DFN mitteilungen

Kinder, wie die Zeit vergeht!

die 100. Ausgabe zum Advent

Auf die Verlässlichkeit

das Vertrauensniveau in der DFN-AAI

Neue Strukturen für die Wissenschaft

NHR & NFDI im Gespräch

9 770177 689001

Impressum

Herausgeber: Verein zur Förderung
eines Deutschen Forschungsnetzes e. V.

DFN-Verein
Alexanderplatz 1, 10178 Berlin
Tel.: 030 - 88 42 99 - 0
Fax: 030 - 88 42 99 - 370
Mail: presse@dfn.de
Web: www.dfn.de

ISSN 0177-6894

Redaktion: Maimona Id, Nina Bark
Lektorat: Angela Lenz
Mitarbeit an dieser Ausgabe: Stella Lenz
Gestaltung: Labor3 | www.labor3.com
Druck: Druckerei Rüss, Potsdam

Fotonachweis
Titel: michaklootwijk / Adobe Stock
Rückseite: michaklootwijk / Adobe Stock

Prof. Dr. Dieter Kranzlmüller
Professor für Informatik an der Ludwig-Maximilians-Universität München (LMU), Vorsitzender des Direktoriums des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften (LRZ)

Wie wollen wir gemeinsam die Zukunft von Forschung und Wissenschaft gestalten? In der Beantwortung dieser essenziellen Frage ist eine Aufbruchstimmung in der deutschen Wissenschaftscommunity zu spüren: Innerhalb von zwölf Monaten sind aus ihrer Mitte nach Jahren der Vorbereitung gleich zwei neue nationale Player auf dem öffentlichen Parkett erschienen: die Nationale Forschungsdateninfrastruktur (NFDI) und das Nationale Hochleistungsrechnen (NHR). Sie sind angetreten, den Umgang mit Forschungsdaten in Deutschland neu zu formieren, zu strukturieren und neue Wege der fächerübergreifenden Zusammenarbeit zu beschreiten. Nicht zufällig sind beide als Verein organisiert – nach dem Vorbild des Gauss Centre for Supercomputing e. V., der Gauß-Allianz e. V. und nicht zuletzt des DFN-Vereins, salopp gesagt, der Mutter aller E-Infrastrukturen hierzulande.

NFDI und NHR bauen beide auf streng wissenschaftsgeleiteten Prozessen auf und setzen auf bedarfsgerechte Lösungen. Beide haben ein kompetitives Ausschreibungsverfahren angestrengt, um die innovativsten Ideen und Konzepte aus der Community zu vereinen.

Der Verein Nationale Forschungsdateninfrastruktur hat es sich auf die Fahne geschrieben, für das Forschungsdatenmanagement in der Wissenschaft disziplinübergreifend eine gemeinsame Sprache zu finden sowie einheitliche Standards zu schaffen. Er möchte Forschenden in nie gekannter Weise ermöglichen, ihren Wissensschatz auszutauschen und Daten gemäß den FAIR-Prinzipien nachzunutzen.

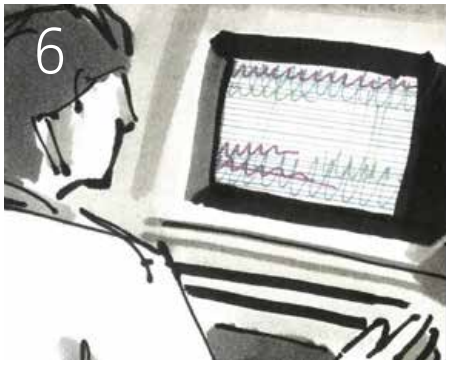
Der Verein für Nationales Hochleistungsrechnen ist mit dem Ziel an den Start gegangen, kostbare HPC-Ressourcen der Ebene 2 zu koordinieren, gerecht zu vergeben und damit verteilte Infrastrukturen effizient zu nutzen. Darüber hinaus möchte er fächerübergreifendes Community-Building fördern.

Beide sehen einen wichtigen Aspekt im Aufbau und der Ausbildung von Nachwuchskräften, um die Strukturen für kommende Generationen nachhaltig zu festigen. Nicht umsonst sind die Förderperioden mit jeweils zehn Jahren hoch angesetzt.

Wie aufregend der Aufbau eines Vereins besonders in unserer Wissenschaftscommunity ist, können Sie in dieser Ausgabe der DFN-Mitteilungen – der Nummer 100 – anhand der Titelcover aus 37 Jahren nachvollziehen. Das eine oder andere kommt Ihnen bestimmt noch bekannt vor. Mit den beiden neuen Vereinen ist die Wissenschaftslandschaft in Deutschland wieder ein Stück reicher geworden, ganz nach dem Motto: „Das Ganze ist mehr als die Summe seiner Teile“ – sehr viel mehr, wie ich finde!

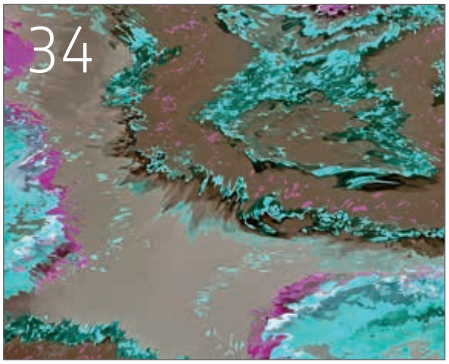
Herzlichst Ihr
Dieter Kranzlmüller

Inhalt



Im Spiegel der Zeit – Die DFN-Mitteilungen
Titel sagen mehr als tausend Worte – in hundert Ausgaben durch das Deutsche Forschungsnetz (DFN).

Rechnen verbindet – Startschuss für den NHR-Verein
Fair, einfach und transparent: Ein neues Antragsverfahren erleichtert Forschenden den Zugang zu Rechenzeit.



Quantennetze – zwischen Realität und Zukunft
Der Weg zu Quantennetzen im Produktionsbetrieb ist nicht mehr allzu weit: Die Anwendungsmöglichkeiten sind breit gefächert.

DFN-Verein

Wissenschaftsnetz

International

Forschung

Sicherheit

Campus

Weiterentwicklung der DFN-PKI mit GÉANT TCS
Besser automatisiert und komfortabel: Mit TCS ist die Ausstellung von Zertifikaten nun über die DFN-AAI möglich.

Recht

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Maimona Id, DFN-Verein (id@dfn.de); **2** Andrea Wardzichowski, DFN-Verein (wardzichowski@dfn.de); **3** Dr. Jakob Tendel, DFN-Verein (tendel@dfn.de); **4** Leila Dekkar, GÉANT Association (leila.dekkar@geant.org); **5** Harinaina R. Ravelomanantsoa, i RENALA (harinaina.ravelomanantsoa@irenala.edu.mg); **6** Dr. Peter Kaufmann, DFN-Verein (kaufmann@dfn.de); **7** Dr.-Ing. Susanne Naegele-Jackson, Friedrich-Alexander-Universität Erlangen-Nürnberg (susanne.naegele-jackson@fau.de); **8** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **9** Jürgen Brauckmann; DFN-CERT Services GmbH (brauckmann@dfn-cert.de); **10** Ralf Paffrath, DFN-Verein (paffrath@dfn.de); **11** Dr. Matthias Baume, Technische Universität München (matthias.baume@tum.de); **12** Nina Muris-Wendt, Technische Universität München (nina.muris-wendt@prolehre.tum.de); **13** Mizuki Ando, Technische Universität München (mizuki.ando@tum.de); **14** Justin Rennert, Forschungsstelle Recht im DFN (j_renno5@uni-muenster.de); **15** Owen Mc Grath, Forschungsstelle Recht im DFN (o.mcgrath@uni-muenster.de)

Im Spiegel der Zeit – Die DFN-Mitteilungen

100 Ausgaben, 37 Jahre, 901 Artikel und 3757 Seiten: Prall gefüllt mit dem Wissen und den Erfahrungen unserer Mitglieder und Teilnehmer, sind die DFN-Mitteilungen ein Zeitzeugnis für die rasante Entwicklung des Internets im Allgemeinen und des Wissenschaftsnetzes im Besonderen.

Text: **Maimona Id** (DFN-Verein)

1985

Beim Durchstöbern der alten Ausgaben haben wir oft gestaunt, das eine oder andere Mal gelacht und nicht wenige Male waren wir beeindruckt, was die Gemeinschaft unseres Vereins – das Fundament für ein stabiles Deutsches Forschungsnetz – in 37 Jahren nachhaltig aufgebaut hat.

Aufregend muss es in den Pionierjahren gewesen sein: von der Vereinsgründung über die Wiedervereinigung Deutschlands und dem lang ersehnten, herzlichen Empfang der ostdeutschen Wissenschaftseinrichtungen bis in die Gegenwart.

Aus der Mitte der Wissenschaft gründete sich am 12. Januar 1984 das Deutsche Forschungsnetz (DFN). Die erste Ausgabe der DFN-Mitteilungen erschien etwa ein Jahr später im Februar 1985. Darin berichtete Gründungsvorstand Prof. Dr. Karl Zander über die bewegten ersten Wochen des Vereins. O-Ton zur ersten im März 1982 am DESY (Deutsches Elektronen-Synchrotron) stattfindenden „Diskussionsversammlung der an einem Rechnerverbund Interessierten“: „Die Optimisten überwogen, Pessimisten leisteten wertvolle kritische Beiträge; eine wenn auch noch kleine Gemeinschaft von motivierten Verbundideologen war entstanden“. Heute bildet das Deutsche Forschungsnetz eine große Gemeinschaft aus 351 Vereinsmitgliedern und 1000 Teilnehmern in ganz Deutschland.

DFM Mitteilungen I Ausgaben 2 - 20

1986

1987

Doppelheft 9/10

Ziel der DFN-Mitteilungen war, die zunächst formal zusammengeschlossenen Institutionen und Einrichtungen dabei zu unterstützen, eine lebendige Gemeinschaft zu bilden, die die gewaltige Aufgabe hatte, das zur damaligen Zeit größte deutsche Verbundprojekt auf dem Gebiet der Kommunikationstechnik zu errichten und zu betreiben. Außerdem sollte die Zeitschrift ein Ort sein, an dem die DFN-Community sich über ihre Erfahrungen, Ideen und Vorstellungen zum Aufbau einer fortschrittlichen und leistungsfähigen Infrastruktur austauschen kann.

Mit den 100 Covern unserer Vereinszeitschrift nehmen wir Sie in dieser Ausgabe mit auf eine Zeitreise durch die Jahrzehnte: von den 80er Jahren mit den Anfängen und Entwicklungen des Internets bis in die 20er Jahre des neuen Jahrtausends. Wie sich die Mitteilungen dabei auch optisch verändert haben, können Sie anhand der Titelbilder und beim Stöbern in den alten Ausgaben auf unserer Webseite entdecken.

Wir danken allen Autorinnen und Autoren, externen wie internen, die die DFN-Mitteilungen mit ihren informativen und fundierten Artikeln über die Jahre bereichert haben. Und natürlich geht ein ganz großer Dank an unsere treuen Leserinnen und Leser, denen wir in jeder Ausgabe einen spannenden Einblick in die Welt des Deutschen Forschungsnetzes geben möchten. Bleiben Sie uns gewogen, viel Spaß beim Stöbern!

Alle bisherigen Ausgaben der DFN-Mitteilungen finden Sie unter: **https://www.dfn.de/publikationen/dfnmitteilungen/**

Rechnen verbindet – Startschuss für den NHR-Verein

Mit einem weinenden, aber auch einem lachenden Auge verabschiedet der DFN-Verein das Projekt „Geschäftsstelle für den Strategieausschuss in der Gründungsphase des NHR“. Am 23. August 2021 wurde der Verein für Nationales Hochleistungsrechnen (NHR) nach gut zweijähriger Projektphase mit dem Ziel gegründet, die Rechenzentren der Ebene 2 in einer gemeinsamen zukunftsfähigen Struktur zusammenzufassen. Damit ist die NHR-Geschäftsstelle jetzt im neuen Verein angesiedelt. Begleitet wurde der Prozess vom NHR-Strategieausschuss, einem von der Gemeinsamen Wissenschaftskonferenz (GWK) eingesetzten Expertengremium. Der Vorsitzende Prof. Dr. Rolf Krause und die stellvertretende Vorsitzende Prof. Dr. Miriam Schulte erzählen, welche Vorteile und Synergien sich nun aus NHR ergeben.

Wir beim DFN-Verein haben hautnah die aufregende und intensive zweijährige Projektphase miterlebt, an deren Ende jetzt der neu gegründete NHR-Verein steht. Was ist die zentrale Idee hinter dem Verbund?

Rolf Krause: Eine wesentliche Idee ist, dass die Ressourcen der Rechenzentren einheitlich und zentral vergeben werden. Der Zugriff auf die Rechenzeit und die damit verbundenen fachlichen Kompetenzen erfolgen also nicht mehr ortsabhängig, sondern wissenschaftsgeleitet. Das heißt, ich kann auf verschiedene Rechenzentren zugreifen, ganz egal wo sie sind.

Als Forscher habe ich damit nicht nur eine wesentlich größere Chance, Rechenzeit zu erhalten. Ich kann auch auf viel mehr und auf unterschiedliche Hardware zugreifen. Dadurch wird das deutschlandweite NHR-System mit seinen Ressourcen viel besser ausgenutzt.

Miriam Schulte: Eine der ersten Aufgaben des Strategieausschusses war die Entwicklung eines neuen und einheitlichen Antragsverfahrens, das dafür sorgt, dass der Zugang zu Rechenzeit fair, einfach und transparent ist. Dadurch wird den Forschenden die tägliche Arbeit erleichtert. Bisher war das in den einzelnen Zentren und Landesinitiativen sehr unübersichtlich. Zum ersten Mal wird damit eine deutschlandweit einheitliche Vergabe realisiert.

Wie funktioniert die Verteilung der Rechenzeit denn konkret?

Rolf Krause: Dazu gab es eine Arbeitsgruppe im Strategieausschuss, die Ideen entwickelt hat, wie der Zugriff auf Rechenzeit bestmöglich gestaltet werden kann. Das war mit erheblichen Diskussionen verbunden. Aber jetzt sind wir einen großen Schritt weiter: Die NHR-Zentren haben auf Grundlage unserer Empfehlungen eine gemeinsame Vergabeordnung entwickelt, welche zukünftig über ein gemeinsames Antragsportal realisiert wird. Die technischen Möglichkeiten zur Umsetzung sind da. Die Kolleginnen und Kollegen arbeiten daran, das Portal aufzubauen. Das Ganze muss sich im Alltag bewähren und soll anschließend komplett aufgebaut werden.

Gibt es weitere Vorteile für Forschende?

Miriam Schulte: Die NHR-Zentren sind an inhaltlichen Forschungsthemen ausgerichtet, jedes hat seinen fachlichen Fokus. Dadurch habe ich als Nutzerin jetzt die Möglichkeit, die richtige Fachcommunity zu finden. NHR macht mich unabhängig davon, welche Forschungsschwerpunkte es an meinem Heimatrechenzentrum gibt. Bisher haben die Leute in ihren Heimatrechenzentren ein Stück weit isoliert gearbeitet und Dinge für sich entwickelt. Über NHR kommen sie nun an das thematisch zuständige Zentrum und finden dort entsprechende Partner mit ähnlichem Forschungsfokus. Da entstehen Synergien, die wir bisher noch gar nicht erahnen können.

Rolf Krause: Mit einem breiten Angebot an gemeinsamen Veranstaltungen, Workshops und Trainingsangeboten werden die Nutzer zusammengebracht und es entsteht eine hervorragend vernetzte und gut funktionierende Community. Das ist die große Stärke von NHR.

Miriam Schulte: Meine große Hoffnung ist darüber hinaus, dass wir es mit NHR

Prof. Dr. Miriam Schulte, Leiterin des Instituts für Parallele und Verteilte Systeme (IPVS), Lehrstuhl für „Simulation großer Systeme“ im Fachbereich Informatik der Universität Stuttgart

Forschungsschwerpunkte: gekoppelte Simulationen, massiv parallele Gleichungssystemlöser, effiziente Datenstrukturen, biomechanische Systeme und Umweltsysteme

schaffen werden, wissenschaftliche Software besser zur Verfügung zu stellen. Ich meine damit Hilfsbibliotheken, die bei einer Rechnung allgemeine Aufgaben übernehmen und vielleicht auf den Rechnern schon vorinstalliert sind. Wenn ich mir solche Programme selbst herunterladen und mit allen Abhängigkeiten installieren oder sogar selbst schreiben muss, ist das ein ziemlicher Aufwand. Wir sollten hier auch ganz speziell Software aus Deutschland fördern, bisher kommen solche Bibliotheken meist aus den National Labs in den USA.

Rolf Krause: Wenn wir uns mit den USA vergleichen, wo sehr viel Entwicklung im HPC-Bereich stattfindet, muss man feststellen, dass die Forschung in Deutschland ziemlich zersplittert ist. Lediglich in bestimmten Bereichen wie Performance Monitoring, speziellen Algorithmen oder Anpassungen an besondere Hardware, GPUs etc. spielen wir ganz vorne mit. Geht es jedoch um Softwarebibliotheken, dann greifen wir sehr häufig auf Entwicklungen der National Labs in den USA zurück. Etwas Vergleichbares wie die National Labs haben wir in Deutschland nicht. Mit NHR haben wir zum ersten Mal die Chance, auf nationaler Ebene einen Verbund zu schaffen, der künftig genug Know-how und Ressourcen zur Verfügung stellt, um auf internationaler Ebene – auch im Softwarebereich – mitzuspielen.

Miriam Schulte: In Deutschland gibt es viele clevere Detaillösungen, aber es ist gar nicht so einfach, diese in die Breite zu bringen. Mit NHR haben wir eine Infrastruktur, die das ermöglicht und die deutsche Entwickler-Community stärkt. Es geht darum, die vorhandenen Ressourcen zu koordinieren. Wenn wir das schaffen, bringt uns das sicherlich auch auf internationaler Ebene weiter.

Was waren die größten Herausforderungen, welche Lektionen haben Sie gelernt?

Rolf Krause: Die allergrößte Herausforderung war es, den politisch formulierten Willen zur Kooperation in ein wissenschaftlich schlüssiges Konzept umzusetzen, welches allen beteiligten Zentren eine gute Struktur bietet, in der sie erfolgreich miteinander arbeiten können. Es ist überaus wichtig, dass Zuwendungsgeber und Forscher offen miteinander reden können, ohne dass sich die Fronten verhärten. Leute mit unterschiedlichem Background treffen zusammen, die Sachverhalte teils völlig anders interpretieren. Das klingt trivial, aber es ist schon eine Herausforderung, wenn Politik und Wissenschaft an einem Tisch sitzen. Hier hat das Team der NHR-Geschäftsstelle hervorragende Arbeit geleistet und die Treffen organisatorisch und inhaltlich so vorbereitet, dass wir gemeinsam sehr gute Ergebnisse erzielen konnten.

Das klingt, als ob es im Strategieausschuss auch mal ans Eingemachte geht.

Rolf Krause: Ja, vielleicht rumpelt es mal, aber es macht auch Spaß. Wir diskutieren viel. NHR hat nun einmal zwei Dimensionen: eine wissenschaftliche und eine politisch-strategische. Die Herausforderung bestand letztlich darin, gemeinsam die richtigen Zentren auszuwählen und sie beim Aufbau des Verbundes zu unterstützen.

Miriam Schulte: Ich bin noch ziemlich neu im Strategieausschuss. Ich habe

die letzten zwei Jahre aber als Teil der Gutachterkommission erlebt und den Entstehungsprozess genau beobachten können. Die Anträge waren zum Teil so heterogen, dass sie schwer zu vergleichen waren. Da stellt sich die Frage, ob man exaktere Vorgaben hätte machen müssen, weil die Begutachtung doch sehr schwierig war. Mein Fazit ist aber, dass wir von den vielen tollen Ideen aus den Anträgen eher profitiert und beim Lesen eine Menge gelernt haben.

Rolf Krause: Unbedingt. Wie Du schon sagst, die Zentren haben in ihren Anträgen vielfältige und teils sehr verschiedene Ideen dargestellt. Natürlich war eine inhaltliche Abstimmung in dem kompetitiven Auswahlverfahren nicht zu erwarten. Wir haben versucht, die innovativen Ideen aus den Anträgen zu sortieren und gebündelt als Empfehlung an den NHR-Verbund zurückzugeben.

Miriam Schulte: Eine weitere Herausforderung: Außerhalb der klassischen High Performance Computing-Community wissen viele Forschende noch gar nicht, dass es NHR gibt. Deutschlandweit gibt es viele Nutzer, die auf die größeren Maschinen gehen wollen, aber noch davor zurückschrecken, weil das Know-how fehlt. An dieser Stelle sollen sie jetzt durch NHR unterstützt werden. Mit der Stärkung der methodischen Kompetenzen und einem sinnvollen und effizienten Einsatz der Methoden erreichen wir, dass die teure Infrastruktur energie- und kosteneffizient genutzt wird. Natürlich müssen die NHR-Zentren auf die Leute zugehen und auch außerhalb der eigenen lokalen Nutzerkreise neue Nutzer akquirieren. Es braucht noch viel mehr Aufklärungsarbeit und ein gutes Angebot an Schulungen, die aber auch Teil der Anträge waren.

