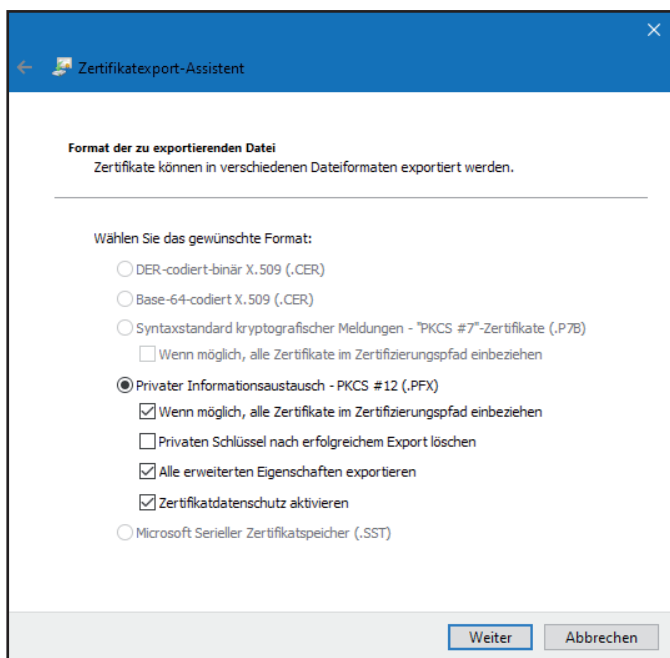


Abb. 10

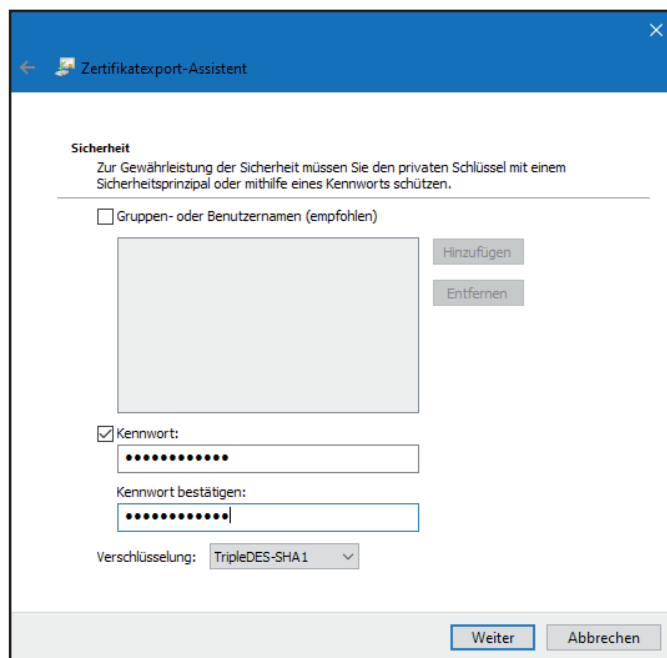


Abb. 11

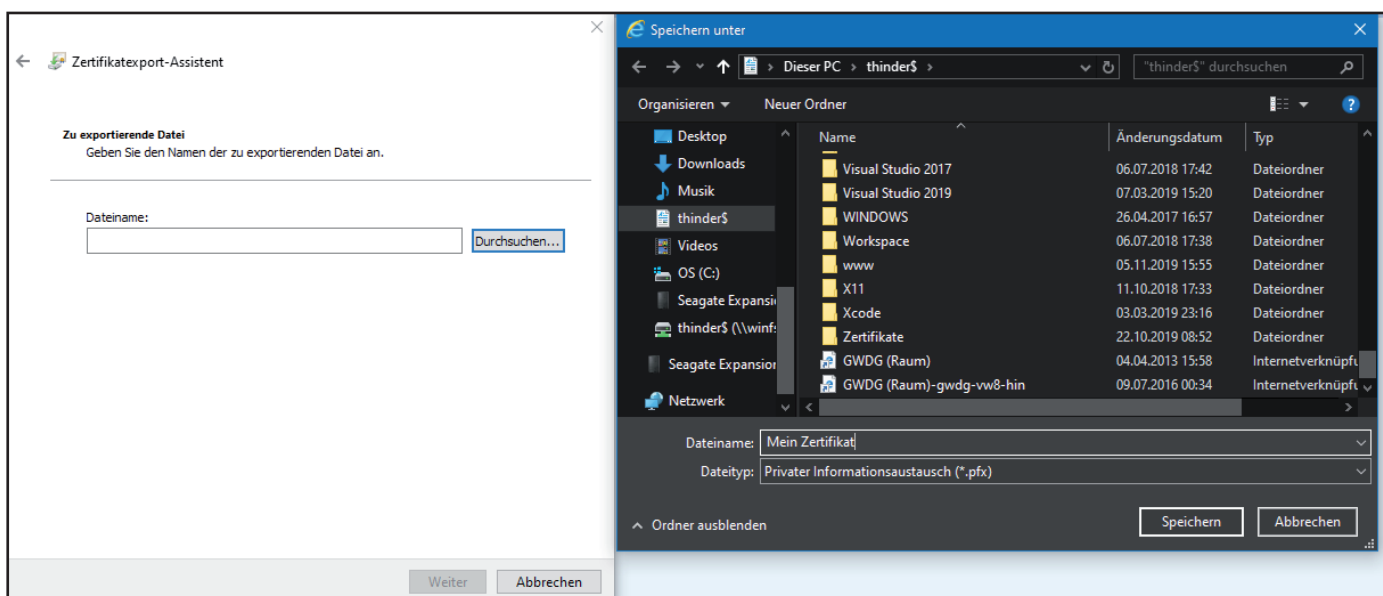


Abb. 12

geklickt, wird der Vorgang des Sicherns des Zertifikats mit dem Zertifikatexport-Assistent mit einem letzten Dialog abgeschlossen, der mit dem abschließenden Klick auf die Schaltfläche „OK“ beendet wird (siehe Abbildung 15).