Was macht den NHR lebendig neben der Infrastruktur?

Rolf Krause: Ganz einfach, das sind die Menschen. Wir reden immer von Infrastruktur und Hardware, aber am Ende sind es die Menschen, die die Gemeinschaft bilden und den Verein lebendig machen. Es gibt bereits erste vielversprechende gemeinsame Projekte zwischen den beteiligten NHR-Zentren.

Ein ganz zentraler Punkt ist die Förderung des wissenschaftlichen Nachwuchses. Eines der ersten Projekte des NHR-Vereins ist der Aufbau einer Graduiertenschule. Damit wird nicht nur die zukünftige Basis der HPC-Forschung gestärkt – durch das gemeinsame Ausbildungsprogramm entsteht auch eine gemeinsame Community und die Zusammengehörigkeit wird gefördert. Der Ansatz lautet: gemeinsame Struktur, partiell gemeinsame Forschung und gemeinsame Ausbildung.

Zu einer lebendigen Gemeinschaft gehört neben der fachlichen Diversität auch die soziale. Spielt das eine Rolle im NHR-Verbund?

Rolf Krause: Diversität ist ein gutes Stichwort. Im Hinblick auf Internationalität haben wir kein großes Problem. Mit der künftigen Graduiertenschule bekommt NHR hoffentlich ein sehr internationales Publikum. In Bezug auf den Frauenanteil sehe ich jedoch nach wie vor die klassische Geschlechterverteilung in den verschiedenen Disziplinen. In der Informatik gibt es weiterhin relativ wenige Frauen, auch wenn das in den vergangenen Jahren etwas besser geworden ist.

Miriam Schulte: Gerade bei den Anträgen hatten wir schon ein Gender-Problem. Mit den internationalen Gutachtern – das muss ehrlich gesagt werden – haben wir gekämpft. Deren Tenor war, dass sie das aufgrund der Männerüberzahl unter den Antragstellern eigentlich nicht befür-

Prof. Dr. Rolf Krause, Direktor des Euler Institute an der Università della Svizzera italiana, Lehrstuhl für Wissenschaftliches Rechnen an der Fakultät für Informatik, Kodirektor des „Center for Computational Medicine in Cardiology“. Forschungsschwerpunkte: Computional Medicine, Computational Engineering, High Performance Computing, Machine Learning, Mathematical optimization, Scientific Software

worten können. Da waren vielleicht zwei Frauen darunter.

Rolf Krause: Tatsächlich gibt es unter den Rechenzentrumsleitungen keine einzige Frau. Erst auf Ebene der Projektleitungen findet man einige wenige. Dennoch bleibt der Anteil deutlich unter 20 Prozent. Dementsprechend müssen wir bei den kommenden Generationen ansetzen. Mit der Graduiertenschule hat der NHR-Verbund die Möglichkeit, das Geschlechterverhältnis zu beeinflussen.

Miriam Schulte: Wir haben alle, sowohl Männer als auch Frauen, einen unheimlichen Bias (Anm. Red. geschlechtsbezogener Verzerrungseffekt). Frauen schrecken vor der Technik zurück und werden aber auch von der männlichen Community oft auf unpassende Weise behandelt. Den Männern ist das oft gar nicht bewusst. Wahrscheinlich müssen wir in unserem Umfeld bei den Rechenzentren anfangen. Ich habe bisher immer gedacht, dass wir so etwas nicht brauchen, aber vielleicht müssen wir über Schulungen oder Workshops in dieser Richtung nachdenken.

Rolf Krause: Wir haben gewisse Rollenbilder und Verhaltensweisen, die wir irgendwie aufbrechen müssen. Im Hochleistungsrechnen könnten wir vielleicht mehr die Anwendungsseite und weniger die rein technische Seite beleuchten. Wenn eine sinnvolle Anwendung dazu kommt, sieht das Geschlechterverhältnis schon wieder anders aus, ist mein Eindruck.

Miriam Schulte: Das stimmt. Wenn Du den Studiengang Informatik zum Beispiel mit zehn Prozent anderen Inhalten anreicherst und dann Medieninformatik nennst, dann hast Du auf einmal 50 Prozent Studentinnen, obwohl es zum größten Teil die gleichen Inhalte geblieben sind.

Rolf Krause: Wir assoziieren Hochleistungsrechnen immer mit Informatik. Ich denke, das ist zu eng gefasst. Die Idee des Hochleistungsrechnens ist ja letzten Endes, den Forschenden aller möglichen Fachdisziplinen geeignete Werkzeuge zur Verfügung zu stellen, mit denen sie schnell zu ihren Ergebnissen kommen. Und diese sind in den seltensten Fällen Informatiker, da ist vielleicht jemand aus der Medizin oder aus der Biologie, der nicht weiß, was eine GPU oder eine CPU ist. Die brauchen Unterstützung bei der Beantwortung der Frage, welche Hardware am besten zu ihrer Anwendung passt und wie sie ihre Programme am effizientesten auf einem Hochleistungsrechner zum Laufen bringen. Wir müssen kooperativ denken, im Sinne des Gesamtbildes. Um mal in der Mathematik zu bleiben, am Ende sind wir vor der Tafel alle gleich.

Zu guter Letzt: Was wünschen Sie dem NHR-Verein für die nächsten zehn Jahre?

Rolf Krause: Ich wünsche mir, dass wir es schaffen, möglichst viele Leute anzusprechen und Nutzer zu gewinnen, die sich im interdisziplinären Bereich zu Hause fühlen. Gerade der wissenschaftliche Nachwuchs spielt hier eine große Rolle. Und natürlich, dass wir weiterhin so gut zusammenarbeiten. Dieser großartige Start und diese positive Grundstimmung sind nicht selbstverständlich!

Miriam Schulte: Dem kann ich nur zustimmen. Ich glaube, dass wir gerade mit den Ebene-2-Zentren im NHR die Chance haben, die Grenzen zwischen der Informatik und den Anwendungen zu öffnen – vielleicht sogar besser als auf der obersten HPC-Ebene-1. Ich wünsche mir für unsere NHR-Communities ein großes Plus an Synergien und Effizienz. Aber vor allem wünsche ich allen Beteiligten viel Spaß und Freude daran, im Hochleistungsrechnen etwas zu bewegen.

Die Fragen stellte Maimona Id (DFN-Verein)

NHR-ECKDATEN

- → Gemeinsame Förderung durch Bund und Länder im Verhältnis 50/50
- → Fördervolumen insgesamt: bis zu 62,5 Mio. Euro/Jahr
- → Laufzeit der Förderung: zunächst zehn Jahre
- → Dem NHR-Verbund gehören folgende Hochschulen/Rechenzentren der Ebene 2 an:
  - NHR4CES@RWTH – IT Center – RWTH Aachen
  - NHR@ZIB – Zuse-Institut Berlin – Berlin University Alliance
  - NHR4CES@TUDa – Hochschulrechenzentrum (HRZ) – Technische Universität Darmstadt
  - NHR@TUD – ZIH – Zentrum für Informationsdienste und Hochleistungsrechnen – Technische Universität Dresden
  - NHR@FAU – Regionales Rechenzentrum Erlangen - Universität Erlangen-Nürnberg
  - NHR@GWDG – Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen – Universität Göttingen
  - NHR@KIT – Steinbuch Centre for Computing (SCC) – Karlsruher Institut für Technologie
  - PC2 – Paderborn Center for Parallel Computing – Universität Paderborn
  - NHR Süd-West – Johannes Gutenberg-Universität Mainz, Technische Universität Kaiserslautern, Goethe-Universität Frankfurt und Universität des Saarlandes

Auf dem Weg zum Verein –

Mit der Gründung des NHR-Vereins wird in Deutschland das Hochleistungsrechnen der Ebene 2 an den Hochschulen, das bisher auf Länderebene organisiert war, in der Wissenschaft neu strukturiert. Der NHR-Verein besteht aus mehreren NHR-Zentren, die sowohl die Hochleistungsrechner betreiben als auch ein koordiniertes Beratungsangebot zur Methodenkompetenz des wissenschaftlichen Hochleistungsrechnens anbieten. Ziel ist es, Wissenschaftlerinnen und Wissenschaftlern der deutschen Hochschulen bedarfsgerecht die für ihre Forschung benötigte Rechenkapazität zur Verfügung zu stellen und ihre Kompetenzen zur effizienten Nutzung dieser Ressource zu stärken.

Dr. Heide Ahrens
Generalsekretärin der Deutschen Forschungsgemeinschaft (DFG)

Mit dem Aufbau des NHR-Verbundes leisten Bund und Länder einen wesentlichen Beitrag zur Bereitstellung von Hochleistungsrechnerkapazität für deutsche Hochschulen. Durch die Finanzierung auch von Betrieb und Personal wird eine effektive Nutzung sichergestellt. Die DFG unterstützt die eingeschlagene Linie sehr, neben der Investition auch langfristig die operativen Kosten aus einer Hand zu finanzieren. Wir erwarten davon Signalwirkungen auch für weitere Technologiegebiete.

Prof. Dr. Hans-Joachim Bungartz
Professor für Informatik und Mathematik an der TU München, Mitglied des Direktoriums des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften (LRZ)

Bei den Diskussionen in der Arbeitsgruppe des Wissenschaftsrats war es zunächst nur um die Zielstruktur und deren institutionelle Aufhängung gegangen. Mit zunehmender Konkretheit des Ganzen wurde die Frage „Und wie kommt man da hin?“ immer virulenter. Und auch wenn wir die Anfrage an den DFN-Verein, sich für die NHR-Gründungsphase einer Geschäftsstelle anzunehmen, nicht auf dem Schirm hatten, so kam sie doch im Nachhinein nicht wirklich überraschend: So häufig ist die Kombination aus technischer Kompetenz, organisatorischer Erfahrung sowie enger Einbindung in die Landschaft bei gleichzeitiger institutioneller Unabhängigkeit und Neutralität nun auch wieder nicht. Schnell war klar, dass ein Ablehnen (etwa via Verstecken hinter vereinspolitische Bedenken – das geht immer) keine Option war, dass sich der DFN-Verein trotz aller Risiken (wenn’s schiefging, würden die vereinten Finger natürlich mit Vehemenz auf uns zeigen, das war klar …) hier einbringen musste. Und dies auf eine unternehmerische Art, die alles andere als frei von Herausforderungen war und durchaus das eine oder andere Mal bei der Obrigkeit ein „So geht das aber nicht!“ auslöste, die allerdings für die Einhaltung von vorgegebenem Ziel und Zeitrahmen unabdingbar war. Schlüssel zum Erfolg waren wie so oft die Menschen: schnell und breit suchen, die richtigen finden, und die dann werkeln lassen. Und so trat das ein, wofür der DFN-Verein ja schon ein bisschen steht (wir wurden ja nicht ohne Grund gefragt): Es funktioniert, und zwar ziemlich gut.

Peter Wenzel-Constabel
Referat Infrastrukturen für die Wissenschaft, Bundesministerium für Bildung und Forschung (BMBF)

Das Besondere am NHR-Verbund ist, dass er für Forschende aus allen deutschen Hochschulen Kapazitäten im Hochleistungsrechnen bereitstellt – bundesweit und unabhängig vom Standort. Durch Aus- und Weiterbildung im Hochleistungsrechnen, durch die Weiterentwicklung des wissenschaftlichen Rechnens trägt das NHR entscheidend dazu bei, die Qualität der deutschen Hochschulforschung zu sichern und den Wissenschaftlerinnen und Wissenschaftlern neue Möglichkeiten in ihrer Forschung zu eröffnen.

Dr. Babett Gläser
Abteilungsleiterin Forschung, Sächsisches Staatsministerium für Wissenschaft, Kultur und Tourismus

Mit neun Hochleistungsrechenzentren in ganz Deutschland stellt der NHR-Verein Forschenden bundesweit Kapazitäten und Kompetenzen zur Verfügung. Die leistungsfähige Infrastruktur bietet Wissenschaftlerinnen und Wissenschaftlern großartige neue Möglichkeiten zur Vernetzung. Aufgrund der großen Bedeutung für die deutsche Wissenschaftslandschaft wird die Förderung des NHR-Verbundes von Bund und allen Ländern gemeinsam getragen. Persönlich freue ich mich, dass auch die Technische Universität Dresden (ZIH) dabei ist.

Nationales Hochleistungsrechnen (NHR) in Deutschland

NHR-CHRONOLOGIE

Januar 2012

Wissenschaftsrat (WR) veröffentlicht Positionspapier „Strategische Weiterentwicklung des Hoch- und Höchstleistungsrechnens in Deutschland“: High Performance Computing (HPC) ist unverzichtbar für die Wettbewerbsfähigkeit Deutschlands, die Forschungsinfrastruktur ist jedoch nicht ausreichend.

April 2015

Wissenschaftsrat setzt Arbeitsgruppe ein und veröffentlicht „Empfehlungen zur Finanzierung des Nationalen Hoch- und Höchstleistungsrechnens in Deutschland“ – als Grundlage für eine langfristig stabile und kosteneffiziente Weiterentwicklung und Finanzierung des Hoch- und Höchstleistungsrechnens.

August 2018

Gemeinsame Wissenschaftskonferenz (GWK) stellt Anfrage beim DFN-Verein – für die Übernahme des Projekts „Einrichtung einer vorläufigen NHR-Geschäftsstelle“. Einen Tag später stimmt der DFN-Vorstand der Aufnahme des Projekts zu.

November 2018

GWK beschließt Abkommen über die gemeinsame Förderung von Forschungsbauten, Großgeräten und des Nationalen Hochleistungsrechnens an Hochschulen (Verabschiedung AV-FGH).

April 2019

Geschäftsstelle des Strategieausschusses für Nationales Hochleistungsrechnen (NHR) nimmt ihre Arbeit auf – betreut vom DFN-Verein, der als einer der zentralen Akteure der nationalen Forschungsinfrastrukturen den Aufbau begleitet. Das gemeinsam vom BMBF und dem DFN-Verein initiierte Projekt hat eine Laufzeit von zwei Jahren.

Mai 2019

GWK setzt den Strategieausschuss ein. Das unabhängige Gremium der GWK hat die Aufgabe, Empfehlungen zu NHR auszusprechen und ist mit acht Wissenschaftler*innen, dem Bund und acht Ländern als Vertretung der GWK besetzt.

Juni 2019

Konstituierende Sitzung des Strategieausschusses in der Geschäftsstelle des DFN-Vereins

September 2019

Der Strategieausschuss verabschiedet ein Ausschreibungskonzept zur Aufnahme von Rechenzentren in die Förderung.

Dezember 2019

Die GWK beschließt das Ausschreibungskonzept.

Januar 2020

Ausschreibung der NHR-Förderung durch die DFG

August 2020

Empfehlung des Strategieausschusses zur Aufnahme von acht Rechenzentren in die Förderung des NHR auf Basis eines wettbewerblichen und wissenschaftsgeleiteten Auswahlverfahrens

November 2020

Mit dem GWK-Beschluss werden die acht empfohlenen Rechenzentren in die Förderung aufgenommen.

Januar 2021

Beginn der Förderung

August 2021

Gründung des NHR-Vereins in Berlin: Die Übernahme der Geschäftsstelle durch den NHR-Verein ist zum 1. Januar 2022 geplant.

Oktober 2021

GWK beschließt die Aufnahme des Konsortiums Süd-West als neunten Partner in die Förderung.

NFDI – ein effizienteres Forschungsdatenmanagement für die Wissenschaft

Nach Jahren der Vorbereitung wurde im Oktober 2020 der Verein Nationale Forschungsdateninfrastruktur (NFDI) e. V. gegründet. Dieser ist mit dem hehren Ziel angetreten, in Deutschland ein Forschungsdatenmanagement mit einheitlichen Standards zu etablieren, um Forschende aus allen Wissenschaftsdisziplinen besser bei ihrer Arbeit zu unterstützen. Welche Herausforderungen es dabei zu meistern gilt, erzählt NFDI-Direktor Prof. Dr. York Sure-Vetter im Interview.

Wozu brauchen wir in Deutschland eine nationale Forschungsdateninfrastruktur?

Wir verfügen in Deutschland über einen gewaltigen, stetig wachsenden Schatz an unterschiedlichsten wissenschaftlichen Daten. Die meisten dieser Daten werden heute nur noch digital erzeugt. Die Wissenschaft und die Wissenschaftsinfrastruktur stehen dabei vor völlig neuen Herausforderungen wie beispielsweise der datenschutzkonformen Nutzung von privaten Gesundheitsdaten oder der hochskalierbaren Nutzung von extrem großen Mengen von Klimadaten.

Zudem ist der Umgang mit Forschungsdaten in den verschiedenen Wissenschaftsdisziplinen heute noch sehr heterogen. Dabei ist die Erkenntnis darüber, welche Chancen und Risiken das Teilen von Daten in einer Disziplin jeweils mit sich bringt, bei vielen Forschenden noch gar nicht angekommen. Das führt beispielsweise dazu, dass ein Laborexperiment für Dritte nicht reproduzierbar ist, oder dass Rohdaten für die Beantwortung neuer Forschungsfragen nicht nachnutzbar sind. Das ist insgesamt sehr ineffizient und auf Dauer gesehen unbefriedigend.

Das Ziel von NFDI ist, ein nachhaltiges Forschungsdatenmanagement mit einheitlichen Standards zu etablieren und in die Breite der Wissenschaftsdisziplinen zu tragen. Dafür müssen Datenbestände systematisch erschlossen, langfristig gesichert und gemäß den FAIR-Prinzipien (Findable, Accessible, Interoperable und Re-usable) über Disziplinen- und Ländergrenzen hinaus zur Verfügung gestellt werden. Dieses Ziel ist nur durch eine interdisziplinäre Zusammenarbeit von allen Wissenschaftsbereichen und Infrastruktureinrichtungen erreichbar.

Wie soll diese Infrastruktur aufgebaut werden und wer hat das Know-how?

Das Besondere an NFDI ist, dass wir einen Ort des Austauschs für alle Wissenschaftsdisziplinen schaffen, an dem sie miteinander das Forschungsdatenmanagement der Zukunft gestalten und dabei ihre unterschiedlichen Kompetenzen und Erfahrungen einbringen.

So besteht jedes Konsortium nicht nur aus Wissenschaftlerinnen und Wissenschaftlern mit ausgeprägter fachlicher Expertise, sondern auch aus Infrastrukturfachleuten mit großer Kompetenz für die

Prof. Dr. York Sure-Vetter: Direktor der Nationalen Forschungsdateninfrastruktur (NFDI) und Professor am Karlsruher Institut für Technologie (KIT)

Forschungsschwerpunkte: Künstliche Intelligenz (KI) und Data Science, Semantic Web, Linked Data, Data and Text Mining, Service Science (Foto: NFDI)

notwendigen Infrastruktur-Komponenten. Wie beim DFN-Verein kennen sich diese mit den Services aus, die für die Wissenschaft benötigt werden. Darüber hinaus bauen wir Kompetenzprofile wie das des neuen Berufsbilds Data Stewart auf. Diese fachliche Dualität ist ein ganz wichtiger Pfeiler bei NFDI und in jedem Konsortium tief verankert: Fachwissenschaft plus Infrastruktur.

Die Services wiederum sollen an bereits bestehende technische Infrastrukturen andocken. Von vorneherein war klar, dass NFDI sich auf der reinen Anwendungsebene bewegt: kein „Blech“, so lautete die Devise bei der Ausarbeitung der Empfehlung für den Aufbau der NFDI – weder finanziert noch aufgebaut oder betrieben. Für diesen Teil sind wir auf starke Partner angewiesen und haben sie teilweise auch schon mit an Bord: Infrastrukturinstitute aus dem außeruniversitären Forschungsbereich, Rechenzentren, Archive und Bibliotheken, die z. B. die Hardware und die Prozesse, um das „Blech“ am Laufen zu halten, betreiben oder die Datensätze sammeln, aufarbeiten und archivieren.

Was ist das Neue an der Idee einer NFDI?

Neu ist der Anspruch, alle Wissenschaftsdisziplinen in Deutschland an einen Tisch zu bringen, um das Forschungsdatenmanagement ganzheitlich zu verbessern. In NFDI sind die einzelnen Fach-Communities darum disziplinabhängig in eigeninitiativ agierenden Konsortien organisiert. Jede hat ihre eigenen Datensätze mit teilweise individuellen Anforderungen wie beispielsweise speziellen Datenformaten. Gleichzeitig gibt es viele generalisierbare Herausforderungen und Lösungsansätze, die jeweils für viele oder sogar für alle gleich sind. In NFDI profitieren alle Wissenschaften davon, dass wir die Herausforderungen gemeinsam meistern und dabei aus verschiedenen Erfahrungen lernen.

Die einzelnen Communities sind auf einem sehr unterschiedlichen Entwicklungsstand. Es war sozusagen eine Art Hausaufgabe für Wissenschaftsdisziplinen, im Rahmen der Antragstellung bei der DFG auch eine Bestandsaufnahme zu machen und sodann zu entscheiden, was der jeweils nächste sinnvolle Schritt für eine Verbesserung im Umgang mit digitalen Forschungsdaten ist. Jede Disziplin hat ihre spezifischen Herausforderungen und demnach unterschiedliche Schritte, die sie in NFDI gehen will. In den Lebenswissenschaften sind ethische Fragen und

Fragen des Datenschutzes besonders wichtig. In den Naturwissenschaften geht es unter anderem darum, Rohdaten aus Laborexperimenten mit Metadaten anzureichern und besser zur Verfügung zu stellen.

Synergien zu nutzen und diesen Schatz an unterschiedlichen Kompetenzen allen zur Verfügung zu stellen, das war ursprünglich der Anspruch des Rats für Informationsinfrastrukturen (RfII), der mit seinem Positionspapier „Leistung aus Vielfalt" den ersten Aufschlag zur NFDI gemacht hat. Konsequent weitergedacht bedeutet dieser Anspruch heute, dass die Communities ihre Schritte nicht allein, sondern

Mehr Raum für Daten: Eröffnung der NFDI-Geschäftsstelle am 15.10.2020 in Karlsruhe (von links nach rechts) Sabine Brünger-Weilandt (FIZ Karlsruhe), Holger Hanselka (KIT), Eva Lübke (NFDI-Direktorat), York Sure-Vetter (NFDI-Direktorat) und Frank Mentrup (Oberbürgermeister Karlsruhe) *Foto: Cynthia Ruf/KIT*

gemeinsam gehen und dabei voneinander lernen und fächerübergreifend zusammenarbeiten.

Wie stellen Sie den Erfahrungsaustausch zwischen den Konsortien sicher? Wie erreichen Sie die fächerübergreifende Zusammenarbeit?

Um den Austausch über die Konsortialgrenzen hinweg zu fördern, bauen wir momentan sogenannte Sektionen auf. Die ersten vier Sektionskonzepte wurden bereits Ende September eingerichtet und haben ihre Arbeit aufgenommen. In den Sektionen treffen sich Personen aus unterschiedlichen Konsortien und diskutieren über ausgewählte Querschnittsthemen. Ein Beispiel ist die Sektion zur Common Infrastructure: Hier arbeiten wir an technischen Lösungen für eine gemeinsame Infrastruktur auf Basis der Anforderungen, die aus den verschiedenen Konsortien gesammelt werden.

Gehören zur Common Infrastructure auch die Basisdienste wie zum Beispiel zur Authentifizierung und Autorisierung?

Basisdienste können aus allen Sektionen kommen. Ihr genanntes Beispiel zur Authentifizierung und Autorisierung passt natürlich sehr gut zur Sektion Common Infrastructure. Ursprünglich wurde die dritte Runde für die Basisdienste geöffnet. Sehr schnell folgte die Erkenntnis, dass eine Vorbereitungsphase notwendig ist, um wichtige Akteure frühzeitig mit einzubeziehen bei der Definition des Vorgehens zur Etablierung von Basisdiensten. So geht es in der Hauptsache darum sicherzustellen, dass der Prozess anforderungsgetrieben ist und daher aus den Reihen der Konsortien und der Sektionen mitgestaltet wird. Weitere Akteure wie beispielsweise der Wissenschaftliche Senat des NFDI-Vereins können unterstützen, indem die strategische Perspektive für Basisdienste vorausgedacht wird.

> „Eine einheitliche Authentifizierung und Autorisierung ermöglicht einen Effizienzgewinn bei der täglichen Arbeit."

Die Querschnittsthemen und zugehörige Dienste sind eben nicht domänenspezifisch, sondern sie werden, vereinfacht gesagt, „von allen" benötigt. Die Bereitstellung einer einheitlichen Authentifizierung und Autorisierung durch ein geeignetes Identitätsmanagement ist ein gutes Beispiel für einen Dienst, der allen Konsortien einen Effizienzgewinn bei der täglichen Arbeit ermöglicht.

Es ist bereits jetzt abzusehen, dass die Finanzausstattung der geförderten Konsortien es nicht hergibt, die strukturell notwendigen Basisdienste aus eigener Kraft nachhaltig zu erbringen. Das wirft einige sehr grundlegende Fragen auf. Insgesamt erfordern Basisdienste zwingend eine langfristige Kalkulation der Entwicklungs- und Wartungsaufwände.

GESCHICHTE

03.05.2016 Der Rat für Informationsinfrastrukturen (RfII) verabschiedet das Papier „Leistung aus Vielfalt“ mit Empfehlungen für die Zukunft des Forschungsdatenmanagements in Deutschland. Darin wird der Aufbau einer Nationalen Forschungsdateninfrastruktur (NFDI) angeraten.

16.11.2018 Die Gemeinsame Wissenschaftskonferenz (GWK) einigt sich darauf, eine NFDI aufzubauen. Bund und Länder sollen dafür bis Ende 2028 Fördermittel bereitstellen.

26.11.2018 Die Bundesregierung und die Regierungen der Länder beschließen den Aufbau und die Förderung einer NFDI. Die Bund-Länder-Vereinbarung umfasst die wesentlichen Eckpunkte zu Zielen und Struktur.

03.05.2019 Die GWK beschließt, das Direktorat der NFDI in Karlsruhe anzusiedeln und die FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur GmbH sowie das Karlsruher Institut für Technologie (KIT) mit den Aufgaben der Gründungsphase zu betrauen. Dies umfasst den Aufbau der Geschäftsstelle und die Überführung der NFDI in eine eigene Rechtspersönlichkeit.

01.10.2020 Die Förderung der neun Konsortien der ersten Runde beginnt. Dazu gehören DataPLANT, GHGA, KonsortSWD, NFDI4BioDiversity, NFDI4Cat, NFDI4Chem, NFDI4Culture, NFDI4Health und NFDI4Ing.

12.10.2020 Bund und Länder gründen den Verein Nationale Forschungsdateninfrastruktur (NFDI) e. V. in Hannover.

02.07.2021 Die GWK beschließt die Förderung weiterer zehn Konsortien in der zweiten Runde. Diese sind BERD@NFDI, DAPHNE4NFDI, FAIRmat, MaRDI, NFDI4DataScience, NFDI4Earth, NFDI4Microbiota, NFDI-MatWerk, PUNCH4NFDI und Text+.

01.10.2021 Die Förderung der zehn Konsortien der zweiten Runde beginnt.

Wo sehen Sie momentan die größten Herausforderungen beim Aufbau der NFDI?

Wir sind ein ganz neuer Verein, uns gibt es erst seit Oktober vergangenen Jahres. Und es ist tatsächlich die Aufbauarbeit auf allen Ebenen, die uns dieses Jahr sehr stark prägt. Neben den benötigten Informationsinfrastrukturen und den entsprechenden Abstimmungsprozessen ist es vor allem der Aufbau der Vereins- und Governance-Strukturen sowie der Geschäftsstelle, mit der wir uns derzeit befassen. Unser jüngstes Erfolgserlebnis ist, dass wir die Konsortialversammlung ins Leben gerufen haben. Als eine der ersten Entscheidungen hat die Konsortialversammlung sodann Mitglieder in den Wissenschaftlichen Senat entsendet, der damit vollständig besetzt ist. Wir befinden uns in der dritten und letzten Ausschreibungsrunde für die Konsortien – ein durchaus kompetitives Verfahren mit hohen Ansprüchen, aber eben auch mit einer langfristigen Förderung von bis zu zehn Jahren.

Bereits integriert in alle Organisations- und Informationsflüsse sind die Konsortien aus der ersten Runde. Die ersten Sektionen über diese Konsortien hinweg wurden bereits geschaffen. Weitere zehn Konsortien, die in diesem Jahr dazu gekommen sind, werden aktuell integriert. Dabei müssen wir die initialen Schritte so gestalten, dass die zweite und später die dritte Runde ihre Themen und Anforderungen einbringen können, sodass wir keine Silos aufmachen. Dieser Integrationsaspekt ist sicherlich eine der wesentlichen Herausforderungen, die wir aktuell adressieren müssen.

> „Der enge Zeitrahmen ist extrem sportlich und eine große Herausforderung für alle Beteiligten.“

Der gesamte NFDI-Prozess ist geprägt von der zeitlichen Überlappung der drei Phasen des Aufbaus, des Wirkens und der Evaluation. Die ersten Ergebnisse können definitionsgemäß erst nach dem Abschluss der Aufbauphase generiert werden: voraussichtlich ab Anfang 2023, wenn alle 30 Konsortien an Bord sind. Wir werden jedoch bereits 2025 durch den Wissenschaftsrat begutachtet. Die Grundlage für diese Begutachtung ist ein Bericht, der 2024 einzureichen ist. Das heißt, dass wir eigentlich schon ab 2023 mit

NFDI IN ZAHLEN

194 Mitglieder

hat der Verein Nationale Forschungsdateninfrastruktur (NFDI) e. V.: z. B. Universitäten, Hochschulen, Forschungseinrichtungen sowie Ministerien (Stand: November 2021).

19 Konsortien

werden von Bund und Ländern gefördert oder haben eine Förderzusage erhalten (Stand: August 2021).
In jedem Konsortium engagieren sich zahlreiche Einrichtungen.

12 Personen

arbeiten in der Geschäftsstelle des Direktorats in Karlsruhe (Stand: November 2021).

30 Fachkonsortien

können im Rahmen von NFDI eine Förderung erhalten.

1 Ziel

vereint alle Vereinsmitglieder und Konsortien: das Forschungsdatenmanagement der Zukunft effektiver gestalten.

den Vorbereitungen der Evaluation beschäftigt sein werden. Dieser enge Zeitrahmen ist extrem sportlich und eine große Herausforderung für alle Beteiligten.

Was treibt Sie persönlich an als Direktor der NFDI?

Es ist eine sinnstiftende Tätigkeit und eine interessante Aufgabe. Da bringe ich mich gerne mit meinen Kompetenzen ein. Ich bin ausgebildeter Wirtschaftsingenieur mit Promotion und Forschungsinteressen in der Informatik, habe ein großes sozialwissenschaftliches Forschungsinfrastruktur-Institut geleitet, war aber auch in der Industrie bei einem großen deutschen IT-Unternehmen tätig.

Das, was mich schon immer am meisten begeistert hat – sozusagen der emotionale Teil –, ist, ganz verschiedene Menschen mit sehr unterschiedlichen Blickwinkeln kennenzulernen. In der NFDI ist das die nächsthöhere Stufe: Mit bis zu 30 verschiedenen Wissenschaftsdisziplinen in engem Austausch zu arbeiten, finde ich sehr bereichernd. Denn es ist spannend mitzuerleben, was gerade in der Wissenschaft passiert und welche Rolle Forschungsdaten dabei spielen. NFDI ist einfach ein cooler Arbeitsplatz!

Wo steht die NFDI in zehn Jahren?

NFDI ist ein lebendiges Netzwerk aus engagierten Partnern, die das gemeinsame Ziel verfolgen, Forschungsdaten gemäß den FAIR-Prinzipien bereitzustellen. Alle Wissenschaftsdisziplinen sowie alle benötigten Infrastruktureinrichtungen bringen sich entlang ihrer Kompetenzen und Leistungsfähigkeiten in den NFDI-Prozess ein. Forschende und Infrastrukturmitarbeitende profitieren von den Chancen, die sich aus einer Kultur des Datenteilens in den verschiedenen Wissenschaftsdisziplinen jeweils ergeben, und sie tragen zur Erkennung und Minimierung von deren Risiken bei.

Die Fragen stellte Maimona Id (DFN-Verein)

Informationen zum NFDI-Verein finden Sie unter:
https://www.nfdi.de

25 Jahre Technikgeschichte: DFN-WiNShuttle

Der kleine Zugang ins große Wissenschaftsnetz – vor 26 Jahren ging der Dienst WiNShuttle in Betrieb. Der DFN-Verein gehörte zu den ersten Anbietern, die einen bundeseinheitlichen Telefonzugang praktisch zum Ortstarif ermöglichten. Insbesondere der Bildungssektor sollte von der Innovation profitieren. Mit WiNShuttle bekamen Schulen, Volkshochschulen, Lehrende und die Schülerschaft die Möglichkeit, rechnergestützte elektronische Kommunikation zu nutzen. An die Anfänge des Dienstes bis hin zu seiner Stilllegung erinnert sich unsere Kollegin Andrea Wardzichowski mit etwas Wehmut.

Text: **Andrea Wardzichowski** (DFN-Verein)

Es war im Herbst 1996, als ich mich zu Beginn meiner beruflichen Laufbahn am Rechenzentrum Universität Stuttgart (RUS) wiederfand: im Projekt „DFN-WiNShuttle“. Der DFN-Verein war mir schon lange ein Begriff und ich hatte die DFN-Mitteilungen auch schon eine Weile bezogen. Geleitet wurde das Projekt von Karin Schauerhammer vom DFN-Verein in Berlin, am RUS betreute uns Barbara Burr. Gesucht wurde eine Person, die Unix (noch nicht wirklich Linux!)-Systemadministrationskenntnisse mitbrachte sowie Geschick an der Hotline, vor allem telefonisch: Es galt, einen Einwahldienst per Modem und ISDN im Forschungsnetz aufzuziehen. Das hieß aber auch: Die von uns angepeilte Zielgruppe hatte noch gar keinen E-Mail- und Web-Zugang und musste zunächst telefonisch angeleitet werden.

Die Technik

Zu diesem Zeitpunkt hatten wir etwa ein Dutzend Einwahlknoten in großen deutschen Städten bzw. Universitätsstandorten in Betrieb. Dies deckte natürlich nur einen Bruchteil der Zielgruppe ab, denn wir müssen uns erinnern: Es wurde noch unterschieden zwischen Orts- und Ferngespräch und es gab einen Zeittakt, nach dem Telefonate abgerechnet wurden. An den Einwahlknoten kamen die Einwahlrouter MAX4000 von Ascend zum Einsatz. Je nach Größe des Ortes mit einer oder zwei S2M-Leitungen, die jeweils 30 Telefonkanäle beinhalteten. Unvergessen der Moment, in dem wir 30 Karten zur Abholung von Telefonbüchern erhielten. ISDN-Karten im Ascend MAX4000 ermöglichten die ISDN-Einwahl, sogar mit zwei Kanälen gleichzeitig.

Wiedererkennungswert garantiert: WiNShuttle bekam ein eigenes Logo.

In den Städten Stuttgart, Köln, München und Berlin stand je ein SUN-Server gleichen Namens. Diese hatten mannigfaltige Aufgaben: das Einliefern und Abholen von E-Mails, ein ausreichendes Platzangebot für Webseiten sowie die Zustellung von E-Mails und News per UUCP, DNS. Wir hatten außerdem die Idee, die Nutzer nach Kfz-Kennzeichen gleichmäßig über diese vier Server zu verteilen.

Die Zielgruppe

Der Dienst DFN-WiNShuttle erhielt seinen Namen von Klaus Ullmann. Er sah in dem Begriff „WiNShuttle“ das Shuttle als „kleinen Zubringer“ zum großen Wissenschaftsnetz. Der Wunsch nach einem solchen Zugang kam damals aus der DFN-Community. Auch seitens des damaligen Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie (BMBF) bestand großes Interesse daran, insbesondere die Schulen ans Internet anzubinden. Ebenso wünschten sich kleine Einrichtungen aus Forschung und Lehre einen Zugang zum Internet, der günstiger war als eine teure Standleitung. Auch Behörden wie das Bundeskartellamt oder der Deutsche Beamtenbund waren sehr interessiert an unserem Angebot. Wir definierten daher als Zielgruppe Schulen, Bibliotheken und Museen sowie Einrichtungen aus Forschung und Lehre, Volkshochschulen und Vereine. Bei den Einzelpersonen wollten wir sowohl Mitarbeitende von

Hochschulen und Forschungseinrichtungen sowie Lehrende und die Schülerschaft ansprechen als auch Wissenschaftsjournalisten und Vereinsmitglieder, z. B. der Gesellschaft für Informatik (GI) und der German Unix User Group (GUUG). Ebenso sollten in geringerem Maße kleine Ingenieurbüros angesprochen werden.

Mail- und Webadressen

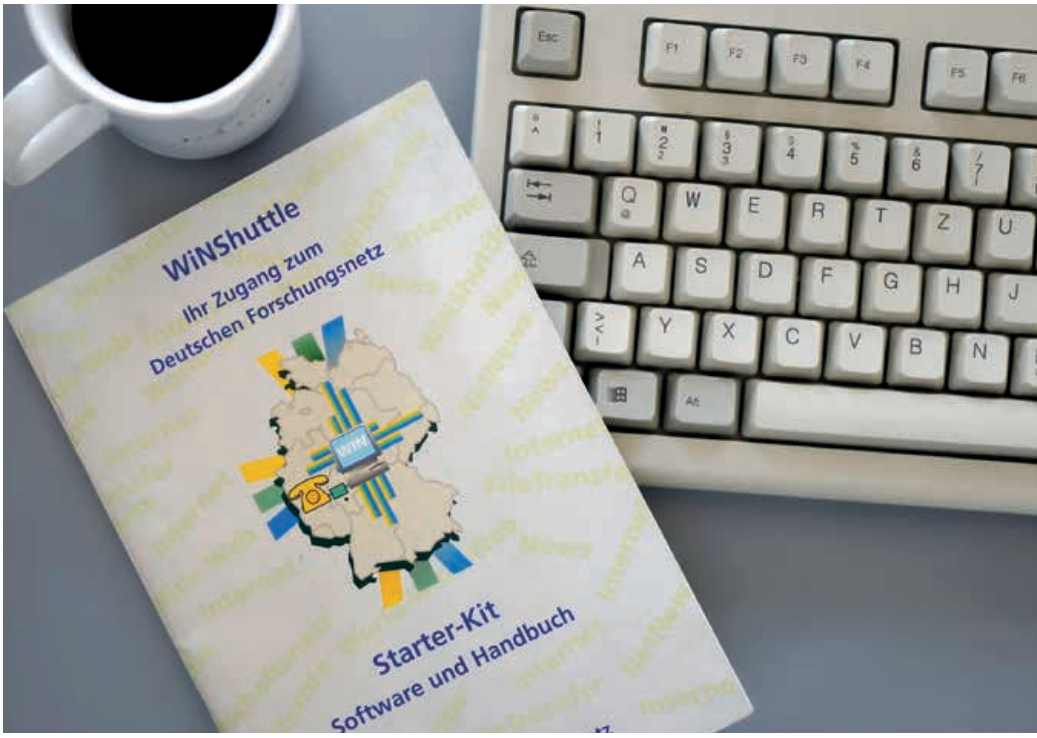
Für die Mail- und Webadressen hatten wir uns etwas „Gutes“ ausgedacht: Während t-online.de und auch aol.com (die seinerzeit schon Internetzugänge anboten) nur einen „flachen“ Namensraum zur Verfügung stellten, bei denen die Adresse für alle Nutzer nach dem @ gleich lautete, wollten wir unseren Nutzern individuellere Mailadressen zukommen lassen. So wollten wir bei häufigen Namenskombinationen eine Durchnummerierung wie bei anderen Anbietern üblich vermeiden.

Der Host-Teil sollte bestehen aus „rechnername.Kfz-Kennzeichen.shuttle.de.“ Den „Rechnernamen“ konnte der Nutzer sich frei aussuchen. Durch die Gliederung in Kfz-Kennzeichen sollten Doppelungen vermieden werden. Passend dazu gab es eine Webadresse in folgender Form: http://www.Kfz.shuttle.de/rechnername/ Eigentlich doch so schön!

Auch das Offene Deutsche Schulnetz (ODS) verfolgte eine ähnliche Strategie beim Aufbau seiner Mailadressen. Dort hieß es: @ schulbezeichnung.Kfz.BL.schule.de. Wir verwalteten auch diese Maildomains für Schulen mit und standen bis zum Schluss mit dem ODS im Mailaustausch. Diese Adressen konnten in Zusammenarbeit mit dem ODS über WiNShuttle genutzt werden.

Die Weiterentwicklung

Bereits im Januar 1998 verließen wir das Projekt am Rechenzentrum der Uni Stuttgart und gründeten in Stuttgart-West zusammen mit dem DFN-NOC einen weiteren Standort der DFN-Geschäftsstelle. Das war ein mutiger Schritt seitens des DFN. Allerdings hätten wir bei einem Weiterbetrieb an der Universität etwa alle fünf Jahre unser Personal auswechseln müssen, weil längere Verträge eine Festanstellung zur Folge gehabt hätten. Der DFN-Verein beschloss damals, dass dies für Bereiche, die letztlich „Betrieb“ machen, keine gute Aussicht sei.