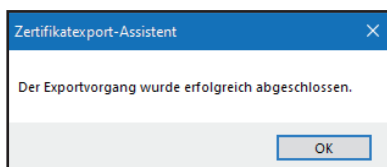


Abb. 15

Anschließend noch die beiden offenen Dialogfenster nacheinander durch Klick auf die Schaltflächen „Schließen“ und „OK“ schließen (siehe Abbildung 16).

Anmerkung: Die Sicherung hat auch noch einen anderen, praktischen Aspekt, der nicht unterschätzt werden sollte. Im Laufe der Tätigkeit sammeln sich mit der Zeit einige Zertifikate an. Wenn nun mit einem oder mehreren Zertifikaten E-Mails verschlüsselt worden sind, können diese alten E-Mails nur mit dem dann aufbewahrten Zertifikat wieder entschlüsselt werden, selbst wenn

zu diesem Zeitpunkt das Zertifikat sein Ablaufdatum überschritten haben sollte. Deshalb ist die Sicherung und Aufbewahrung ein wichtiger Schritt. D. h. bei einem Rechnerwechsel müssen dann am besten alle alten und das aktuelle Zertifikat in die entsprechenden Zertifikatspeicher importiert werden. Dieser Vorgang wird im Teil 2 in einer der nächsten GWDG-Nachrichten näher beschrieben.

AUSBLICK

Nachdem in diesem Artikel die Beantragung und Sicherung von Zertifikaten zur E-Mail-Verschlüsselung erläutert wurden, sollen in den nächsten Teilen folgende Themen detailliert behandelt werden:

- Installation und Verteilung von Zertifikaten
- Verschlüsselung bei Outlook-Mailanwendungen
- Verschlüsselung bei Thunderbird, Notes 9, mutt und Apple-Mailanwendungen