Leicht gemacht mit Starter-Kit: Zum WiNShuttle-Anleitungsheft gab es vier 3,5 Zoll-Disketten mit Treibersoftware für Windows 3.11. *Foto: Nina Bark, DFN*

Mit dem Umzug setzten wir auch unsere steile Lernkurve in Bezug auf „Bürokommunikation“ um. An der Uni hatten wir leichtsinnigerweise den Nutzern auch unsere Telefondurchwahlen verraten. Dies führte natürlich in allen Störungsfällen dazu, dass nicht die beispielsweise mit studentischen Hilfskräften besetzte Hotline-Nummer die Anfragen bekam, sondern regelmäßig Leute, die mit der Behebung der Störung befasst waren. Regel also fortan: Durchwahlen bleiben vertraulich.

Im Dezember 1999 hatten wir bundesweit 56 Einwahlknoten in Betrieb. An einigen Standorten waren wir schon an das Breitband-Wissenschaftsnetz B-WiN angebunden und nicht mehr an das „alte“ X.25-WiN. Drei der Einwahlknoten hatten bereits 90 Einwahlkanäle, vier Knoten 60. Wir überwachten auch sehr genau die Auslastung, um rechtzeitig neue Leitungen bestellen, neue Geräte aufstellen und damit den Bedarf decken zu können.

Und wir erlebten die Öffnung des Telefonmarktes: Es gab neue Anbieter, die bundesweite Einwahlnummern zum Ortstarif zur Verfügung stellten. Im Juni 2000 konnten wir einen bundesweiten Ortstarif in Zusammenarbeit mit der EWE TEL GmbH in Oldenburg anbieten. Das war alles noch sehr kompliziert: Gerade die Schulen, die den Service nutzen wollten, mussten einen kostenfreien Zusatzvertrag mit EWE TEL abschließen, um die Nummer anwählen zu können. Erst später wurde dies deutlich einfacher und unbürokratischer.

Zu diesem Zeitpunkt hatten wir auch längst das Domaingeschäft aufgenommen. Vielen Nutzern waren die drei Punkte in der Mail-

adresse schlicht zu viel. Die Registrierung von .de-Domains übernahmen die DFN-Hostmaster, .com/.net/.org-Domains hingegen mussten die Nutzer selber registrieren, zumindest zu Beginn.

Beworben wurde der Dienst auch auf den Messeauftritten auf der CeBit, mehrfach auf der Didacta und kleineren Messen wie ProNets in Neumünster oder „Schule & Computer“ in Norderstedt. Gerade auf den kleineren Veranstaltungen war auch ich einige Male mit Vorträgen vertreten.

Spezielle Bedürfnisse von Schulen

Gerade bei den Schulen standen wir vor einer nicht zu unterschätzenden Aufgabe: Alle Lehrenden und alle aus der Schülerschaft sollten eine Mailadresse erhalten. In unseren Verträgen waren aber nur drei Adressen vorgesehen, die alle in die gleiche POP3-Mailbox liefen. IMAP gab es als Protokoll schlicht noch nicht. Die für uns eleganteste Lösung war der Einsatz von UUCP (unix-to-unix-copy), eigentlich ein Protokoll zur Übertragung von E-Mails und News aus Mailboxzeiten, als man Rechner noch rein per Telefonleitung vernetzte. Es erfüllte aber einen wichtigen Zweck: Auf einem Linux-Server gab es für jeden Nutzer eine Mailadresse und die E-Mails wurden per UUCP übertragen und in einzelne Postfächer gelegt. Wir hatten auf unserem Mailserver daher praktisch keinen Aufwand mit Hunderten von Mailboxeinträgen. Es gab außerdem zu dieser Zeit auch schon eine Linux-Variante des ODS, die genau das erledigte: den „ODS-Server“, der ehrenamtlich vom inzwischen verstorbenen Helmut Hullen gepflegt wurde.

Allerdings wurden wir dann doch von den Anforderungen eingeholt und mussten in den Verträgen mehrere „POP3-Mailboxen“ anbieten. Dazu gehörten eine Erweiterung unserer Nutzerdatenbank und ein Interface, um Mailadressen zu verwalten. Dieses Mailinterface stammte aus meiner Tastatur, auch wenn ich keine ausgesprochene Softwareenwicklerin war.

Damit einher ging auch ein grundlegender Umbau der Mail-Infrastruktur. Wie alle Einrichtungen mussten wir immer mehr Maßnahmen ergreifen, um E-Mail-Spam abzuwehren. Das setzte die Mailserver so unter Last, dass die Nutzer zum Teil ihre eigenen E-Mails nicht mehr flüssig lesen oder eigene E-Mails zum Versand einliefern konnten. Dies führte dazu, dass wir neue Mailserver installierten, um die Aufgaben zu trennen: reine Server mit Postfächern, auf denen die Nutzer ihre E-Mails versenden konnten und Mail-Eingangsserver, die die E-Mails aus dem Internet auf Spam untersuchten und ggf. ablehnten. Bereits seit Juni 2002 nutzten wir Realtime Blackhole Lists (RBL) zum Ablehnen von offensichtlichen Spam-Mails. Ab Januar 2003 hatten wir dann auch DSL im Angebot. Als Besonderheit konnten wir hier, wie bei Modem- und ISDN-Einwahl auch, die Verbindung mit einer festen IP-Adresse anbieten. In den folgenden Jahren wich dann die Einwahl großflächig dem DSL und wir begannen mit dem Abbau von Einwahlknoten. Inzwischen hieß das Wissenschaftsnetz auch schon „G-WiN“ und einige kleinere Einrichtungen entschieden sich für den Umzug auf einen DSL-Anschluss, um Kosten einzusparen.

Weiterbetrieb und langsame Einstellung verschiedener Dienste

In den folgenden Jahren gab es diverse Änderungen. Die DSL-Angebote wurden um höhere Bandbreiten erweitert. Für eine funktionierende Abfrage bezüglich der Existenz eines Users bei Mail ("user verify") mussten wir einführen, dass alle Nutzer sämtliche ihrer E-Mail-Adressen bei uns bekanntgaben. Bisher hatten wir einfach alles weitergeleitet (Wildcard-Alias). Aber dies war nicht mehr geboten, nachdem immer mehr Spam auf „Buchstabensalatadressen“ ankam. Bei der Benachrichtigung aller Teilnehmer fiel auf, wie schnell auch E-Mail-Adressen von Ansprechpersonen in Nutzerdatenbanken veralten.

Im Juli 2013 wurde der letzte Einwahlstandort für analoge Einwahl/ISDN geschlossen, ebenso der Dienst News/Usenet und die DSL-Zugänge im Dezember 2016.

Die Stilllegung

Auf der 76. Mitgliederversammlung des DFN-Vereins am 5. Juni 2018 wurde beschlossen, den Dienst WiNShuttle endgültig einzustellen. Es herrschte Einigkeit darüber, dass dieser sowie die von ihm erbrachten Services inzwischen überall erhältlich sind und der DFN-Verein sie darum nicht zusätzlich betreiben muss.

Die rechtlichen Vorgaben besagten, dass allen Nutzern eine Kündigung zugestellt werden muss, auch wenn wir inzwischen vermuteten, dass viele ihren Account gar nicht mehr benutzen. Rechtssicherheit bot nur eine Zustellung der Kündigung durch Einwurfeinschreiben. Dieses „Projekt" wurde ab dem Sommer 2018 dann von mir geplant und mit Kolleginnen und Kollegen in Berlin und Stuttgart durchgeführt. Am 30. Juni 2021 wurden die letzten WiNShuttle-Verträge beendet. Viele der aktiven Nutzer bedauerten die Schließung. Einige sorgten sich sogar um unsere Arbeitsplätze, woraufhin wir sie natürlich beruhigen konnten.

Was bleibt

Während der „Shuttle“-Zeit und erst recht, nachdem wir eigene Räumlichkeiten bezogen hatten, übernahm das „Shuttle-Team“ viele andere Aufgaben für den DFN-Verein. Aus dem Shuttle-Betrieb konnten wir viel lernen und mitnehmen, was uns zum Beispiel für den Aufbau des Dienstes MailSupport zugutekam. Auch den Bereich „Serverbetrieb“ entwickelten wir kontinuierlich weiter. Auf diesen Erfahrungsschatz aus 25 Jahren greifen wir täglich zurück. Er steht dem DFN-Verein und seinen Mitgliedern nach wie vor zur Verfügung und wir geben ihn auf allen Ebenen auch zukünftig gerne weiter. ◆

Kurzmeldungen

Alles im Blick: DFN-Teilnehmerportal nun im Regelbetrieb

Nach erfolgreichem Pilotbetrieb steht das Teilnehmerportal des DFN-Vereins nun seit dem 22. November für alle Interessierten bereit. Mit diesem neu geschaffenen Angebot der DFN-Geschäftsstelle besteht für Teilnehmer am Wissenschaftsnetz die Möglichkeit, sich einen kompakten Überblick zu den von ihnen genutzten DFNInternet-Diensten zu verschaffen.

Als Erweiterung zum Pilotsystem wurde im ersten Produktivrelease die Funktion zur selbstständigen Anpassung von Kontaktinformationen für Ansprechpersonen integriert. Weiterhin ist es jetzt möglich, online neue Dienstvereinbarungen für den DFNInternet-Dienst mit allen notwendigen Daten auszufüllen. Ziel ist es, das Up- und Downgrade für vorhandene Dienste sowie die Neubeauftragung auf diesem direkten Weg zu vereinfachen. Weitere Grundfunktionen, die bereits im Pilotsystem für Teilnehmer mit DFNInternet-Diensten verfügbar waren, sind die Darstellung der Stammdaten sowie die Daten zum Rahmenvertrag und zur Dienstvereinbarung DFNInternet inklusive der technischen Parameter der DFNInternet-Dienste. Zum Beispiel können Informationen zur vereinbarten Dienstkategorie, zu betrieblichen Kontaktpersonen, zu den versorgten IP-Netzbereichen sowie zur Teilnehmeranbindung (Übertragungskapazität, verwendete Schnittstellen und Installationsorte) abgerufen werden.

Das DFN-Teilnehmerportal wird kontinuierlich mit dem Ziel erweitert, den Nutzenden eine umfassende Sicht auf alle bereitgestellten DFN-Dienste zu bieten. Auf der Agenda stehen zum Beispiel die Bereitstellung von Messdaten zum übertragenen Datenvolumen, zur Auslastung von Teilnehmeranbindungen sowie zur Verfügbarkeit von Diensten.

Hinweis: Für die Nutzung des Teilnehmerportals ist ein DFNInternet-Dienst auf der Basis eines Rahmenvertrages zur Teilnahme am Deutschen Forschungsnetz und der entsprechenden Dienstvereinbarung Voraussetzung. Dienste aus der Zeit vor 2005, die auf Basis von G-WiN-Anwenderverträgen geschlossen wurden, werden nicht unterstützt. Eine Umstellung auf die aktuellen Verträge ist jedoch mit geringem Aufwand möglich. Das Team von DFNInternet unterstützt Sie dabei gerne. ◆

Das DFN-Teilnehmerportal finden Sie unter:
https://teilnehmerportal.dfn.de
Haben Sie Fragen zum Teilnehmerportal? Dann melden Sie sich gerne per E-Mail unter:
teilnehmerportal@dfn.de

Stabile Außenanbindung: Neue DFN-Peerings im X-WiN

Die Außenanbindungen des Wissenschaftsnetzes X-WiN werden im Austausch mit Partnernetzen strategisch weiterentwickelt. Ziel ist eine optimale Konnektivität und Performance bei gleichzeitig größtmöglicher Kosteneffizienz. So konnten im September zwei weitere direkte Peerings (Private Network Interconnect, PNI) mit Cloud- und Content-Providern etabliert werden. Innerhalb von sechs Tagen nach initialer Kontaktaufnahme wurde ein PNI mit 100 Gbit/s zum Netz der Hetzner Online GmbH geschaltet. Hetzner bietet neben der Miete von dedizierten Servern auch Cloud-Dienste an, die in der Wissenschaftscommunity rege genutzt werden.

Mit der Microsoft Corporation konnte kurz darauf am Kernnetzknoten Frankfurt/Main ebenfalls ein 100 Gbit/s-PNI in Betrieb genommen werden. Dadurch ist es nun möglich, Onlinedienste wie Azure oder Office365 auf direktem Weg zu erreichen. Um die Ausfallsicherheit dieser Verbindung zu erhöhen, wird mit Microsoft aktuell der Aufbau eines redundanten zweiten PNI am Kernnetzknoten in Düsseldorf vorbereitet. ◆

400G kann kommen: DFN setzt auf Flex-Grid-Technologie

Nicht 2G oder 5G, sondern 400G: Im September konnte der DFN das Projekt zur Umsetzung der Flex-Grid-Technologie im Wissenschaftsnetz erfolgreich abschließen. Durch den Einsatz der Flex-Grid-Technologie ist es nun möglich, die bestehenden Glasfaserstrecken im Kernnetz flexibler zu nutzen und erstmals Übertragungsraten von 400 Gbit/s und höher je Verbindung zu realisieren.

In nächtlichen Changes – abgestimmt mit dem Hersteller der Systeme für die Optische Plattform – wurden an 20 der insgesamt 65 Kernnetzknoten Flex-Grid-fähige ROADM (Rekonfigurierbare Optische Add-Drop-Multiplexer) installiert und in Betrieb genommen. Neben dem Einbau der Hardware mussten umfangreiche Upgrades der eingesetzten Soft- und Firmware durchgeführt werden. In einem nächsten Schritt wird auch die IP-Plattform zur Übertragung dieser Bandbreiten fit gemacht. Zur Evaluierung geeigneter Systeme laufen bereits Vorbereitungen. ◆

BELLA – Das Licht am Ende des Kabels

Auf der TICAL2021-Konferenz in Südamerika Ende August feierte das BELLA-Konsortium die erste direkte Datenübertragung zwischen den Forschungsnetzen (NRENs) GÉANT und RedCLARA über das 6000 Kilometer lange transatlantische EllaLink-Unterseekabel, das zwischen Sines in Portugal und Fortaleza in Brasilien verläuft. Damit wurde nach vielen Jahren der Planung und Vorbereitung für die Forschungsnetze und Partnerorganisationen in ganz Europa und Lateinamerika ein Traum Wirklichkeit.

Text: **Jakob Tendel** (DFN-Verein)

Im Schlepptau: Im Januar 2021 geht das Unterseekabel in Madeira, Portugal an Land *Foto: ellalink*

Dieter Suchar, Head of the Information Technology Department ESO

Die ESO untersucht Anwendungsfälle, die mit BELLA erst möglich werden und ganz neue Perspektiven in der wissenschaftlichen Datenübertragung und in den Betriebsprozessen eröffnen. Nachdem wir die Gelegenheit hatten, an einigen Tests teilzunehmen und uns von der Leistungsfähigkeit der BELLA-Infrastruktur überzeugen konnten, freuen wir uns nun auf die Möglichkeit, diese für die ESO-Observatorien in Chile einschließlich des ELT (Extremely Large Telescope) – künftig das größte optische Teleskop der Welt – zu nutzen.

Nachdem das EllaLink-Kabel im Juni auf der Veranstaltung der Europäischen Kommission „Leading the Digital Decade" in Portugal eingeweiht wurde, bot die TICAL2021 die perfekte Bühne, um den Startschuss für die Datenübertragung im Wissenschaftsbereich zu geben. Die freudigen Zuschauer bestanden aus den Mitgliedern der Nutzerkreise, die mit am meisten von der hohen Kapazität des weltweit ersten Unterseekabels zwischen Europa und Lateinamerika profitieren werden.

Wer darf als Erstes?

Ein Forschungsbereich, der unmittelbar von der verbesserten Konnektivität nach Südamerika profitieren wird, ist die europäische Astronomieforschung. Die Hochlagen der Anden mit sprichwörtlich sternklarem Himmel, vor allem in Chile, sind ideale Standorte für Teleskope aller Art. Viele dieser Großanlagen werden von europäischen Forschungsorganisationen wie der Europäischen Südsternwarte (European Southern Observatory, ESO) betrieben: in Chile das Vitacura-Zentrum sowie die drei weltweit einzigartigen Beobachtungsstandorte La Silla, Paranal und Chajnantor. Die Instrumente an den hier genutzten Teleskopen produzieren zunehmend große Datenmengen. Deshalb möchte die ESO für die Datenübertragung von Chile zu ihrem Hauptsitz in Garching bei München – hier befinden sich die wichtigsten wissenschaftlichen und technischen Abteilungen und die Verwaltung der Organisation – seit Langem die Forschungsnetze stärker einbinden. Hinsichtlich dieser Datenübertragung blickt die ESO seit Beginn des Projekts hoffnungsvoll auf BELLA. Sie gehört nun zu den Ersten, die Übertragungstests auf der frisch eingeweihten Strecke durchgeführt haben.

Seit 2005 arbeitet die ESO mit ihrer Community und der Industrie an der Entwicklung eines extrem großen optischen Infrarot-Teleskops. Es handelt sich dabei um ein bodengestütztes Teleskop mit einem 39-Meter-Hauptspiegel – das künftig größte Teleskop für sichtbares und infrarotes Licht weltweit. Das Extremely Large Telescope (ELT) wird außerdem mit einer Reihe hochmoderner Instrumente ausgestattet sein, die ein breites Spektrum wissenschaftlicher Möglichkeiten abdecken können. BELLA wird eine wichtige Rolle dabei spielen, die Massen an Forschungsdaten, die das ELT produzieren wird, auch möglichst effizient zu nutzen.

Große Teleskope wie das ELT haben weltweit die höchste Priorität in der bodengebundenen Astronomie. Sie werden das bestehende astrophysikalische Wissen auf eine ganz neue Ebene bringen, eine tiefere Erforschung unseres Universums ermöglichen und schärfere Blicke auf kosmische Objekte ermöglichen als je zuvor.

Wer steht hinter BELLA?

Für die Umsetzung eines so großen Projekts wie BELLA bedurfte es der Zusammenarbeit verschiedenster Organisationen. Die Finanzierung und Vertragsgestaltung mit EllaLink erfolgten über die europäischen sowie die lateinamerikanischen Forschungsnetze. Von europäischer Seite wurden die finanziellen Mittel durch drei Direktorate der Europäischen Kommission bereitgestellt:

DG-CONNECT (Directorate-General for Communications Networks, Content and Technology) unterstützte den Bau des Unterseekabels, während DG-GROWTH (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs) eine direkte, dauerhafte Verbindung der ESA zum Raumfahrtzentrum Guayana in Auftrag geben konnte. Die Mittel aus beiden Direktoraten wurden für das Projekt BELLA-S verwendet.

DG-DEVCO (Directorate-General for International Cooperation and Development) ermöglichte über das Projekt BELLA-T den Ausbau der terrestrischen Glasfaserinfrastruktur des lateinamerikanischen Forschungsnetzes RedCLARA. Der Ausbau des RedCLARA-Backbone auf Geschwindigkeiten von 100 Gigabit pro Sekunde musste gewährleistet sein, um die nahtlose Anbindung der latein-

Nächste Station Kapverden: Die Anlandung am Strand von Portinho ist der erste Schritt auf dem Weg zu einem Unterseekabelzentrum im mittleren Atlantik *Foto: ellalink*

amerikanischen Forschungsnetze an BELLA zu garantieren.

Die Gesamtfinanzierung des BELLA-Programms beläuft sich auf rund 40 Millionen Euro, davon kommen 25 Millionen Euro von den drei Direktoraten der Europäischen Kommission. Zusätzlich werden 15 Millionen Euro von der Gemeinschaft lateinamerikanischer Forschungsnetze beigetragen.

Vorbereitet und beantragt wurden die BELLA-Projekte durch ein Konsortium aus regionalen Forschungs- und Bildungsnetzen: GÉANT und RedCLARA sowie die nationalen Wissenschaftsnetze von Brasilien, Chile, Kolumbien, Ecuador, Frankreich, Deutschland, Italien, Portugal und Spanien.

Ausblick

Die im EllaLink-Kabel verbaute Technik unterstützt auch zukünftige optische Verfahren zur Datenübertragung und erlaubt so eine sukzessive Steigerung des Datendurchsatzes über die erwarteten 25 Jahre Betriebsdauer. Das theoretische Maximum der Gesamtkapazität des Kabelsystems liegt heute bei etwa 72 Terabit pro Sekunde. Die Forschungsnetze verfügen mit ihrem dauerhaften Nutzungsrecht von circa neun Prozent der Kapazitäten derzeit über theoretisch 6,75 Terabit pro Sekunde.

Neben der Steigerung des Durchsatzes auf dem Unterseekabel laufen ebenfalls Aktivitäten, die Zubringeranschlüsse an beiden Landungspunkten entsprechend auszubauen. Auf der europäischen Seite wird für eine optimale Einbindung in das GÉANT-Netzwerk gesorgt und auf südamerikanischer Seite wird über den gesamten Kontinent an einer Verstärkung der terrestrischen Vernetzung gearbeitet. Dadurch soll neben der Anbindung an das EllaLink-Kabel auch die Vernetzung der Länder untereinander weiter verbessert werden.

Die Netzwerkinfrastruktur für Forschung und Bildung umspannt den gesamten Globus, sie schafft den Zugang zu Inhalten und Ressourcen, verbindet Menschen, ermöglicht neue Erfahrungen und fördert die Zusammenarbeit und das Wachstum interdisziplinärer Gemeinschaften. BELLA ist eine wichtige Ergänzung dieser globalen Infrastruktur und wird vielen Wissenschaftsbereichen, Forschenden und Studierenden Vorteile bringen. Neben der Astronomieforschung werden insbesondere das Erdbeobachtungsprogramm Copernicus sowie gemeinsame Vorhaben in der Klimaforschung und Kooperationen von Hochschulen auf beiden Seiten des Atlantiks stark von BELLA profitieren. ◆

WAS IST BELLA?

BELLA (Building the Europe Link with Latin America) bedient den langfristigen Bedarf der europäischen und lateinamerikanischen Wissenschaftsgemeinschaft an gemeinsamer Interkonnektivität. Der Bedarf soll durch zwei Projekte gedeckt werden. Zum einen über BELLA-S, das der Forschungsnetzgemeinschaft ein dauerhaftes Nutzungsrecht an neun Prozent des Spektrums auf dem Unterseekabel EllaLink sichert und so für zukunftssichere Konnektivität sorgt. EllaLink ist das erste direkte Unterseekabel zwischen Europa und Lateinamerika, das auch für moderne Datenübertragung geeignet ist. Das zweite Projekt ist BELLA-T: Hier geht es um den Ausbau der terrestrischen Glasfaserverbindungen für die lateinamerikanischen Forschungsnetze. Das verschafft den Forschungs- und Bildungsgemeinschaften auf dem gesamten Kontinent die dringend benötigten Hochgeschwindigkeitsverbindungen und stellt sicher, dass die gesamte Region von dem enormen Fortschritt der Konnektivität profitieren wird.

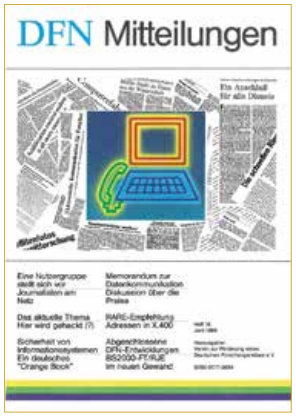
BELLA
Building the Europe Link to Latin America

Eine Auswahl an spannenden Videoclips zum Bau des Kabels sowie weitere Informationen finden Sie unter:
https://ella.link/news/videos/
https://bella-programme.redclara.net/index.php/en/

DFM Mitteilungen I Ausgaben 11 - 25

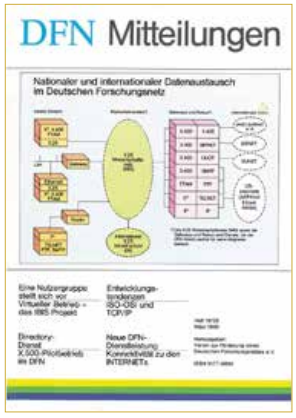
1989

Doppelheft 13/14



17/1989 – X.25
Das X.25-Netz für die Wissenschaft, kurz X.25 WiN, geht an den Start – den Vertrag unterzeichnen Prof. Dr. Eike Jessen und Friedrich Winkelhage für den DFN-Verein und Bundesminister für Post und Telekommunikation Dr. Christian Schwarz-Schilling. Der Bundesminister für Forschung und Technologie, Dr. Heinz Riesenhuber, gratuliert zur erfolgreichen Vertragsunterzeichnung.

Doppelheft 19/20



Doppelheft 22/23

1991

25/1991 – „Dresdner Fenstersprung“
Ein Jahr nach der deutschen Wiedervereinigung, 1991, wird das erste deutsche Wissenschaftsnetz WiN durch ERWiN erweitert. Dadurch bekommen 51 Teilnehmer aus den neuen Bundesländern Zugang. Die TU Dresden gehörte zu den ersten offiziellen Teilnehmern. Ein Jahr zuvor richtete sie mittels Modem und HDN ein Provisorium zum X.25-WiN ein: der Auslöser für den berühmten „Dresdner Fenstersprung“.

DFM Mitteilungen | Ausgaben 26 - 40

Doppelheft 26/27

1993

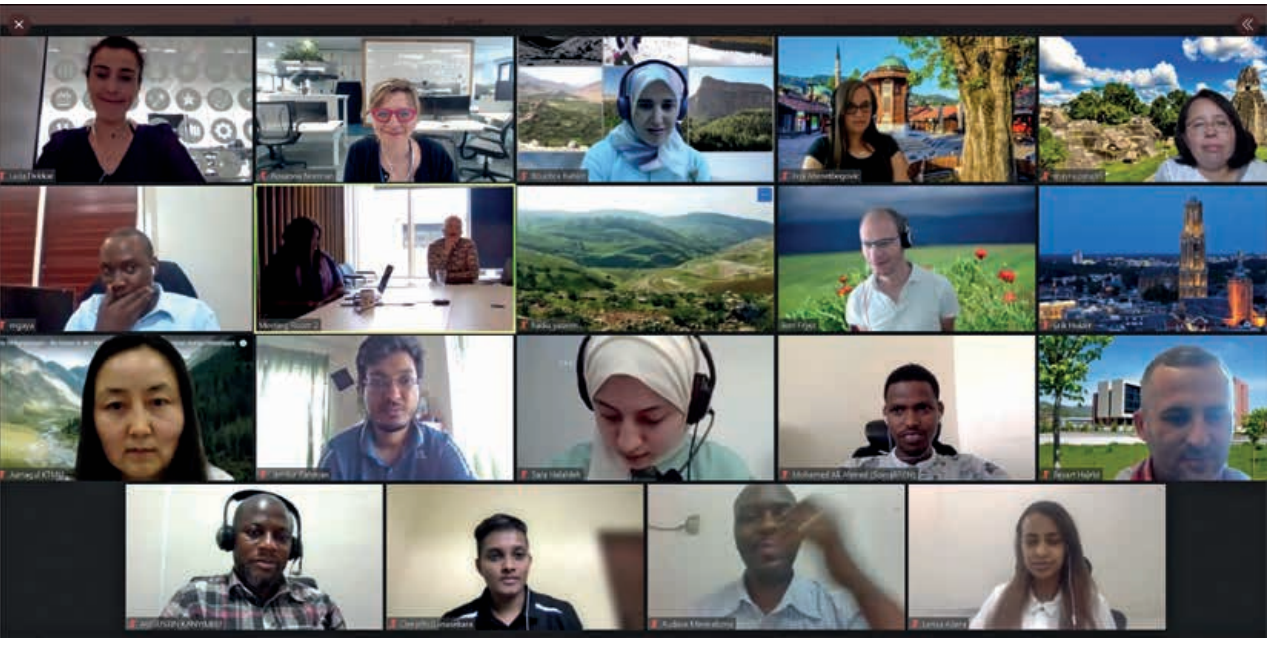
1995

35/1994 – DANTE – Europa rückt näher zusammen
Am 25. März 1994 fand in Amsterdam die offizielle Gründung des ersten europäischen Forschungsnetzes DANTE Ltd. statt. Damit wurde die erste länderübergreifende Infrastruktur für wissenschaftliche Datenkommunikation geschaffen: ein Meilenstein für die europäische Forschungsgemeinschaft. Heute sorgt der Nachfolger GÉANT mit bis zu 300 Gbit/s für Konnektivität zu den weltweiten Forschungsnetzen.

Have you heard of the GÉANT Emerging NREN Programme?

The GÉANT Emerging NREN Programme (ENP) has been taking place alongside TNC, GÉANT's flagship yearly conference, since 2018. In its consecutive editions the programme has aimed to integrate individuals from emerging NRENs from around the globe into the TNC community and create further synergies and connections at different organisational levels between European and international NRENs. This is how we achieve it.

Text: **Leila Dekkar** (GÉANT Association)



Strengthen and enrich the NREN community: the ENP participants 2021 enjoy a tailor-made programme at TNC and have the opportunity to build new relationships.

TNC attendance

TNC is the largest Research & Education networking conference which aims to present participants with a unique overview of the latest developments in research networking, both in the technical field and in the area of application and management. Every year TNC brings together a wide cross section of specialists from a variety of roles in the areas of networking, Trust & Identity, access management and more from all NRENs, universities, research organisations and institutions, and industry.

First and foremost, the ENP programme gives access to TNC with the support of EU-funded projects such as GN4-3, CAREN3, EaPConnect, AfricaConnect3 and Asi@Connect.

The purpose of the programme is to bring to the conference personnel from NRENs that would not be financially able to participate otherwise, focusing particularly on engineering and technical staff.

Dedicated ENP programme coordinated with the conference's local NREN host

ENP participants also enjoy a tailor-made programme that includes dedicated sessions with the TNC host:

- In 2018 participants took part in a walking tour following the physical route of the Uninett (Norwegian NREN at the time) network's route through Trondheim, Norway, led by a Uninett engineer. This was followed by a visit to the NREN's offices, with technical talks and presentations as well as a visit to the Network Operations Centre.
- In 2019, participants were hosted by EENet of HITSA in Estonia. In addition to attending presentations about the Estonian NRENand Telia, the leading telecom operator in the region, participants visited a High Performance Computing farm, the TalTech Innovation and Business Centre Mektory (three floors of start-ups, laboratories and hi-tech showrooms), and the e-Estonia Briefing Centre.
- In 2021 the hosting went virtual and Jisc, the UK NREN, rose to the occasion by introducing participants to the Janet network, their cloud solutions and their cyber security services.

Every year, based on the participants' profile, the programme also includes an introduction to TNC for first timers comprising a meeting with the GÉANT CEO and other thematic sessions with GÉANT community members.

Integration with the International NREN community

In order to make the ENP more valuable, all participants are paired with GÉANT community members based on common professional backgrounds, in order to facilitate informal dialogue between individuals sharing the same interests.

The objective of this pairing experience is to make TNC participation more relevant and impactful for the ENP candidates by providing the opportunity to strengthen and enrich the NREN community and build new relationships. Participants from the GÉANT community also greatly benefit from the exchange as it enhances their understanding of NRENs around the world by listening to different perspectives on needs and challenges.

Lightening talk submissions

ENP participants are also encouraged to submit Lightning Talk proposals. In the past three TNC conferences, 10 ENP participants were selected in this very competitive process and delivered very interesting, rich and diverse presentations with titles such as: Digital Crop-Disease Surveillance Systems in sub-Saharan Africa to Student Information systems, Face Recognition - Internet of Things Fused System for Criminal Recognition and Location Identification in West Africa or a student information system with integrated management software Cocktail in Madagascar.

What is the ENP participant profile?

Each year NRENs and RRENs from around the world are invited to nominate representatives to take part in the programme. We encourage the participation of young engineers, NREN staff members or researchers who are part of the community but are not usually able to attend conferences and would benefit from the knowledge exchange. We also strongly promote diversity among participants, for instance by encouraging applications from women wherever possible.

In just three editions the programme has reached 54 participants from 32 different countries and territories: Albania, Armenia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Belarus, Benin, Bhutan, Burundi, Cuba, Cyprus, Democratic Republic of the Congo, Ethiopia, Georgia, Guatemala, Honduras, Jordan, *Kosovo, Kyrgyzstan, Macedonia, Madagascar, Malawi, Morocco, Mozambique, Montenegro, Myanmar, Nigeria, Somalia, Sri Lanka, Tajikistan, Tanzania and Ukraine!

ENP 2021: fully online

At the beginning of June 2021, prior to TNC21, ENP went fully online and was very well attended with 17 participants from 15 countries.

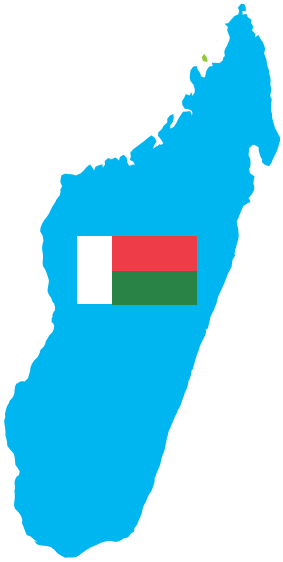
The programme kicked off with an informal get together with Erik Huizer, GÉANT CEO, where participants had the opportunity to introduce themselves showing photos of their most loved places in their country and to take part in a Q&A session. This session was followed by an introduction to TNC21 by the conference organisers.

A subsequent meeting was hosted by Jisc where the UK NREN provided a tailored comprehensive overview of its services and activities. In addition, a thematic session on NREN services and innovation was delivered by Klaas Wierenga, GÉANT CITO.

All participants also took part in TNC21, supported by dedicated check-in coffee sessions, and morning sessions scheduled for each day of the conference to introduce the programme for that day. In addition, this year two of the participants were selected for the very popular Lightning Talks session. ◆

Starke Partner weltweit

Konnektivität fördern, Zukunft gestalten, Herausforderungen gemeinsam meistern: Nationale Forschungsnetze rund um den Globus betreiben leistungsfähige Infrastrukturen für Wissenschaft, Forschung und Lehre. Ein Blick in die Welt der NREN-Community.



i RENALA – Research and Education Network for Academic and Learning Activities

As one of the emerging NRENs in the global community of national research and education networks, i RENALA has the major goal of vigorously advancing the digitalisation of the research and education landscape in Madagascar. Dedicated to its missions, i RENALA with passion is overcoming numerous challenges and calls for further national and international support.

Text: **Harinaina R. Ravelomanantsoa** (i RENALA)

The Malagasy NREN was created in June 2012 under the form of a non-profit association, for an indefinite period and independent of all religious or political affiliation. It starts with an initial investment amounting to 13M euros from the following donors: Afnic (French Internet Domain Name Registry), CIRAD (French Agricultural Research Centre for International Development), Coopération Française, IRD (Institute of Research for Development), MESupReS, MNDPT and RENATER, the national research and education network in France.

Today i RENALA has 29 members including 24 connected to the network. In its missions, i RENALA manages the IRU (Indefeasible Rights of Use) capacity purchased for 25 years and provided by the internet provider TELMA (Telecom Malagasy SA). To ensure its functioning (human and technical resources), NREN collects annual fees from its members. Its different activities bring i RENALA to work in close cooperation with technical and financial partners and provide a collection of shared services, applications and resources dedicated to benefiting the Malagasy higher education and scientific research community.

Infrastructure

At its launch i RENALA had a dedicated capacity of 1 STM1 (Synchronous Trans-

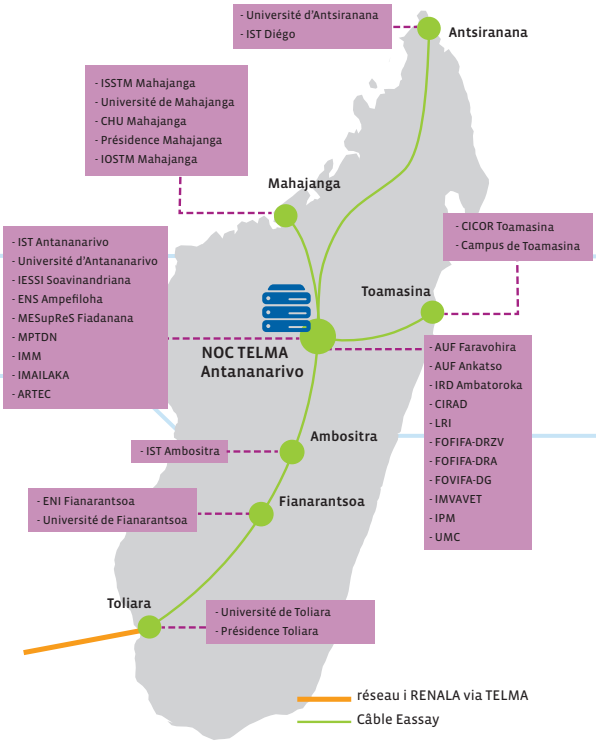


Image 1 - i RENALA: national infrastructure/ Source: i RENALA

port Module) – that is 155Mbit. In 2015, the Ministry of Higher Education and Scientific Research, MESupReS, purchased a second STM1 to meet the demand of the national students. In 2019, a new agreement was signed between MESupReS and TELMA to increase NREN's bit rate. In 2021, i RENALA therefore possessed, through the operator TELMA, a dedicated international output of 7 STM1 (7 x 155Mbit) arriving in Paris. This capacity is distributed between NREN members in accordance with the needs expressed.

Internationally, i RENALA is located in Antananarivo, where its NOC (Network Operations Center) and its offices are found and it possesses three dedicated national STM1 (3 x 155 Mbit).

i RENALA servers are distributed between the NOC installed on its premises and the NOC installed at TELMA.

Services

In order to reduce financial costs, i RENALA shares the services offered with the members, while catering for the specificities of their needs.

The services provided by i RENALA are classed into four categories:

- cross-cutting (accommodation,cooperation, security, connectivity),
- those specific to administration (university management),
- those dedicated to teachers and students (access to libraries of online university resources and connection to an educational platform) and
- those dedicated to researchers (portal of dedicated services on access to global scientific information, research news such as symposia, conferences, lectures, online publications, calls for bids for projects, scholarships, partnerships,etc.).

Servers		Resources	Capacity	Use (%)	Use and Comments
TELMA NOC	**Dell (ESXi)**	vCPU	32	50	i RENALA Services
		RAM	96 GB	94	Alert notifications on an ESX
		Disk	18 TB	83	Errors since 2016
	IBM	CPU	4	60	i RENALA Services
		RAM	20 GB	73	
		Disk	500 GB	70	
	Dell	CPU	4	65	Backups
		RAM	4 GB	40	
		Disk	146 GB + 1.8 TB	81	
	Dell	CPU	4	65	Dedicated for the PGI Cocktail (DataBase & WebOject)
		RAM	4 GB	40	
		Disk	146 GB + 1.8 TB	81	
	Dell	CPU	24	10	
		RAM	32 GB	2	
		Disk	1.7 TB	16	
i RENALA NOC	**Hewlett Packard**	CPU	16	22	i RENALA Services
		RAM	62.78 GB	63	
		Disk	3.62 TB	34	

Table 1 - Technical and statistical resources

Use of services (%)	
Non-connected members	17.24
Domain name	55.17
Website	37.93
Email service	34.48
LDAP	10.34
Moodle	13.79
Digital Work Environment - DWE	3.45
Nextcloud	3.45
Public IPs	68.97
Jabber	44.83
BigBlueButton	6.90
146 GB + 1.8 TB	81
24	10
32 GB	2
1.7 TB	16
16	22
62.78 GB	63
3.62 TB	34

Table 2 - Rate of use of cross-cutting services

Notable Projects

Among i RENALA's missions is the support for university institutions in the switch to the LMD (Licence - Master - Doctorat) system. As such, in 2014, in partnership with AUF-DROI (French-speaking University Agency - Indian Ocean Regional Directorate), NREN launched deployment of the PGI Cocktail (Integrated Management Software) in the university institutions that had agreed to participate in the project, also called "pilot institutions".

Raising awareness amongst members of the reasons for the existence of the Malagasy NREN is a priority for i RENALA. Because since the switch to digital technology is still meeting resistance in the face of change, i RENALA's services are currently not widely used.

Support the Malagasy higher education and scientific research community with their work: Project Manager Harinaina R. Ravelomanantsoa (sitting) and the Operational Unit of i RENALA

With this purpose, since 2017, the "i RENALA-Tour" project has been launched. This project brings the operational team to annually meet the members (managers, teachers, researchers, administrative staff and students) to present the services, benefits and operation of i RENALA, as well as talk with the different actors of institutions to get to know their needs and expectations.

I RENALA FOUNDING MEMBERS:

Two Ministries: Ministry of Higher Education and Scientific Research (MESupReS - Ministère de l'Enseignement Supérieur et de la Recherche Scientifique)
Ministry of Digital Development, Digital Transformation, Post Offices and Telecommunications (MNDPT - Ministère du développement Numérique, de la transformation Digitale, des Postes et des Télécommunications)
Six public Universities, three IST (Higher Institutes of Technology), two private institutions and eight Malagasy research centres including those located in Madagascar (CIRAD, IRD, Pasteur Institute).

In order to ensure good management of the networks of member institutions, i RENALA, AUF-DROI and Coopération Française signed a tri-partite agreement that launches the organisation of several annual meetings of the heads of the members' networks: "InfoSup". The purposes of this event are to homogenise the skills of each engineer or technician in the management of a university and research website and share the difficulties encountered and experiences.

eduroam offers secure wireless access to the Internet to staff and students of the higher education and research community during their travels. Users of a member establishment of the project will then have this access in all other member establishments by using their regular password. Currently, only the i RENALA operational unit benefits from it, with the deployment to member institutions being underway.