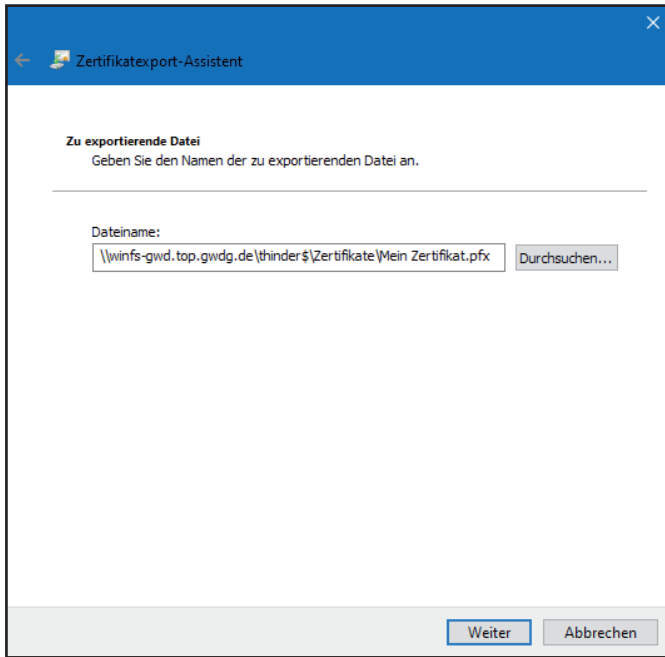


Abb. 13

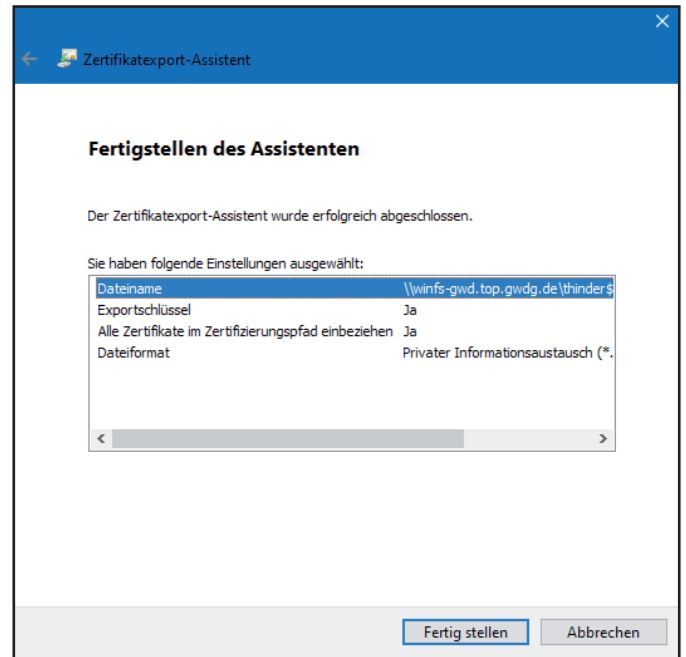


Abb. 14

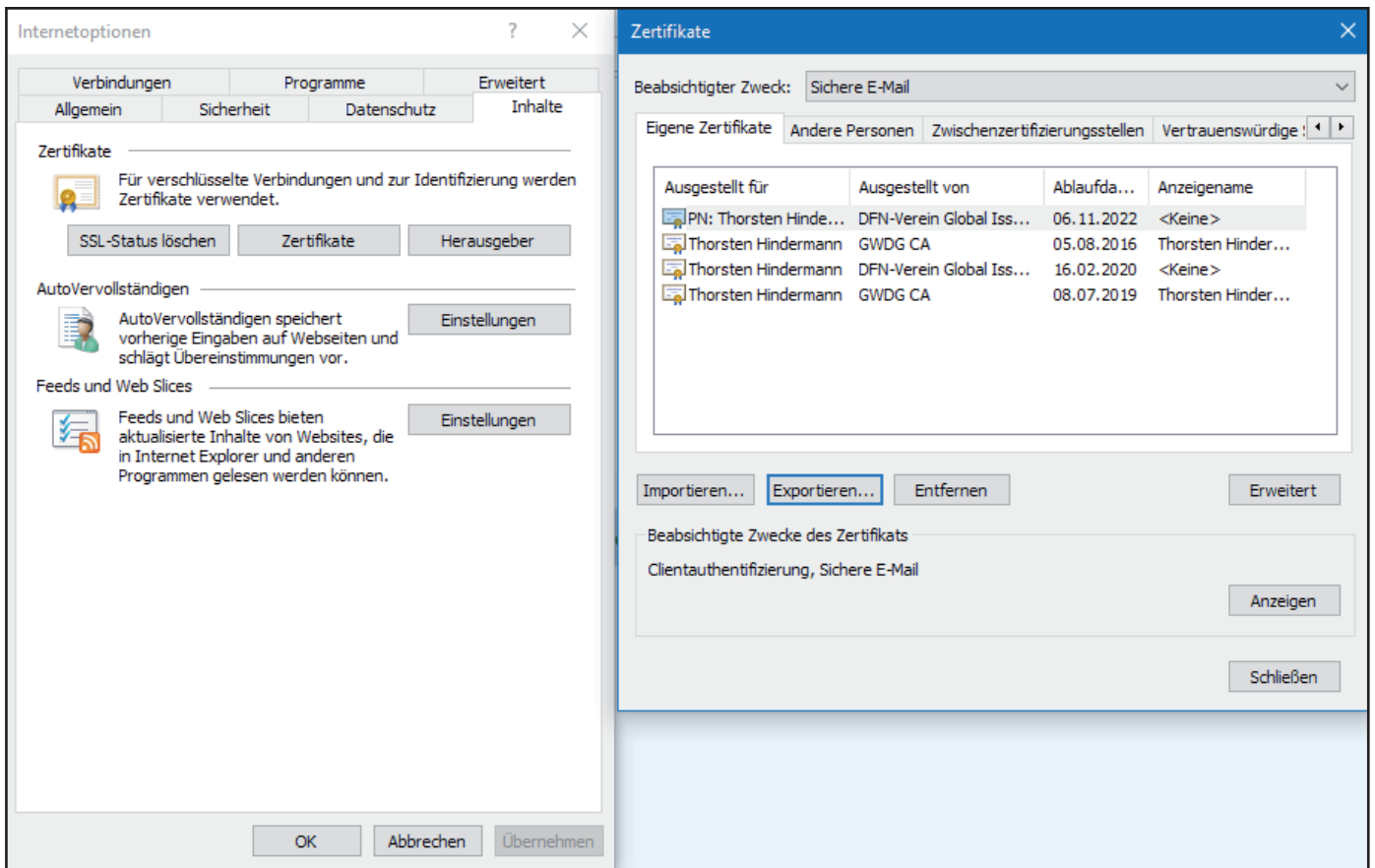
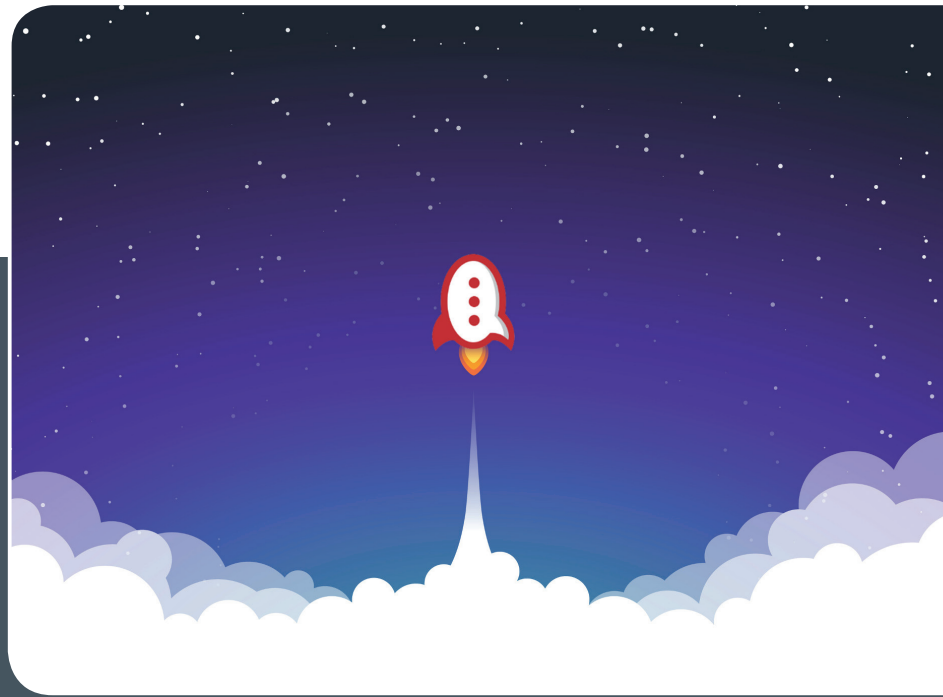


Abb. 16



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.

Tipps & Tricks

Cloud-Verschlüsselung mit Cryptomator unter iOS

In den GWDG-Nachrichten 4/2017 hatten wir beschrieben, wie man von einem Windows-PC aus Daten vor dem Hochladen auf <https://owncloud.gwdg.de> verschlüsseln kann. Hier soll jetzt beschrieben werden, wie man von einem iOS-Gerät (iPhone oder iPad) aus darauf zugreifen kann.