MGIX or "Madagascar Global Internet eXchange" is the first Malagasy Internet point of exchange. Since its launch in 2016, it has amongst its members: GOTICOM (Group of Information and Communications Technology Operators), i RENALA, ISOC Madagascar (Internet Society Madagascar Chapter), NIC-MG (Network Information Center Madagascar, the Malagasy registrar) and the 4 national telecommunications operators (Airtel Madagascar, Gulfsat Madagascar, Orange Madagascar, Telecom Malagasy SA - TELMA). The financial support and donations of the members and different partners (Afnic, AFRINIC [Regional Internet Registry], Coopération Française, ISOC, MNDPT, NIC-MG, PCH - Packet Clearing House, Union Africaine) has allowed MGIX to quickly become operational. In order to ensure a neutral and effective functioning, the administrative and technical management was entrusted to i RENALA.

The objectives of MGIX, amongst others, is to facilitate the data exchanges and transfers, and communications and transactions over the Internet, as well as all operations contributing to them and to make common services available that are necessary for per-

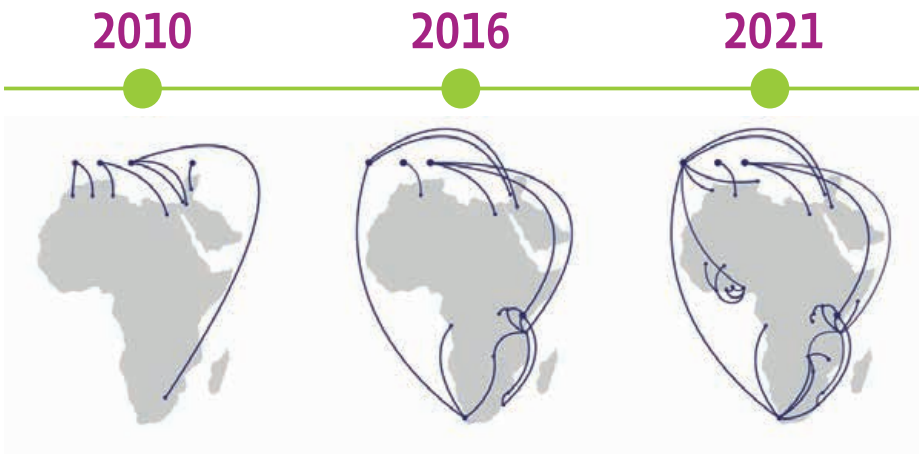


Image 2 - Evolution of the state of connectivity and development of RE in Africa/Source: European Union

forming this project. The interconnection to MGIX allows the networks of professionals, such as research communities, institutions and Internet providers or operators, to exchange traffic, without transit and without passing through transnational or international infrastructures, on the basis of express peering agreements that they establish amongst themselves.

Ubuntunet Alliance & Africaconnect3

Opening up to the world of higher education and scientific research is part of i RENALA's guidelines. Thus, in 2012, the Malagasy NREN became the 14th member of UbuntuNet Alliance, a regional network of Southern and Eastern Africa. Since then, i RENALA has participated in RREN meetings and events.

In 2019 i RENALA hosted UbuntuNet-Connect, the annual flagship conference of UbuntuNet Alliance under the theme: NRENs: "Facilitating Collaboration in the Digital Space." This conference enabled all Eastern and Southern African NRENs and international stakeholders to meet face to face and discuss top priorities innovations and challenges in the region.

In 2019, UbuntuNet Alliance launched AfricaConnect3: it is a four-year Pan-African project co-funded by the European Commission and the national research and education networks of Africa, who are also the beneficiaries of it. The previous AfricaConnect projects established regional data communication networks dedicated to research and education in Africa. AfricaConnect3 aims to consolidate the results of the previous projects and expand the scope of activities to release the potential of education and research in order to strengthen the development of human capital in Africa due to access to infrastructure and digital technologies. With the financial support of Coopération Française and a promise of participation from the Malagasy State through MESupReS, i RENALA has been able to integrate the project.

Conclusion

Although the concepts of sharing services and skills are in the discussions, they are still not an integral part of the common functioning within the university institutions and research centres. Despite the support of some members and their partners, i RENALA is struggling to get up to speed.

With the objective of opening internationally, connecting i RENALA to the UbuntuNet Alliance, GÉANT and world-wide research and education communities remains highly relevant. Works were scheduled to begin in the first quarter of 2019 with the support of MNDPT and MESupReS, as well as the different financial partners but, due to unforeseen circumstances, they were postponed until 2021.

Meanwhile, i RENALA continues to ensure the continuity of the LMD system, ensure its technical and administrative efficiency and invest in national and international projects related to digital development.

Today, the Malagasy NREN is unfortunately facing financial difficulties that do not allow it to renew its equipment and continue it's growth. Nevertheless, i RENALA remains strongly committed to its mandate and is really keen to investigate further international support and collaborations. ◆

REFERENCES

1. https://www.irenala.edu.mg/
2. https://ubuntunet.net/
3. https://europa.eu/european-union/index_fr
4. https://eduroam.org/
5. https://www.mgix.mg/
6. https://africaconnect2.net/
7. https://africaconnect3.net/

Quantennetze – zwischen Realität und Zukunft

Reine Zukunftsmusik sind sie schon längst nicht mehr, aber meistenteils in experimentellem Zustand – die Quantennetze. Unser Autor Dr. Peter Kaufmann und unsere Autorin Dr. Susanne Naegele-Jackson begeben sich erneut in die Welt der Qubits und erklären, welche Strukturen, Netzkomponenten und Geräte notwendig sind und warum gerade Heterogenität im Bereich der Quantennetzarchitektur eine große Rolle spielt.

Text: **Peter Kaufmann** (DFN-Verein), **Susanne Naegele-Jackson** (Friedrich-Alexander-Universität Erlangen-Nürnberg)

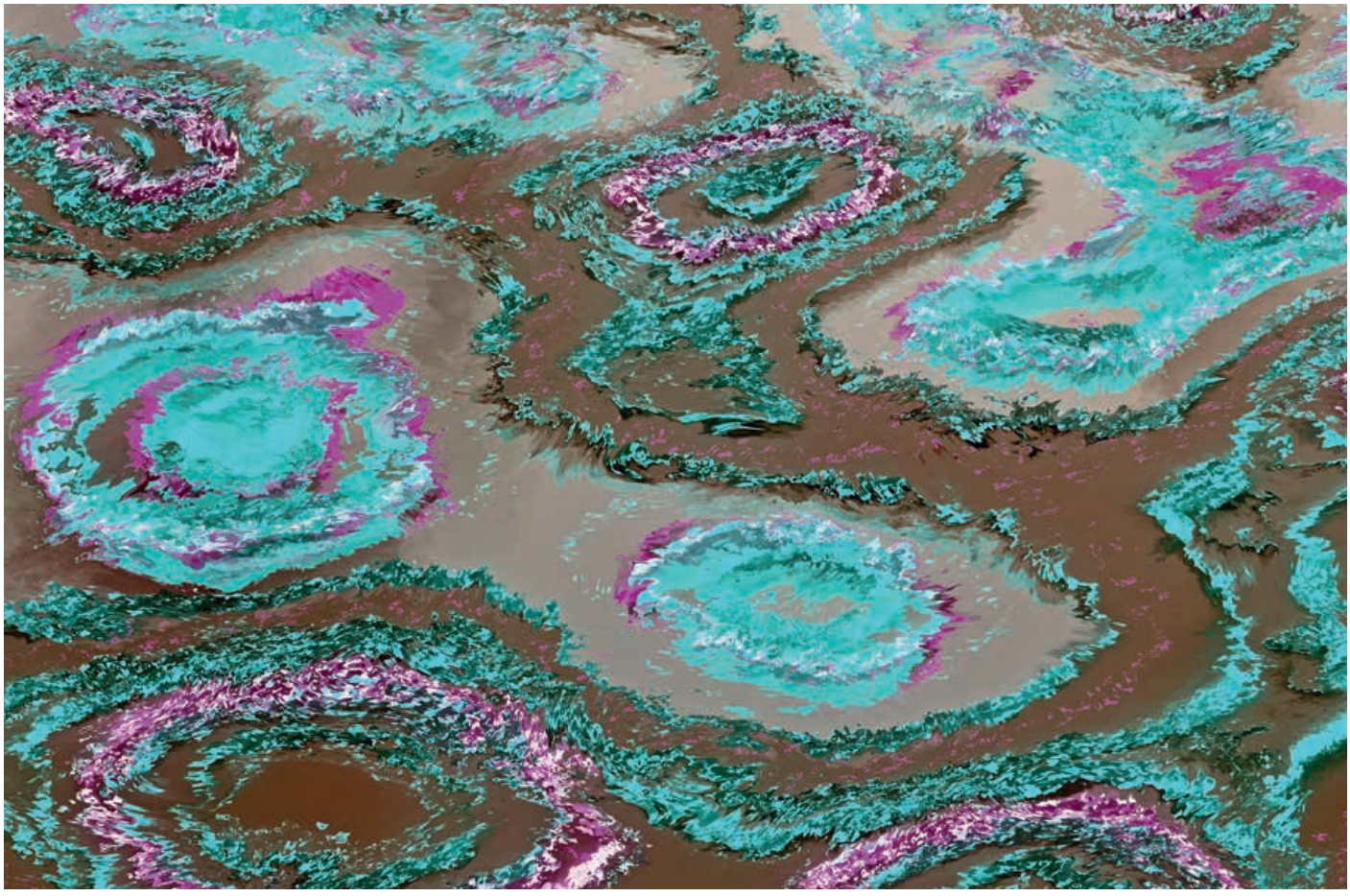


Foto: ludariimago/adobe-Stock

Warum eigentlich Quantennetze?

Ein Quantennetz muss Quantenanwendungen unterstützen, also Qubits (einzeln oder verschränkt) übertragen. Dafür braucht es eine bestimmte Struktur sowie neue Netzkomponenten, sogenannte Quanten-Devices, die die Quanteneffekte behandeln können.

Die besonderen Treiber der Quantennetzarchitektur werden die recht unterschiedlichen Quantenanwendungen sein. Die Aussage scheint trivial zu sein, aber darin versteckt sich ein wichtiger Unterschied zwischen klassischen Netzen und Quantennetzen. Quantendatenübertragung ist nämlich häufig nicht das zentrale oder alleinige Ziel eines Quantennetzes, sondern oft nur eine Komponente einer übergreifenden Quantenanwendung.

Beispielsweise zielen Anwendungen für den Aufbau der besonders sicheren Schlüsselübertragung (QKD – Quantum-Key-Distribution) auf die Nutzung der Bell-Paare ab, dabei werden jedoch keine weiteren Quanteninhalte transportiert. Für Anwendungen aus dem Bereich der Quantensensortechnik (zum Beispiel in der Medizin oder Geologie) oder für die Kopplung von Quantencomputern werden dagegen auch Quantennutzinformationen übertragen. Der Bedarf, Quantenfragmente zu übertragen, wird also in den Anwendungen sehr unterschiedlich sein. Dadurch werden auch die Anforderungen daran, wie effizient die Verteilung der Quanteninformation sein muss, von den Anwendungen abhängen. Die Effizienz, die in klassischen Netzen kaum noch einen Gedanken wert ist, ist in Quantennetzen von höchster Bedeutung: Alle Quantenzustände zerfallen nämlich sehr schnell (meistens in deutlich weniger als einer Sekunde), entweder inhärent oder verstärkt durch äußere Einflüsse. Deshalb spielt die Wiederholungsrate für die Erzeugung von Quantenzuständen wie zur Erzeugung von Bell-Paaren und die Güte beziehungsweise Qualität (Fidelity) der am Ziel ankommenden Quanteninformationen eine zentrale, aber auch anwendungsabhängige Rolle. Nicht alle Anwendungen bedürfen der gleichen Qualität von Quantenzuständen im Zielbereich, so können Sicherheit und Sensortechnik zum Beispiel jeweils unterschiedliche Anforderungen an Güte und Qualität haben.

Technische Anforderungen und Komponenten

Die zentralen technischen Anforderungen an ein Quantennetz sind die Erzeugung und der Transport von Qubits und deren Verschränkungen. Die dafür notwendigen technischen Komponenten sind oft noch in der Frühphase der Entwicklung, es fehlen aktuell unter anderem noch ausgereifte Quanten-Repeater. Hinzu kommt, dass Quantenzustände durch physikalisch sehr verschiedene Umgebungen (Photonen, Elektronen, Atome etc.) beschrieben werden können. Dadurch existiert eine große Vielfalt an Hardware und es werden Gateways zwischen diesen Welten erforderlich. Dazu gehört auch der Wechsel zwischen Transport und Speicherung. Bei der Kommunikation über Glasfasern oder in der Atmosphäre bzw. im Weltraum werden Quanten-Photonen-Zustände verwendet, während für die zeitweise lokale Speicherung auf stationäre „Quanten-Atome“ oder Ähnliches zurückgegriffen werden muss (Photonen bewegen sich stets mit Lichtgeschwindigkeit).

> Ein Netzwerkarchitekturentwurf muss für zukünftige Hardwareentwicklungen offen sein.

Diese Heterogenität ist gerade für die sich entwickelnde Quantenwelt von außerordentlicher Wichtigkeit – auch, weil vieles noch unklar und experimentell ist. Daher muss ein Entwurf für eine Netzarchitektur offen sein für zukünftige Hardwareentwicklungen. QKD läuft beispielsweise in vielen Testumgebungen im Metropolenbereich bisher ohne Quanten-Repeater und kann daher nicht ohne Weiteres als Basis für andere Anwendungen dienen, die erst mit Quanten-Repeatern wirksam arbeiten können. Immerhin könnten nach bisherigen Erfahrungen klassische Datenkanäle und Quantendatenkanäle in einigen Fällen durchaus nebeneinander koexistieren, also auf der gleichen Glasfaser laufen.

Bestandteile eines Quantennetzes

Quanten-Devices können je nach den funktionalen Quantenanforderungen sehr verschieden aufgebaut sein. So gehören ein Quantencomputer (als Endgerät) ebenso wie ein Quanten-

MEHR INFORMATIONEN

Einen Artikel über die Welt der Qubits finden Sie in Ausgabe 99 der DFN-Mitteilungen ab Seite 22. Er behandelt die Entwicklungspotenziale von Quantencomputern und Quantenverschlüsselungen, gibt einen Überblick über Forschungsprogramme im Bereich Quantentechnologie und fasst einige physikalisch-technische Besonderheiten der Quantentechnologie zusammen.

GERÄTE IN EINEM QUANTENNETZ

Quanten-Router/Quanten-Repeater
Bei einem Quanten-Router handelt es sich um einen Quanten-Repeater mit einer Control-Plane. Er nimmt am gesamten Netzmanagement teil und trifft Entscheidungen darüber, für welche Qubits das Entanglement Swapping zur Erzeugung von E2E-Paaren durchgeführt wird.

Automatischer Quantenknoten
Das ist ein Quanten-Repeater ohne Netzmanagement-Funktionen. Für die lang-reichweitige Verkettung werden viele solcher automatischen Quantenknoten benötigt.

Endknoten
In einem Quantennetz müssen Endknoten verschränkte Paare empfangen und bearbeiten können. Sie müssen nicht unbedingt Entanglement-Swapping durchführen (sind also keine Quanten-Repeater). Endknoten müssen auch nicht unbedingt ein Quanten-Memory besitzen, da manche Anwendungen die Messung der Qubits sofort bei Empfang durchführen und die Ergebnisse unmittelbar in die klassische Umgebung hineinreichen können.

Non-Quanten-Knoten
Nicht alle Knoten in einem Quantennetz benötigen eine Quanten-Data-Plane. Ein Non-Quanten-Knoten kann sich auf rein klassische Aufgaben beschränken, obwohl er Teil des Quantennetzes ist.

Linktypen
Ein Quanten-Link verbindet zwei Quanten-Repeater und kann zur Erzeugung eines verschränkten Paares zwischen ihnen verwendet werden. Er kann zusätzlich auch klassische Kanäle bedienen. Ein klassischer Link verbindet zwei Knoten, die klassischen Netzverkehr transportieren können.

Und schließlich gehört die Vielfalt der Grundkomponenten, Laserquellen, Detektoren etc. zu den notwendigen Quanten-Devices, die die Qubits und ihre Verschränkungen in ihren verschiedenen technisch-physikalischen Darstellungen (Photonen, Elektronen, Atome …) erzeugen und detektieren können.

Repeater oder die technische Umgebung für die Erzeugung und Verteilung von verschränkten Qubits zu den Quanten-Devices.

Aufgrund ihres großen Funktionsumfangs bilden Quanten-Repeater den Kern eines Quantennetzes. Zu ihren Aufgaben gehören insbesondere das Erzeugen einer Link-lokalen Verschränkung zwischen Nachbarknoten, das Erweitern der Verschränkung von Link-lokalen Paaren zu lang-reichweitigen E2E-Paaren mittels Entanglement Swapping (siehe Seite 38), die Teilnahme am Netzmanagement (Routing etc.), sowie die Durchführung von Distillationen beziehungsweise Extraktionen zur Verbesserung der Fidelity der erzeugten Qubit-Paare.

Einfaches Management und Monitoring

Die fundamentale Einheit des Quantennetzes, das Qubit, kann nicht einfach kontrolliert, gemessen oder untersucht werden – es würde sofort zerstört werden (No-Cloning-Theorem). Daraus resultieren besondere Herausforderungen für die Entwicklung von Management- und Monitoring-Werkzeugen für Quantennetze. Voraussichtlich kann hier in erster Linie auf klassische Control- und Managementwerkzeuge mit besonderen Anpassungen zurückgegriffen werden wie beispielsweise SDN-Konzepte.

Darstellung eines Quantennetzes

Eine Anwendung auf zwei Endknoten (hier vereinfacht: ohne Zwischenknoten) benötigt verschränkte Paare, welche vom Quantennetz erzeugt werden müssen (siehe Abbildung 1). Beide Endknoten müssen dafür jeweils einen Kommunikationsendpunkt eröffnen – eine Art Quanten-Socket, den das Netz zur Identifizierung der Quantenverbindung nutzt. Beide Endknoten nutzen für den Verbindungsaufbau klassische Netzkomponenten. Wenn das Quantennetz die Anforderung bekommt, E2E-verschränkte Paare zu erzeugen, werden klassische Kanäle sowohl für den Verbindungsaufbau als auch zur Erfüllung der Ressourcenanforderungen verwendet.

Klassische Transportkanäle können einerseits sehr eng mit den Quantenkanälen verwoben sein, beispielsweise für den Transport zweier klassischer Bits bei einer Quantenteleporta-

tion. Sie können aber auch sehr eigenständig agieren, wenn zum Beispiel wichtige Bestandteile einer Quantenanwendung (Nutzerdatentransfer) ganz ohne „Quantenzutaten“ auskommen.

Nach der gegenseitigen Identifikation werden die nötigen Quantenoperationen in Angriff genommen: die Erzeugung verschränkter Qubits über einzelne Links, die Durchführung von verschränkten Swappings sowie weitere Signalisierungen zum Transfer der Swapping-Ergebnisse und die Nutzung anderer Control-Informationen.

Die verschränkten Qubit-Paare, die keine Nutzerdaten transportieren, werden zusammen mit weiteren ID-Informationen dann im Endknoten an die Quantenanwendung übergeben. Die Umsetzung all dieser Prozesse in Routing, Signalisierung etc. wie auch die Abgrenzungen technischer und administrativer Art (technische/administrative Domains) ist Gegenstand weiterer Forschung, beispielsweise in der IRTF/IETF.

Herausforderungen bei der Implementierung

Ein Qubit kann unter anderem mit dem Polarisationszustand eines Photons oder dem Spinzustand eines Atoms dargestellt werden.

Bei der technischen Umsetzung von Quantennetzen ist die erste Herausforderung, die Dekohärenzeffekte in den Griff zu bekommen. Diese Effekte ergeben sich vorrangig, wenn die Photonen bei der Übertragung in Wechselwirkung mit ihrer Umgebung treten und so Quanteninformationen verloren gehen. Die typische Lebensdauer kohärenter Zustände reicht derzeit von wenigen Mikrosekunden bis zu etwas mehr als einer Sekunde. Bei Geräten, die vom Netz getrennt waren, wurde auch eine Lebensdauer von bis zu einer Minute beobachtet.

> Bei der klassischen Datenkommunikation können Signale durch Repeater wiederholt werden.

Für Quantenkanäle kommen sowohl Glasfasern als auch eine optische Freiraumkommunikation, zum Beispiel im Vakuum, in Betracht. Im Vakuum ist die Dekohärenz eines Photons sehr gering, bei der Übertragung in einer Glasfaser hingegen wird die Intensität des Photons exponentiell mit Länge der Übertragungsdistanz abgeschwächt. Die zweite Herausforderung für Quantennetze ist daher die Skalierbarkeit auf lange Strecken und die Vermeidung der damit verbundenen Kanalverluste und Dekohärenzeffekte.

Bei der klassischen Datenkommunikation können durch den Einsatz von Repeatern Signale wiederholt und verstärkt werden. Daraus ergibt sich die dritte Herausforderung : Das No-Cloning-Theorem macht ein solches Kopieren und erneutes Übertragen in Quantennetzen unmöglich. Ohne Quanten-Repeater wird das Rauschen zu groß, was zu einer hohen Fehlerrate bei Qubits und schließlich zum Kommunikationsausfall führt. Aktuell können QKD-Anwendungen im Netz nur bis zu mehreren Hundert Kilometern sicher umgesetzt werden. Im Sommer 2021 stellte Toshiba eine neue Dual-Band-Stabilisierungstechnik vor, mit der eine QKD-Anwendung über eine Reichweite von immerhin 600 Kilometer umgesetzt werden konnte. Bei dieser Methode werden über die Glasfaser zwei Signale über zwei verschiedene Wellenlängen übertragen. Eine der Wellenlängen wird dann mit der zweiten (Qubit-) Wellenlänge in regelmäßigen Abständen so verschachtelt, dass Schwankungen ausgeglichen und Phasenverfeinerungen vorgenommen werden können.

Für längere Distanzen werden daher Quanten-Repeater benötigt, die in der Lage sind, die Gesamtstrecke in einzelne Segmente zu unterteilen, um dann zwischen jeweils benachbarten Knoten verschränkte Paarzustände auszutauschen und sich dadurch mit wiederholtem Verschränkungsaustausch bis zum Endpunkt entlang zu hangeln (siehe Abbildung 1 und 2).

So ist es möglich, das Problem der Verluste und des No-Cloning-Theorems zu umgehen. Außerdem können durch die kurzen Übertragungssegmente bei dieser Methode auch die Fehlerraten reduziert werden. Die Entwicklung solcher Quanten-Repeater ist derzeit noch nicht abgeschlossen, da effiziente und hochgenaue Quantenspeicher, Gate-Operationen und Messungen benötigt werden. Verschränkungen zwischen zwei benachbarten Knoten mit Quantenspeicher konnten in ersten Versuchen bereits

SCHEMA „TWO-HOP-PFAD“

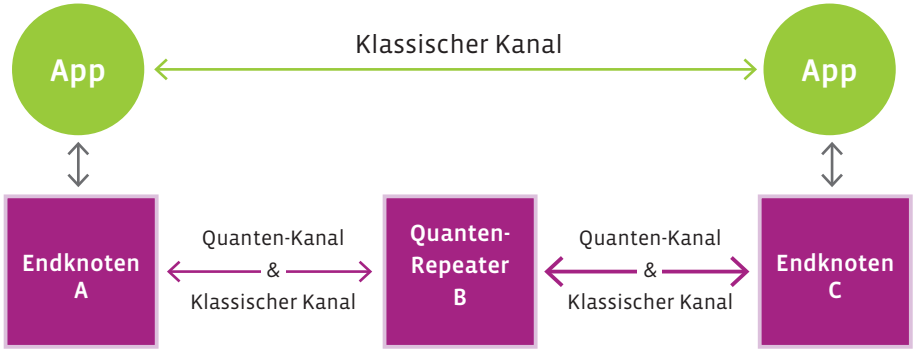


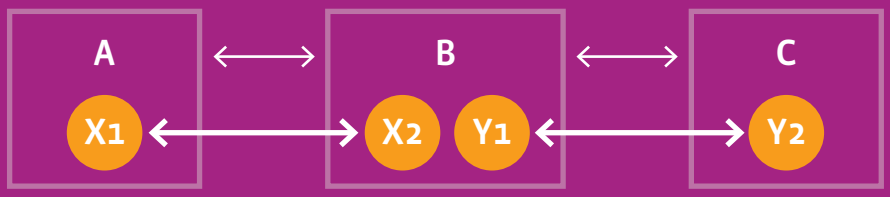
Abbildung 1: Beispiel für einen „Two-Hop-Pfad“. Die Integration klassischer Kanäle kann sehr eng sein oder auch recht abgesetzt erfolgen.

ÜBERTRAGUNGEN VON VERSCHRÄNKUNGEN (ENTANGLEMENT SWAPPING)

Das große Problem bei der Erzeugung verschränkter Paare über einen Link ist der mit wachsender Entfernung der Knoten zunehmende „Zustandszerfall“; wegen des No-Cloning-Theorems ist es außerdem nicht möglich, das Signal zwischendurch zu verstärken. Es ist also nicht direkt möglich, verschränkte Paare (auch Bell-Paare) über beliebig große Entfernungen hinweg stabil zu verteilen.

Um dies dennoch zu ermöglichen, wurde das Entanglement Swapping entwickelt, also die Übertragung und Aneinanderreihung von Verschränkungen.

Ausgangszustand: Drei Knoten A, B, C mit zwei verschränkten Qubit-Paaren



Endzustand: Qubit Y2 nimmt Zustand X2 an und ist mit X1 verschränkt

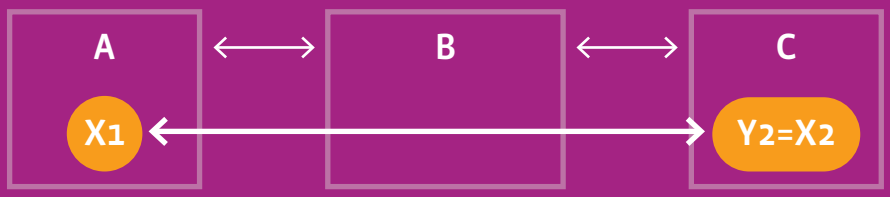


Abbildung 2: Swapping-Prozess

Ein Bell-Paar zwischen zwei Endknoten des Quantennetzes, also eine Quanten-E2E-Verbindung, kann durch eine fortlaufende kombinierte Erzeugung (Aneinanderreihung) von Bell-Paaren entlang der Linkabschnitte (mit Zwischenknoten) erstellt werden. Jeder Zwischenknoten entlang des Weges kann die beiden benachbarten Qubit-Paare (rechte/linke Seite) miteinander verknüpfen und damit eine neue Verschränkung zwischen den Qubits auf seinen beiden Nachbarknoten erzeugen.

In Abbildung 2 wird der Prozess vereinfacht dargestellt, die Details hierzu finden Interessierte auf den Seiten des DFN-WiN-Labors.

2015 umgesetzt werden. Über Glasfaser wurde da schon eine Entfernung von 1,3 Kilometern erzielt, mittlerweile sind Verschränkungen über 50 Kilometer gezeigt worden.

Als Alternative zu Quanten-Repeatern kann bei langen Übertragungsstrecken auch ein Relay Schema, basierend auf Trusted Nodes, angewandt werden: Dabei muss jeder beteiligte Zwischenknoten auf der Strecke speziell gesichert und damit „Trusted Node“ sein. Trusted Nodes sind zwar in der Lage, Qubits mit ihren Nachbarn auszutauschen, können aber kein Entanglement Swapping umsetzen. An jedem Trusted Node wird eine eingehende Nachricht entschlüsselt, authentifiziert und anschließend neu verschlüsselt und dann mit einem neuen Authentifizierungs-Tag an den nächsten Knoten weitergereicht. Dadurch ist die Ende-zu-Ende-Sicherheit von QKD-Anwendungen nicht mehr gewährleistet und man muss dem Trusted-Node-Betreiber trauen.

Eine weitere Alternative für große Übertragungsstrecken ohne den Einsatz von Quanten-Repeatern ist die satellitenbasierte Quantenkommunikation. Diese hat den Vorteil eines viel geringeren Kanalverlusts und einer vernachlässigbaren Dekohärenz im Weltraum.

Für den Aufbau einer Quantennetzinfrastruktur ist außerdem besonders entscheidend, inwieweit die neue Technologie auch in den bereits für die klassische Datenkommunikation genutzten Glasfasernetzen betrieben werden kann. Auch andere bereits bekannte Technologien könnten zum Beispiel für QKD-Anwendungen infrage kommen, beispielsweise sepa-

rate Dark Fibers und Wellenlängen bei 1550 Nanometer oder Mechanismen wie Time-Division Multiplexing (TDM) und Wavelength-Division Multiplexing (WDM). In der chinesischen Stadt Hefei wurde 2018 in einem Test gezeigt, dass QKD auf einer kommerziellen Backbone-Leitung gleichzeitig mit 3,6 Tbit/s an klassischen Daten über insgesamt 66 Kilometer übertragen werden konnte. Die Quantum-Bitfehlerrate (QBER) betrug dabei 2,5 Prozent.

Quantennetz-Projekte in Europa und der Welt

Forschende des EU-Flagship QIA (Quantum Internet Alliance) entwickeln aktuell einen Entwurf für ein verschränkungbasiertes-Quantum-Internet über vier Knoten hinweg – mit Repeatern, Entanglement und Teleportation. In jüngsten Versuchen konnte gezeigt werden, wie eine Verschränkung in Multimode-Festkörper-Quantenspeichern zwischen zwei räumlich getrennten Quantenknoten bis zu 25 Mikrosekunden lang gespeichert werden kann.

Ein weiteres europäisches Projekt ist CiViQ (Continuous Variable Quantum Communications). Hier arbeiten Forschende derzeit an Untersuchungen, die zeigen sollen, wie bei cv-QKD durch Sättigungsangriffe auf Quantendetektoren Sicherheit kompromittiert werden kann. In experimentellen Versuchen werden dabei Sättigungsangriffe herbeigeführt, entweder durch eine große kohärente Verschiebung oder durch einen externen Laser. Dadurch werden die eintreffenden Photonen gestört und nicht mehr in ein korrektes elektrisches Signal verwandelt.

Die BMBF-Initiative QuNET entwickelt Gesamtnetzarchitekturen für Behörden, die sowohl Quantenschlüssel übertragen als auch die Verwendung der Schlüssel in klassischen Kommunikationsnetzen ermöglichen. In Phase II des Projekts liegt der Fokus auf der praktischen Benutzbarkeit und der Skalierbarkeit der Netzwerke, insbesondere auch für die Anwendungsfälle, bei denen mehrere Kommunikationspartner involviert sind. Prototypische Grundlagen wurden bereits in Phase I entwickelt. So konnten in einer quantengesicherten Videokonferenz zwischen zwei Bundeseinrichtungen die Projektergebnisse auf Basis verschiedener Quantentechnologien demonstriert werden.

In den USA betreiben Fermilab und Caltech derzeit zwei Quanten Teleportations-Testbeds (CQNET and FQNET). Beide Testbeds sind baugleich und untersuchen Teleportation. Erste Übertragungsweiten beliefen sich in Versuchen bei einer Wellenlänge von 1536.5 Nanometer auf über zwei mal 22 Kilometer. Beide Netze stehen multidisziplinären Forschungszwecken zur Verfügung und werden derzeit vor allem dafür verwendet, die Geschwindigkeit der Verschränkungsverteilung und die Genauigkeit zu verbessern.

Die Österreichische Akademie der Wissenschaften in Wien und die University of Science and Technology of China (USTC) haben 2018 erstmals eine Vier-Punkte-Übertragung vorgeführt: Dabei waren die Städte Graz und Hefei über den Satelliten Micius verbunden, der in der Lage ist, Quantenschlüssel zu erzeugen und auch quantenverschlüsselte Signale zu verarbeiten. Die Übertragung zwischen Graz und Micius sowie zwischen Micius und Hefei basierte auf Laserstrahlen. Darüber hinaus wurde die Strecke aber von Graz nach Wien und in China von Hefei nach Beijing mit Glasfasern erweitert. Insgesamt umfasste die Strecke somit 7600 Kilometer. Im Test konnte gezeigt werden, dass beispielsweise Graz Daten verschlüsseln konnte mithilfe eines Micius-Graz Schlüssels. Dieser Schlüssel wurde dann von Micius in die Nachricht nach Hefei eingebettet und wiederum verschlüsselt mit einem neuen Micius-Hefei-Schlüssel an das Xinglong Observatory in Hefei übermittelt.

> Der Weg zu Quantennetzen im Produktionsbetrieb ist nicht mehr allzu weit.

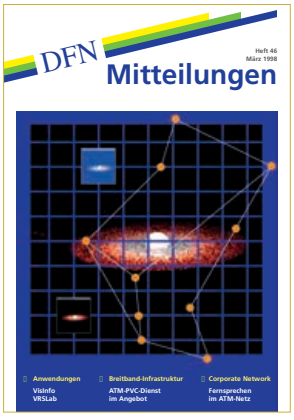
Die Testbeds zeigen, dass der Weg zu Quantennetzen im Produktionsbetrieb nicht mehr allzu weit ist und damit auch ein breiterer Zugang zu QKD und anderen Quantenanwendungen in den nächsten Jahren möglich wird. In der Zwischenzeit können interessierte Nutzende auf QKD- und Quantennetz-Simulatoren wie QKDNetSim und QuISP (optimiert für Repeater/Router Software Entwicklung) zurückgreifen und damit testen und analysieren. ◆

Mehr Informationen zum Thema Quantenforschung und Quanteninternet finden Sie auf **https://www.win-labor.dfn.de/.**

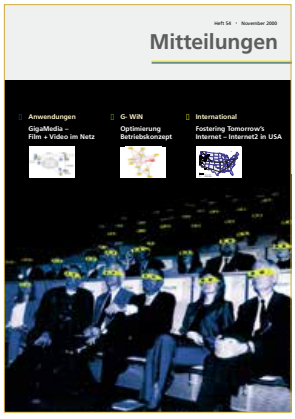
DFM Mitteilungen I Ausgaben 41 - 54

1997

45/1997 – Aufbau der Gigabit-Struktur
1997 begann der Ausbau der Übertragungskapazitäten im damaligen B-WiN, dem Breitband-Wissenschaftsnetz hin zum G-WiN, also in den Bereich von mehreren Gigabit-pro-Sekunde. Mit dem Einsatz neuer optischer Komponenten konnten multimediale Inhalte wie Bilder und Videos aus dem allgemeinen Internet abgerufen werden und sogar Videokonferenzen mit mehreren Teilnehmern an verschiedenen Orten wurden möglich. Der Vorstoß in den Gigabit-Bereich war kein linearer Ausbau der Netzkapazitäten, sondern ein Schritt in die neue Dimension der optischen Kommunikationsnetze.

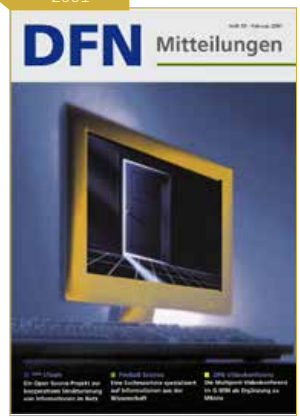


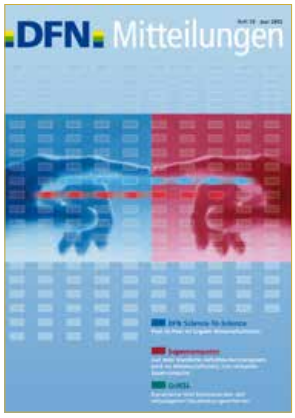
1999



DFM Mitteilungen I Ausgaben 55 - 68

2001





2003

63/2003 – DFNRoaming – unterwegs im Wissenschaftsnetz
„Wo es Euch beliebt" – so lautet der erste Artikel zum damals neu geplanten Pilotprojekt DFNRoaming. Ziel war es, reisenden Forscherinnen und Forschern einen einfachen und sicheren Netzzugang in das DFN zu ermöglichen. Viel Überzeugungsarbeit war notwendig, um möglichst viele Einrichtungen zum Mitmachen zu bewegen. Heute sind Nutzende aus mehr als 100 Ländern weltweit bei eduroam registriert und tragen zum Erfolg des Dienstes bei.

2005

Worauf wir uns verlassen können

Die Verlässlichkeit digitaler Identitäten ist ein wesentlicher Faktor im Vertrauensgefüge einer Föderation wie der DFN-AAI. Aber auf welche Weise erfahren Dienstanbieter, welche Identitäten das für den Zugriff auf einen Dienst relevante Vertrauensniveau aufweisen? Das seit 2009 in der DFN-AAI hierfür verwendete starre Schema der sogenannten Verlässlichkeitsklassen soll künftig durch das flexiblere und präzisere REFEDS Assurance Framework abgelöst werden.

Text: **Wolfgang Pempe** (DFN-Verein)

Foto: nomadsoul1

AAI und IdM – verlässliche Identitäten

Unabhängig vom technischen Kontext sind Betreiber von Onlinediensten grundsätzlich darauf bedacht, den Zugriff auf den betreffenden Dienst und die zugehörigen Ressourcen vor unbefugtem Zugriff zu schützen und jede Form von Missbrauch und unberechtigter Nutzung zu unterbinden. Neben den üblichen Maßnahmen zur Einhaltung der Betriebs- und Informationssicherheit spielt hierbei die Verlässlichkeit der Identitäten der Nutzenden eine entscheidende Rolle. Wenn Personen auf bestimmte geschützte Ressourcen zugreifen, muss sichergestellt sein, dass die betreffende Person auch die ist, die sie zu sein vorgibt, und dass die mit der Identität verbundenen Daten, anhand derer die Autorisierung für den Zugriff auf die betreffende Ressource erfolgt, auch korrekt sind.

Im Kontext einer Authentifizierungs- und Autorisierungsinfrastruktur wie der DFN-AAI ist es der Identity Provider (IdP) einer Heimateinrichtung, der Identitätsdaten an den Service Provider eines Dienstanbieters überträgt. Diese Daten werden auch als Attribute bezeichnet. Im Zusammenhang mit der AAI wird ein Service Provider daher auch häufig als „Relying Party“ bezeichnet, da er den vom IdP übertragenen Informationen vertrauen muss. Mithin ist es also die Aufgabe der jeweiligen Heimateinrichtung, die Zuverlässigkeit der Nutzendendaten und die Sicherheit der AAI-spezifischen Anmeldeprozesse sicherzustellen und gegenüber

Dienstanbietern und Föderationsbetreibern zu garantieren. Eine zentrale Rolle spielen hierbei das Identity Management (IdM) der Heimateinrichtungen und die damit verbundenen Prozesse und Maßnahmen zur Pflege der Identitäten. Dies betrifft in besonderem Maße das Onboarding, also die erstmalige digitale Erfassung von Identitätsdaten, die Aktualisierung derselben sowie das Offboarding bzw. die Deprovisionierung.

Je nachdem wie hoch der potenzielle Schaden ist, der mit einem unberechtigten Zugriff auf geschützte Ressourcen einhergeht, muss ein Dienstanbieter entscheiden, welche Anforderungen an die Verlässlichkeit digitaler Identitäten und Anmeldeprozesse an den Heimateinrichtungen gestellt werden müssen. Um solche Entscheidungen zu unterstützen, existieren unterschiedliche Kataloge zur Schutzbedarfsfeststellung. Als Beispiel sei hier auf die BSI-Richtlinie zu elektronischen Identitäten und Vertrauensdiensten im E-Government verwiesen (TR-03107-1, Abschnitt 2.5).

Verlässlichkeitsklassen in der DFN-AAI

Als die DFN-AAI 2007 den Betrieb aufnahm, galten an den teilnehmenden Heimateinrichtungen einheitliche Vorgaben für die Qualität des Identity Managements. In den folgenden Jahren zeichnete sich jedoch ab, dass nicht alle Einrichtungen in der Lage waren, diese Vorgaben einzuhalten. Diesem Umstand begegnete die DFN-AAI mit der Einführung der heute bekannten Verlässlichkeitsklassen: DFN-AAI Advanced mit unveränderten Anforderungen, DFN-AAI Basic mit weniger strikten Vorgaben sowie DFN-AAI Test, die lediglich zur Teilnahme an der sogenannten Testföderation qualifiziert. Ein Identity Provider wird einer Verlässlichkeitsklasse zugeordnet, wenn alle drei für die jeweilige Klasse gültigen Anforderungen erfüllt sind. Auf technischer Ebene werden diese Verlässlichkeitsklassen über unterschiedliche Metadatensätze modelliert. Dienstanbieter nehmen eine Risikoabschätzung vor und konfigurieren den jeweiligen Service Provider je nach Schutzbedarf der betreffenden Ressourcen, sodass nur die Metadaten importiert werden, in denen die Identity Provider der gewählten Verlässlichkeitsklasse enthalten sind. Auf diese Weise wird auf technischer Ebene sichergestellt, dass ausschließlich eine Interaktion mit Identity Providern erfolgt, zu denen ein grundsätzliches Vertrauensverhältnis besteht.