Die Cryptomator-App können Sie aus Apples Appstore beziehen. Sie kostet zurzeit 9,99 €. Beim ersten Start der App werden Sie gefragt, ob Sie einen neuen Tresor anlegen oder einen vorhandenen hinzufügen möchten (siehe Abbildung 1).

Nutzung eines vorhandenen Tresors

Als Beispiel wollen wir den Tresor öffnen, der im damaligen Artikel in den GWDG-Nachrichten 4/2017 angelegt worden ist. Tippen Sie dazu auf „Vorhandenen Tresor hinzufügen“. Daraufhin werden Sie gebeten, einen Cloud-Dienst auszuwählen. Für unseren ownCloud-Server wählen Sie hier „WebDAV“ aus (siehe Abbildung 2).

Anschließend werden Sie nach den Zugangsdaten gefragt. Als erstes geben Sie <https://owncloud.gwdg.de/remote.php/webdav/> ein, danach Ihre GWDG-E-Mail-Adresse sowie Ihr GWDG-Passwort (siehe Abbildung 3). Als letztes tippen Sie auf „Fertig“. Das Anmelden kann einen kleinen Moment dauern. Danach sollten Sie Ihre ownCloud-Daten sehen. Navigieren Sie jetzt – bezogen auf unser Beispiel – bitte zum Verzeichnis *crypt*, in dem Ihr

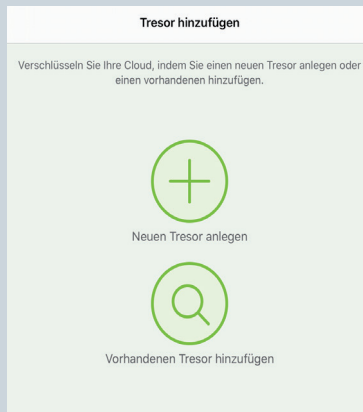


Abb. 1

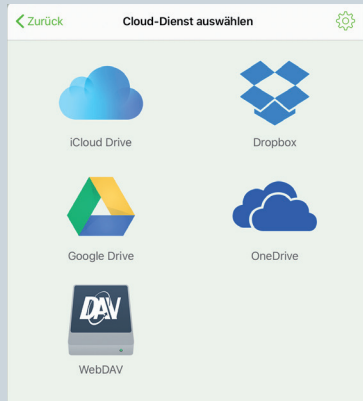


Abb. 2

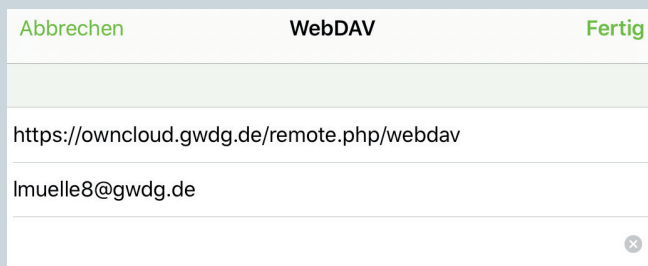


Abb. 3

Tresor *encrypted_data* liegt, und wählen Sie dort *masterkey.cryptomator* aus (siehe Abbildung 4). Jetzt wird der Tresor in der Liste der verfügbaren Tresore angezeigt (siehe Abbildung 5).



Abb. 4

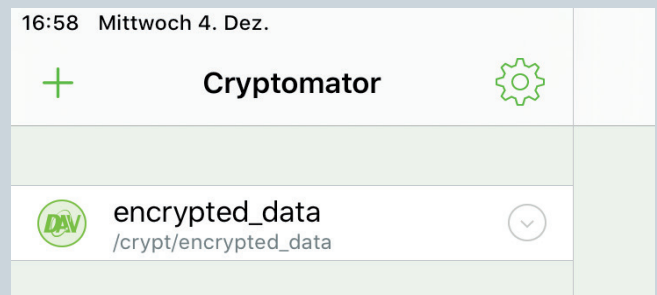


Abb. 5

Um diesen Tresor zu öffnen, tippen Sie auf diesen Tresor. Daraufhin werden Sie aufgefordert, das Tresor-Passwort einzugeben, welches Sie beim Anlegen dieses Tresors vergeben haben (siehe auch die GWDG-Nachrichten 4/2017). Nach dem Öffnen sehen Sie links eine Liste der Verzeichnisse/Dateien, die sich in dem Tresor befinden (in unserem Beispiel ist das *Hamlet.txt*; siehe Abbildung 6).

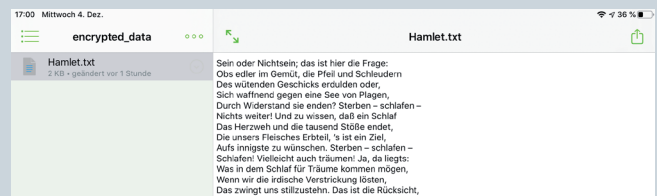


Abb. 6

Tippen Sie auf diese Datei und sie wird geöffnet. Sollte Cryptomator mit dieser Datei nichts anfangen können, so können Sie diese an eine andere App weiterleiten.

Wenn Sie ein iOS-Gerät mit Fingerabdrucksensor besitzen, können Sie diesen auch zum Entsperrern Ihres Tresors verwenden. Das können Sie über die Cryptomator-Einstellungen (auf das „Zahnrad“-Icon tippen) konfigurieren. Dazu tippen Sie auf „Touch ID“ und anschließend auf „Touch ID aktivieren“ (siehe Abbildung 7). Danach können Sie für jeden Tresor festlegen, ob Sie diesen per Touch ID entsperren möchten. In diesem Fall



Abb. 7

müssen Sie noch einmal Ihr Tresor-Passwort eingeben.