In der Regel kommen seitens eines Service Providers jedoch noch weitere Filtermechanismen zur Anwendung. So kann z. B. eine Positivliste der zur Nutzung des betreffenden Dienstes berechtigten Hochschulen vorgehalten werden, die den Kreis der Identity Provider, von denen aus eine Anmeldung am SP erfolgen kann, weiter einschränkt. Ein weiteres, sehr mächtiges Filterkriterium stellt die attributbasierte Autorisierung dar. Dieser Mechanismus ermöglicht es, den Zugriff auf den betreffenden Dienst bzw. bestimmte Ressourcen auf einzelne Personen(gruppen) einzuschränken, für die bestimmte Voraussetzungen erfüllt sind. Auf diesen Ansatz setzt das REFEDS Assurance Framework auf, das im nächsten Abschnitt ausführlicher beschrieben wird.

Bei den bestehenden Verlässlichkeitsklassen handelt es sich um ein ausgesprochen grobes und nicht mehr zeitgemäßes Raster. Gerade an größeren Einrichtungen mit historisch gewachsenen Identity Management-Systemen kann die Verlässlichkeit der Identitäten je nach Datum des Onboardings oder der Gruppen-/Fakultätszugehörigkeit durchaus variieren. Dies hat für IdP-Betreiber mitunter zur Folge, dass technischer Mehraufwand betrieben werden muss, um zu verhindern, dass Personengruppen, deren Identitäten lediglich den Anforderungen der Klasse „Basic“ genügen, sich bei Service Providern anmelden können, die die Verlässlichkeitsklasse Advanced verlangen. Alternativ müsste der IdP als Ganzes in ‚Basic‘ eingeordnet werden, womit der Zugriff auf bestimmte

DIE VERLÄSSLICHKEITSKLASSEN DER DFN-AAI (Stand September 2021)

KRITERIUM	ADVANCED	BASIC	TEST / N.A.
Identifizierung durch Heimateinrichtung	pers. Vorsprechen gegenüber Vertrauensinstanz unter Vorlage amtlicher Dokumente (alternativ: Postident, eID/nPA). Die an den Hochschulen etablierten Einschreibungs- und Einstellungsprozesse werden als gleichwertig akzeptiert	Rückantwort von eindeutiger Adresse (E-Mail, Tel.-Nr., Postanschrift etc.)	Verfahren freigestellt
Verfahren zum Ausweis einer Identität	persönlicher Account bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Anhand eindeutig zuzuordnender digitaler Adresse	Verfahren freigestellt
Datenhaltung und Prozesse zur Pflege der Identitäten	Verpflichtung bzgl. Aktualität innerhalb von zwei Wochen	Verpflichtung bzgl. Aktualität innerhalb von drei Monaten	Verfahren freigestellt

Tabelle 1

Dienste nicht mehr möglich wäre. Weiterhin werden aktuell einige entscheidende Aspekte ausgeklammert, wie z. B. Prozesse zur Vergabe neuer Credentials oder die Frage, ob einmal vergebene Identifier/Nutzerkennungen zu einem späteren Zeitpunkt „recycelt", d. h. anderen Personen zugeordnet werden.

Es wird also Zeit für einen möglichst feingranularen und flexiblen Ansatz, der mehr Kriterien abdeckt und es Dienstanbietern bzw. Service Providern zusätzlich ermöglicht, sich je nach individuellem Schutzbedarf besonders relevante Verlässlichkeitskriterien „herauszupicken", ohne ein abstraktes, undurchsichtiges Kriterienbündel in Form einer Verlässlichkeitsklasse fordern zu müssen. Eine weitere Motivation für den geplanten Wechsel ist das Bestreben, über die Implementierung eines international anerkannten Standards die Anschlussfähigkeit der DFN-AAI im internationalen Kontext zu wahren. Dies betrifft in besonderem Maße die Unterstützung von Forschungscommunities, die auf föderationsübergreifende Zusammenarbeit im Rahmen von eduGAIN angewiesen sind.

Attributbasierter Ansatz – das REFEDS Assurance Framework

Das REFEDS Assurance Framework, kurz RAF (ein für deutsche Verhältnisse unglücklich gewähltes Akronym), spezifiziert einen attributbasierten Ansatz, d. h. Verlässlichkeitsinformationen werden in Form von Attributen bzw. Attributwerten an einen Service Provider übertragen, der anhand dieser Angaben unter Berücksichtigung des Schutzbedarfs der jeweiligen Ressource(n) eine Autorisierungsentscheidung trifft. Unterschiedliche Kriterien der Verlässlichkeit können so unabhängig voneinander adressiert und kombiniert werden. Dieser Ansatz ist inspiriert von den sogenannten „Vectors of Trust" (RFC 8485). Ergänzt wird das RAF durch zwei Authentifizierungsprofile: das REFEDS Single Factor Authentication Profile (SFA) und das REFEDS Multi-Factor Authentication Profile (MFA), in denen Minimalanforderungen an Verfahren zur Authentifizierung von Nutzenden am IdP festgelegt werden. Gemeinsam bilden diese drei Spezifikationen – RAF, SFA und MFA – die sogenannte REFEDS Assurance Suite.

Das RAF wurde 2018 als internationaler Standard eingeführt, der insbesondere föderationsübergreifende Kooperationen im eduGAIN-Kontext unterstützen soll. Eine wichtige Motivation hierbei war der Umstand, dass Föderationen bis dahin – sofern überhaupt gegeben – eigene Levels of Assurance bzw. Verlässlichkeitsklassen definiert hatten, die nur sehr bedingt interoperabel waren, ein Zustand, an dem sich nur allmählich etwas ändert. Einen wichtigen Meilenstein bezüglich der internationalen Unterstützung des RAF hat das NIH gesetzt, das National Institute of Health (USA), dessen Service Provider mittlerweile bestimmte Verlässlichkeitsangaben gemäß des RAF verlangt.

Neben einigen Basisanforderungen, die grundsätzlich erfüllt sein müssen, behandelt das RAF drei Aspekte des Identity Managements. Diese Punkte sind im Kasten zusammengestellt.

Unter „Identifier uniqueness" werden folgende Kriterien behandelt:

- die Rückführbarkeit eines Identifiers auf genau eine natürliche Person,
- die Fähigkeit der Heimateinrichtung, diese Person im Zweifelsfall zu kontaktieren,
- die zur Identifizierung von Nutzenden verwendeten Attribute bzw. Name Identifier
- sowie die Frage, ob bestehende Identifier „recycelt", also ggf. neuen natürlichen Personen zugeordnet werden.

Diese Punkte werden von den Verlässlichkeitsklassen der DFN-AAI nur teilweise abgedeckt.

Bei „Identity proofing and credential issuance, renewal and replacement" geht es um die Qualität der für diese Verfahren implementierten Prozesse. Als Vergleichsgrößen

Das REFEDS Assurance Framework spezifiziert vier grundsätzliche Anforderungen an den Betrieb eines Identity Providers in einer Identity Federation („Conformance Criteria")

1. *The Identity Provider is operated with organizational-level authority*
2. *The Identity Provider is trusted enough that it is (or it could be) used to access the organization's own systems*
3. *Generally-accepted security practices are applied to the Identity Provider*
4. *Federation metadata is accurate, complete, and includes at least one of the following: support, technical, admin, or security contacts*

» **Nur wenn alle vier Kriterien erfüllt sind, darf ein IdP Unterstützung für das RAF signalisieren.**

Darauf aufbauend adressiert das RAF drei Aspekte des Identity Managements in Hinblick auf die AAI

1. *Identifier uniqueness*
2. *Identity proofing and credential issuance, renewal and replacement and*
3. *Attribute quality and freshness*

DIE KATEGORIEN BEIDER SYSTEME IM VERGLEICH

REFEDS ASSURANCE SUITE	DFN-AAI VERLÄSSLICHKEITSKLASSEN
RAF Identifier uniqueness	keine direkte Entsprechung
RAF Identity proofing and credential issuance, renewal and replacement	Verfahren zur Identifizierung durch die nutzende Einrichtung
RAF Attribute quality and freshness	Datenhaltung und Prozesse zur Pflege der Identitäten
Single Factor Authentication Profile, Multi Factor Authentication Profile	Verfahren zum Ausweis einer Identität

Tabelle 2

werden die entsprechenden Anforderungen aus anderen Kriterienkatalogen angeführt, unter anderem die in der eIDAS-Durchführungsverordnung spezifizierten Levels of Assurance. Die Verlässlichkeitsklassen der DFN-AAI behandeln ausschließlich das Verfahren des „Identity proofing".

Bei „Attribute quality and freshness" geht es darum, wie schnell etwaige Änderungen – wie zum Beispiel das Ausscheiden aus einer Einrichtung oder der Übergang vom Studierenden- in den Angestelltenstatus – über die vom IdP ausgelieferten Attribute reflektiert werden. Dieser Aspekt entspricht dem Punkt „Datenhaltung und Prozesse zur Pflege der Identitäten" in den Verlässlichkeitsklassen der DFN-AAI.

Für die im RAF behandelten Kriterien existiert ein kontrolliertes Vokabular, das signalisiert, ob und wie bzw. in welcher Qualität das jeweilige Kriterium für die betreffende Identität erfüllt wird. Als Träger dieser Verlässlichkeitsinformationen dient das Attribut eduPersonAssurance, das beliebig viele Werte transportieren kann. Aus der Liste der übertragenen Attributwerte kann ein Service Provider die für seine Autorisierungsentscheidung relevanten Angaben auswerten. Für weitere Details sei auf die Spezifikation unter https://refeds.org/assurance verwiesen sowie auf die demnächst im DFN-AAI-Wiki verfügbare Dokumentation.

Umsetzung in der DFN-AAI

Für die Einführung der REFEDS Assurance Suite in der DFN-AAI und die Ablösung der Verlässlichkeitsklassen durch das REFEDS Assurance Framework ist folgendes Vorgehen geplant:

1. Im Laufe der kommenden Wochen wird die Onlinedokumentation um ausführliche Informationen zur REFEDS Assurance Suite erweitert. Dabei sollen nicht nur Konfigurationsbeispiele für Identity und Service Provider bereitgestellt werden, sondern auch deutschsprachige Erläuterungen zu den Spezifikationen.

2. Für Januar 2022 sind zwei Workshops geplant, die sich jeweils mit den Themen REFEDS Assurance Framework und Multi-Faktor-Authentifizierung befassen. Ein besonderer Schwerpunkt wird hierbei auf der technischen Umsetzung mithilfe der Shibboleth Software (IdP, SP) liegen.

3. Ende März 2022 werden die getrennten Metadatensätze für die Verlässlichkeitsklassen Advanced und Basic abgeschafft. Für die Produktivumgebung der DFN-AAI werden dann ausschließlich die beiden bereits jetzt schon vorhandenen Datensätze zur Verfügung stehen, die jeweils die Metadaten aller produktiven IdPs und SPs enthalten. Die Metadatenverwaltung der DFN-AAI wird die beiden Klassen Advanced und Basic weiterhin unterstützen. Allerdings werden die IdP-seitige Zugehörigkeit zu einer Verlässlichkeitsklasse und die diesbezüglichen Anforderungen eines Service Providers dann nur noch über entsprechende Entity Attribute in den IdP- und SP-Metadaten verfügbar sein. Diese Art der Kennzeichnung ist bereits seit Längerem implementiert.

4. Zum Jahresende 2022 wird die Unterstützung der Verlässlichkeitsklassen seitens der Metadatenverwaltung eingestellt. Ab Januar 2023 werden Informationen zur Verlässlichkeit digitaler Identitäten in der DFN-AAI ausschließlich über die Mechanismen des REFEDS Assurance Frameworks abgebildet. ◆

Bei Fragen und Anregungen wenden Sie sich jederzeit gerne an das Team der DFN-AAI:
hotline@aai.dfn.de

Weiterentwicklung der DFN-PKI mit GÉANT TCS

Der DFN-Verein erweitert sein Angebot an Zertifikatdienstleistungen: Als Weiterentwicklung der DFN-PKI „Global“ steht nun allen Teilnehmern des Deutschen Forschungsnetzes (DFN) der GÉANT Trusted Certificate Service (TCS) zur Verfügung. Mit TCS wird eine Ausstellung von Zertifikaten über die DFN-AAI realisiert. Zusätzlich werden weitere Möglichkeiten zur PKI-Automatisierung angeboten. 34 Forschungsnetze mit mehreren Tausend angeschlossenen Einrichtungen profitieren bereits von TCS.

Text: **Jürgen Brauckmann** (DFN-CERT)

Foto: Montri Thipsorn /Shutterstock

Der Trusted Certificate Service (TCS) von GÉANT wurde im zweiten Halbjahr 2021 im DFN eingeführt. Mit dem Dienst können Zertifikate für Personen und Server erstellt werden, die – wie beim bisherigen Sicherheitsniveau „Global“ der DFN-PKI – von allen Betriebssystemen und Browsern erkannt werden. Zur Automatisierung stehen mehrere Schnittstellen wie das in vielen Standardwerkzeugen implementierte ACME-Protokoll zur Verfügung. Die DFN-AAI ist eingebunden und kann zur komfortablen Ausstellung von Personenzertifikaten oder auch zum Erzeugen von Anträgen für Serverzertifikate verwendet werden.

TCS wird unter Einbeziehung aller europäischen Forschungsnetze und einer Expertengruppe, der Policy Management Authority, kontinuierlich weiterentwickelt. Die Bedürfnisse von Hochschulen und Forschungseinrichtungen in Europa stehen dabei im Fokus. TCS wird bereits von 34 Forschungsnetzen unterschiedlichster Größe mit mehreren Tausend angeschlossenen Hochschulen, Forschungs- und Bildungseinrichtungen genutzt.

Nach einer von GÉANT organisierten Ausschreibung konnte mithilfe eines gemeinschaftlich erarbeiteten Anforderungskatalogs ein geeigneter Anbieter gefunden werden. Durch die dank der Ausschreibung gebündelte europäische Nachfrage wird eine sehr hohe Kosteneffizienz erreicht. Des Weiteren garantiert dieses Verfahren die Wahl eines Dienstleisters mit einer kritischen Größe, der absehbar in der Lage sein wird, die hohen Anforderungen an öffentlich vertraute PKIs nachhaltig zu erfüllen.

> Die vertragliche Gestaltung ist denkbar schlank gehalten.

Der Dienst wird regelmäßig neu ausgeschrieben. Dies garantiert auf der einen Seite, dass neue Entwicklungen kontinuierlich in die Ausschreibungsbedingungen aufgenommen werden. Auf der anderen Seite finden dadurch Wechsel des Dienstleisters statt, in deren Folge die teilnehmenden Einrichtungen zu neuen Oberflächen, Wurzelzertifikaten und teils neuen Prozessen migrieren müssen.

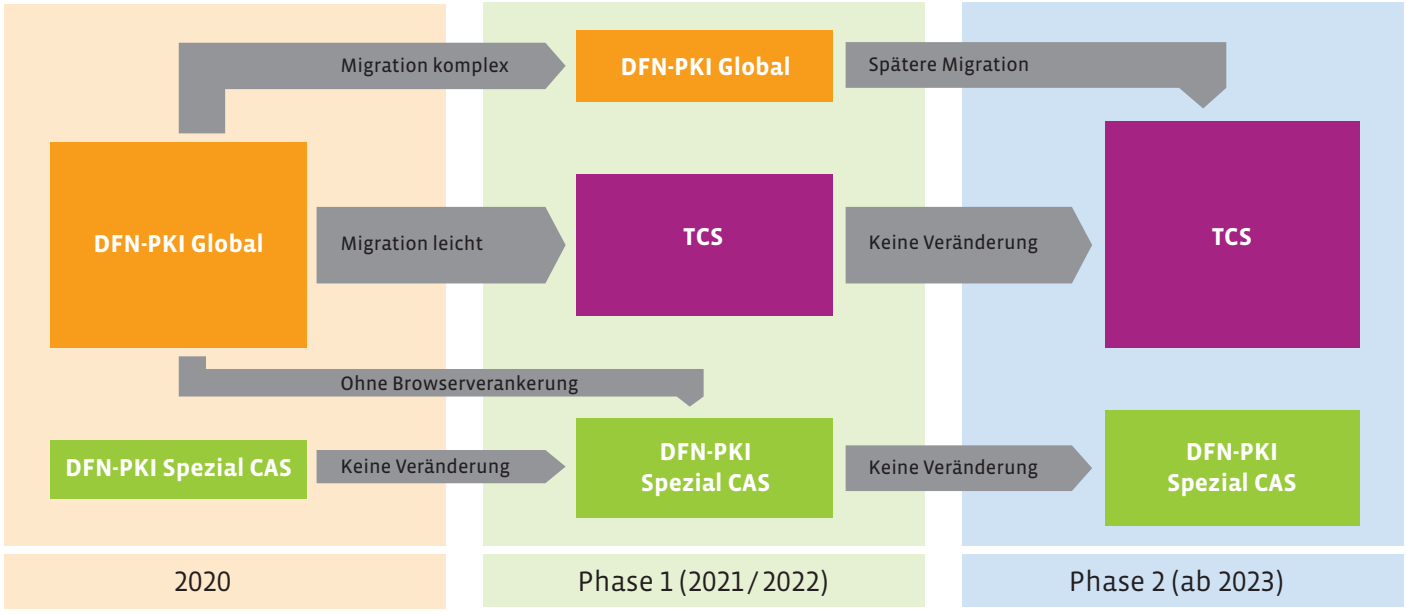
Die vertragliche Gestaltung ist denkbar schlank gehalten: Einrichtungen, die bereits an der DFN-PKI teilnehmen, müssen dem DFN-Verein lediglich eine einfache Beauftragung erteilen. Es ist also kein Vertrag mit GÉANT oder gar dem Dienstleister nötig. Als Bestandteil der DFN-PKI ist die Nutzung von TCS mit den Entgelten für DFNInternet oder dem Dienstpaket abgedeckt (ausgenommen die separate, kostenpflichtige Ausstellung von Spezialzertifikaten, die von Sectigo auf Crypto-Token erstellt und versendet werden).

In den vergangenen Monaten konnte das PKI-Team allen bestehenden Teilnehmern der DFN-PKI einen Zugang zu dem Dienst zur Verfügung stellen.

Auf einen Blick: Die Vorteile von TCS

Aus strategischer Sicht bietet GÉANT TCS strukturell die notwendige Größe, um auch in Zukunft die weiter steigenden Anforderungen an eine browserverankerte PKI-Dienstleistung zu erfüllen. Sowohl die Nutzenden als auch die Browser- und Betriebssystemhersteller haben in den vergangenen Jahren eine kontinuierliche Steigerung des Dienstumfanges von browserverankerten PKIs verlangt und werden dies in absehbarer Zeit

MIGRATION DER DFN-PKI „GLOBAL“



Die Größe der Boxen und Pfeile repräsentiert die Anteile an der Gesamtzahl der Zertifikate (ohne Maßstab)

ENTWICKLUNG DER DFN-PKI „GLOBAL“

Seit Ende 2006 gibt es das Sicherheitsniveau „Global“ in der DFN-PKI. Dieses ist mit PKIs der Deutschen Telekom Security GmbH verkettet, um eine Anerkennung in Browsern und Betriebssystemen sicherzustellen. Seit 2012 wird die DFN-PKI „Global“ nach den relevanten Standards ETSI TS 102 042 bzw. dem Nachfolger EN 319 411-1 auditiert.

Die Sicherstellung des browserverankerten Betriebs ist aufwendig, da sich die Anforderungen kontinuierlich weiterentwickeln. Es müssen nicht nur die ETSI-Standards umgesetzt werden. Weitere Anforderungen kommen aus dem CA/Browser-Forum – einem Zusammenschluss von Zertifizierungsstellen und Browser- bzw. Betriebssystemherstellern –, aber auch aus individuellen Regelwerken einzelner Hersteller wie Mozilla oder Apple. Insbesondere Letztere weisen eine hohe Dynamik auf. Änderungen können große Auswirkungen haben. Beispielsweise wurde 2020 kurzfristig eine drastische Verkürzung des Gültigkeitsintervalls von Apple-Serverzertifikaten durchgesetzt.

Die Erfüllung dieser externen Anforderungen hat für jede browserverankerte PKI größte Priorität, da bei Nichterfüllung schwere Konsequenzen drohen – auch für die Kunden. Für kleine Organisationseinheiten wie beispielsweise die DFN-PKI bedeutet dies, dass strukturell die Anforderungen der eigenen Teilnehmer im Zweifel weniger Gewicht erhalten, als wünschenswert wäre.

auch weiterhin tun. Langfristig lässt sich hier nur mit forschungsnetzübergreifenden Strukturen mithalten.

Die konkreten Vorteile der aktuellen Umsetzung von TCS zeigen sich in den folgenden Aspekten:

- Unterstützung des ACME-Protokolls zur automatischen Zertifikatsausstellung
- Einfachere Prozesse bei der Ausstellung von Nutzerzertifikaten
- Einbindung der DFN-AAI
- Zusätzliche Methoden zur Validierung von Domains
- Einfaches REST-API zur Steuerung fast aller Aspekte der PKI
- Verfügbarkeit von Extended Validation (EV)-Zertifikaten
- Rabattierte Preise für Spezialzertifikate wie Extended Validation Code Signing und Adobe Document