Import einer Datei

Im nächsten Anwendungsfall gehen wir umgekehrt vor: Angenommen, Sie haben auf Ihrem iPhone bzw. iPad eine Datei *Secret_Doc-3.pdf*, die vertrauliche Daten enthält. Um sie in Cryptomator zu importieren, tippen Sie oben rechts auf das Senden-an-Symbol (das blaue Rechteck mit dem Pfeil nach oben) und tippen danach auf das Symbol mit dem Untertitel „In Cryptomator speichern“ (siehe Abbildung 8).

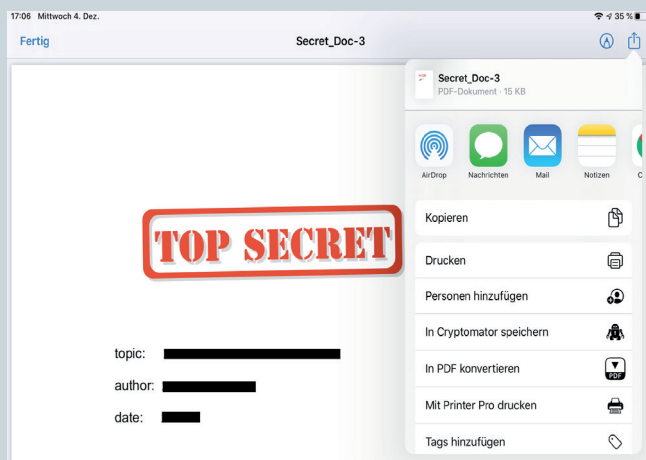


Abb. 8

Jetzt werden Sie an die Cryptomator-App weitergeleitet und gebeten, einen Speicherort für Ihr Dokument auszuwählen. In unserem Beispiel ist das *encrypted_data* (siehe Abbildung 9).

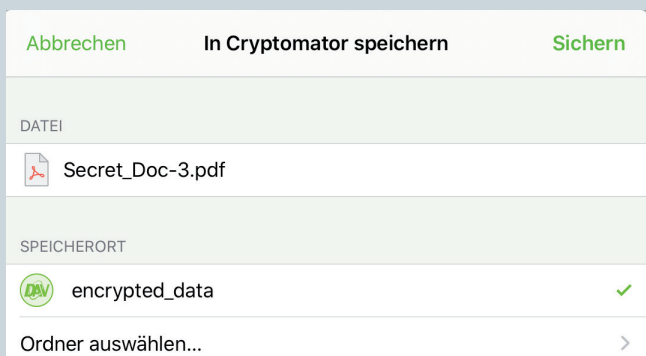


Abb. 9

Tippen Sie jetzt oben rechts auf „Sichern“. Im nächsten Schritt müssen Sie den ausgewählten Tresor entsperren. Das kann entweder durch Eingeben des Tresor-Passwortes oder mit Hilfe des Fingerabdrucksensors („Touch ID“) erfolgen (siehe Abbildung 10).



Abb. 10

Jetzt sollte Ihre Datei im Tresor *encrypted_data* auftauchen und sofort zu <https://owncloud.gwdg.de> hochgeladen werden. Wenn auf Ihrem PC der ownCloud-Client und Cryptomator laufen, dann können Sie sofort auf diese Datei zugreifen.

Anlage eines neuen Tresors

Um einen neuen Tresor in Cryptomator auf Ihrem iOS-Gerät anzulegen, gehen Sie wie folgt vor: Starten Sie Cryptomator und tippen Sie oben links auf das Symbol „+“ (siehe Abbildung 11), um den „Tresor hinzufügen“-Dialog zu öffnen. Dort wählen Sie „Neuen Tresor anlegen“ aus.

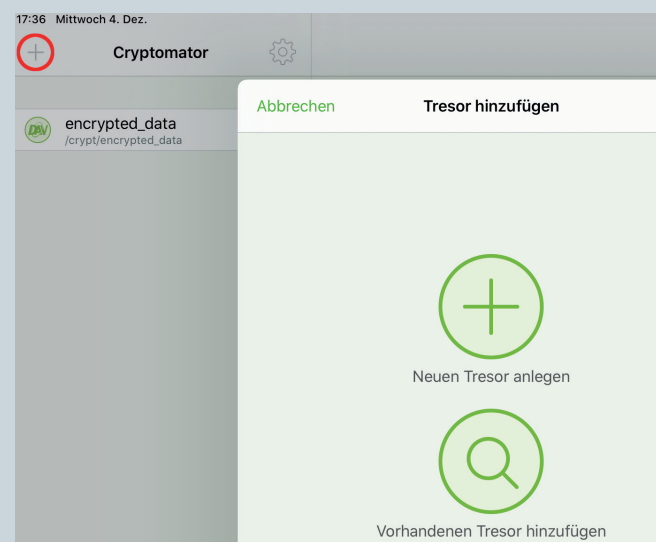


Abb. 11

Nun werden Sie gebeten, einen Cloud-Dienst auszuwählen, zu dem der neue Tresor hochgeladen werden soll. Wählen Sie auch hier wieder „WebDAV“ aus (siehe Abbildung 12).

Wenn Sie, wie in Abbildung 3, schon unseren ownCloud-Server eingerichtet haben, brauchen Sie diesen nur aus der

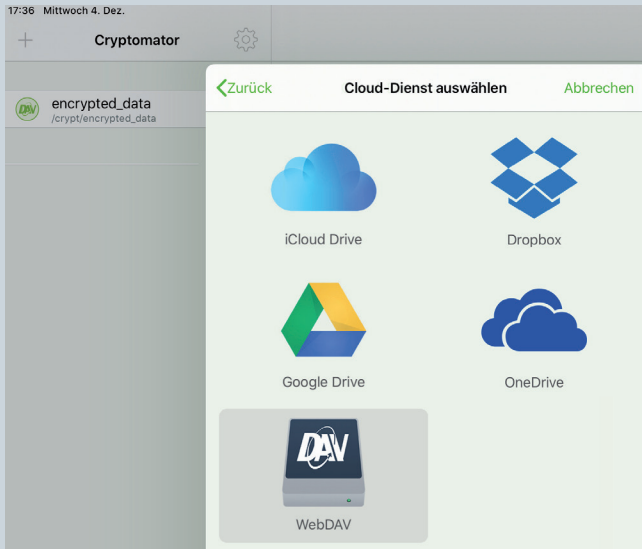


Abb. 12

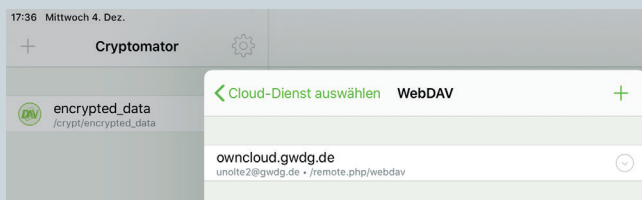


Abb. 13

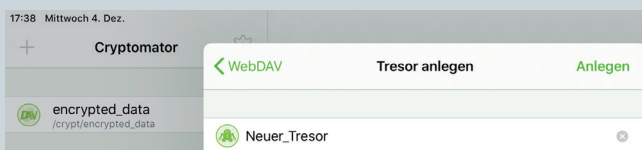


Abb. 14

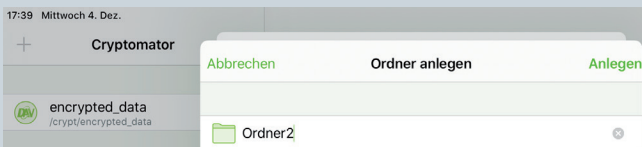


Abb. 15

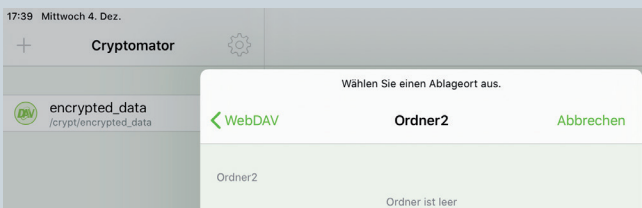


Abb. 16

Liste der WebDAV-Server auszuwählen (siehe Abbildung 13).

Im nächsten Schritt werden Sie gebeten, einen Namen für den neuen Tresor einzugeben. In unserem Beispiel nennen wir ihn *Neuer_Tresor* (siehe Abbildung 14). Danach müssen wir noch einen Ordner auf unserem ownCloud-Server anlegen, in dem der Tresor abgelegt werden soll. Wir nennen ihn *Ordner2*

(siehe Abbildung 15), wählen ihn aus (siehe Abbildung 16) und vergeben ein Passwort (siehe Abbildung 17).



Abb. 17

Dieses Passwort dürfen Sie nicht vergessen, weil Sie sonst keine Möglichkeit mehr haben, an Ihre Daten heranzukommen. Das Anlegen des neuen Tresors kann einen kurzen Moment dauern (siehe Abbildung 18).

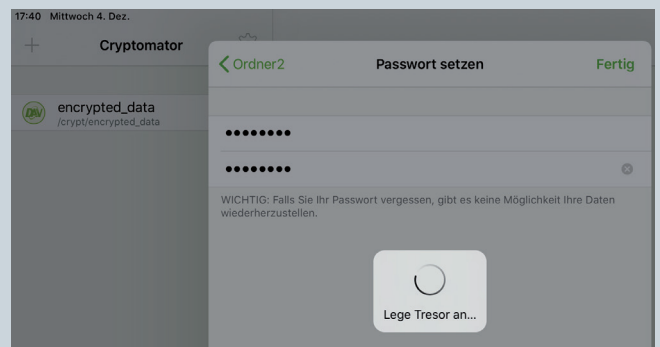


Abb. 18

Danach taucht unser *Neuer_Tresor* in der Liste der vorhandenen Tresore auf (linke Spalte in der App).

Wenn Sie möchten, können Sie diesen Tresor auch über die „Touch ID“ entsperren. Tippen Sie dazu auf das „Zahnrad“-Icon, um in die Einstellungen zu gelangen (siehe Abbildung 19).

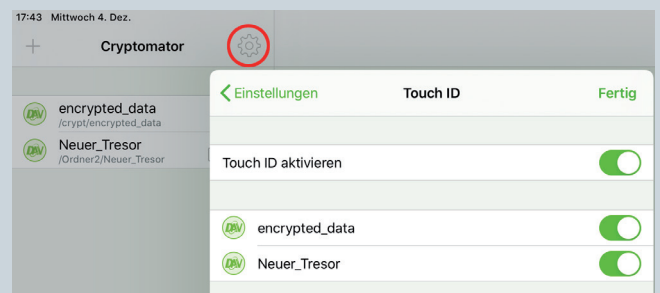


Abb. 19

Schieben Sie anschließend den Schalter für *Neuer_Tresor* nach rechts und tippen dann auf „Fertig“. Jetzt können Sie Dateien in diesem Tresor ablegen. Wenn Sie *Neuer_Tresor* auch auf Ihren PC einbinden, können Sie auch von dort auf diese Dateien zugreifen.

Nolte



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.

Kurz & knapp

Neue Hard- und Software im Benutzerraum

Um unseren Nutzerinnen und Nutzern aktuellere Hard- und Software anbieten zu können, haben wir in den vergangenen Monaten unseren Benutzerraum am Faßberg mit neuen PCs und Bildschirmen ausgestattet.

Hardware

Für die üblichen alltäglichen Office-Anwendungen wurden sechs Desktop-PCs eingerichtet – zwei in englischer (inkl. US-Tastatur) und vier in deutscher Sprache. Diese sind jeweils mit einem 27"-QHD-Monitor (2.560 x 1.440) ausgestattet und sollten mit ihrer Hardware alle gängigen Anwendungen schnell und zuverlässig ausführen können. Dazu gehören ein Prozessor vom Typ Intel Core i5-8600T, 16 GByte DDR4-RAM und eine M.2-SSD mit 512 GByte.

Für darüber hinausgehende Ansprüche wie z. B. Grafik- oder Videobearbeitung bieten wir noch zwei leistungsstärkere Geräte an, welche an einen Curved-Dual-QHD-Monitor (5.120 x 1.440) angeschlossen sind. Diese PCs sind mit einem Prozessor vom Typ Intel Core i7-8705G, 32 GByte DDR4-RAM und ebenfalls einer M.2-SSD mit 512 GByte ausgestattet. Um genug Grafikleistung für den Bildschirm und eventuelle Grafikanwendungen zur Verfügung zu stellen, wird die Onboard-Grafikeinheit von Intel durch eine AMD Radeon RX Vega M GL unterstützt.

Außerdem bieten wir weiterhin unseren Großformatscanner „Contex HD4230“ an. Bei der Nutzung bitten wir zwecks kurzer Einweisung um vorherige Terminabsprache. Dieser Scanner unterstützt das Scannen von Vorlagen bis zu 106 cm Breite.

Darüber hinaus befinden sich im Benutzerraum auch ein Diascanner, ein DIN-A4- und ein DIN-A3-Scanner, der über eine Durchlichteinheit verfügt. Somit kann dieser auch Dias, Negative sowie Overheadfolien einscannen. Zum Scannen der Dias

stehen verschiedene Masken zur Verfügung, um mehrere Dias in einem Arbeitsgang zu scannen. Die Geräte sind an unterschiedlichen PCs angeschlossen, auf denen jeweils die passenden Treiber installiert sind.

Software

Als Betriebssystem kommt auf allen neuen PCs Windows 10 64-bit zum Einsatz. Zur Software, die als Standard auf alle PCs verteilt wurde, gehören u. a. PDF-XChange PRO, Firefox, Chrome Opera, Notepad++, VLC Media Player, IrfanView, X-Win32, WinSCP, Google Earth, 7-Zip und natürlich auch Microsoft Office Professional Plus 2019. Auf einigen PCs sind zusätzlich auch die Adobe Creative Suite und Corel Draw installiert. Wir versuchen natürlich, die Software für die Geräte so aktuell wie möglich zu halten. Falls Software auf einem PC fehlen oder Wünsche oder Vorschläge für neue Software bestehen sollten, können Sie sich gerne an unsere Service-Hotline wenden.

Heise



Öffnungszeiten des Rechenzentrums um Weihnachten und Neujahr 2019/2020

Das Rechenzentrum der GWDG bleibt an den Tagen vom 24.12. bis zum 26.12.2019 sowie am 31.12.2019 und 01.01.2020 geschlossen. Am 23.12., 27.12. und 30.12.2019 ist das Rechenzentrum lediglich von 9:00 bis 17:00 Uhr und am 28.12. und 29.12.2019 wie an Wochenenden üblich von 10:00 bis 18:00 Uhr geöffnet.

Falls Sie sich während der Zeiten, in denen das Rechenzentrum geschlossen 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 während dieser Zeiten von Mitarbeiterinnen und Mitarbeitern der GWDG regelmäßig überprüft.

Wir bitten alle Nutzerinnen und Nutzer, sich darauf einzustellen.

Pohl

Doppelausgabe 01-02/2020 der GWDG-Nachrichten

Die nächsten GWDG-Nachrichten erscheinen wie gewohnt als Doppelausgabe 01-02/2020 Anfang Februar 2020.

Otto

Kursprogramm 2020

Das bisherige bekannte Kursangebot der GWDG wird zurzeit in mehrfacher Hinsicht überarbeitet. Zum einen soll es inhaltlich schrittweise erweitert werden. Hierzu gehören sowohl neue Themen und Schwerpunkte als auch neue Formate neben den bisher üblichen Blockkursen wie z. B. Workshops oder Online-Kurse. Zum anderen soll auch die Präsentation des Schulungsangebotes im Kundenportal der GWDG komplett neugestaltet werden. Des Weiteren sollen zusätzliche Zielgruppen, vor allem Studierende, mit dem erweiterten Schulungsangebot angesprochen werden und das Anmeldeverfahren vereinfacht werden. Da noch abschließende Arbeiten für diese umfangreiche Überarbeitung zu erledigen sind, verzögert sich die Veröffentlichung des Kursprogramms leider noch um einige Tage. Wir planen, spätestens Mitte Januar damit online gehen zu können und bitten daher noch um etwas Geduld. Sobald das Kursprogramm veröffentlicht ist, werden wir natürlich über unsere üblichen Kanäle dazu informieren. Für die nächsten GWDG-Nachrichten 01-02/2020 ist ein ausführlicherer Artikel zu den Neuerungen beim Schulungsprogramm der GWDG geplant.

Otto



FTP-Server

Eine ergiebige Fundgrube!

Ihre Anforderung

Sie möchten auf das weltweite OpenSource-Softwareangebot zentral und schnell zugreifen. Sie benötigen Handbücher oder Programmbeschreibungen oder Listings aus Computerzeitschriften. Sie wollen Updates Ihrer Linux- oder FreeBSD-Installation schnell durchführen.

Unser Angebot

Die GWDG betreibt seit 1992 einen der weltweit bekanntesten FTP-Server mit leistungsfähigen Ressourcen und schneller Netzanbindung. Er ist dabei Hauptmirror für viele Open-Source-Projekte.

Ihre Vorteile

- > Großer Datenbestand (65 TByte), weltweit verfügbar
- > Besonders gute Anbindung im GÖNET



- > Aktuelle Software inkl. Updates der gebräuchlichsten Linux-Distributionen
- > Unter pub befindet sich eine aktuell gehaltene locatedb für schnelles Durchsuchen des Bestandes.
- > Alle gängigen Protokolle (http, https, ftp und rsync) werden unterstützt.

Interessiert?

Wenn Sie unseren FTP-Server nutzen möchten, werfen Sie bitte einen Blick auf die u. g. Webseite. Jeder Nutzer kann den FTP-Dienst nutzen. Die Nutzer im GÖNET erreichen in der Regel durch die lokale Anbindung besseren Durchsatz als externe Nutzer.

>> www.gwdg.de/ftp-server

Stellenangebot

Die GWDG sucht ab sofort zur Unterstützung der Arbeitsgruppe „Nutzerservice und Betriebsdienste“ (AG H) zwei

Studentische Hilfskräfte (m/w/d)

mit einer Beschäftigungszeit von bis zu 40 Stunden im Monat. Die Vergütung erfolgt entsprechend den Regelungen für Studentische/Wissenschaftliche Hilfskräfte. Die Stellen sind zunächst auf ein Jahr befristet.

Aufgabenbereiche

- Mitarbeit im First-Level-Support (Helpdesk)
- Mitarbeit bei der Systemüberwachung und Peripheriebetreuung abends und an Wochenenden

Diese Aufgaben sind unter der Anleitung wissenschaftlicher Mitarbeiter zu bearbeiten.

Anforderungen

- Schnelle Lernfähigkeit
- Gute Kommunikations- und Teamfähigkeit
- Gute Deutsch- und Englischkenntnisse in Wort und Schrift
- Gute IT-Kenntnisse

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 **06.01.2020** über unser Online-Formular unter <https://s-lotus.gwdg.de/gwdgdb/agh/20191209.nsf/bewerbung>.

Fragen zu den ausgeschriebenen Stellen beantwortet Ihnen:

Herr Eric Helmvoigt

Tel.: 0551 201-1845

E-Mail: eric.helmvoigt@gwdg.de oder

Herr Stefan Quantin

Tel.: 0551 201-1816

E-Mail: stefan.quantin@gwdg.de



NEUER MITARBEITER HENDRIK NOLTE

Seit dem 1. November 2019 ist Herr Hendrik Nolte als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „eScience“ (AG E) tätig und verstärkt dort das HPC-Team. Herr Nolte hat an der Georg-August-Universität Göttingen Physik studiert und konnte dabei schon praktische Erfahrungen mit dem Scientific Compute Cluster der GWDG sammeln. Schwerpunkt seiner Tätigkeit sind Arbeiten im Projekt „Tapping Into a Resource Hidden Behind MR Images: Learning Quantitative Imaging Biomarkers from Raw Big Data“, wo er eine Datenanalyse-Pipeline zur Verarbeitung von MRT-Bildern entwickeln wird. Herr Nolte ist per E-Mail unter hendrik.nolte@gwdg.de und telefonisch unter 0551 201-2119 erreichbar.



Wieder



NEUER MITARBEITER JENS LUCHT

Seit dem 1. November 2019 ist Herr Jens Lucht als wissenschaftliche Hilfskraft in der Arbeitsgruppe „IT-Infrastruktur“ (AG I) tätig und verstärkt dort das Netzwerkteam. Er absolviert zurzeit sein Masterstudium im Fach Physik an der Georg-August-Universität Göttingen. Herr Lucht war bereits vorher bei der GWDG im Bereich ownCloud und GitLab tätig und hat umfangreiche Expertise als Netzwerkadministrator in einem Wohnheim des Studentenwerks Göttingen gesammelt. Schwerpunkte seiner Tätigkeit werden Programmierarbeiten für die Netzwerkautomatisierung sowie die Planung und der Aufbau des Kubernetes-Clusters sein. Herr Lucht ist per E-Mail unter jens.lucht@gwdg.de und telefonisch unter 0551 39-30213 zu erreichen.

IBleiber

NEUER MITARBEITER FELIX KETTENBEIL

Seit dem 1. November 2019 ist Herr Felix Kettenbeil als wissenschaftliche Hilfskraft in der Arbeitsgruppe „IT-Infrastruktur“ (AG I) tätig und verstärkt dort das Netzwerkteam. Herr Kettenbeil hat im Rahmen seines Studiums im Fach Informatik an der Georg-August-Universität Göttingen eine Bachelorarbeit zum einem Thema aus dem Bereich der modernen Netzwerktechnologien in Rechenzentren bei der GWDG geschrieben und bringt damit nützliche Grundlagen für unsere Planungen zu Automatisierungen in der Netzwerkinfrastruktur im neuen gemeinsamen Rechenzentrum mit. Er wird überdies die Gestaltung der geplanten Kurse zu Netzwerkgrundlagen für Studierende unterstützen. Herr Kettenbeil ist per E-Mail unter felix.kettenbeil@gwdg.de zu erreichen.

IBleiber





Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen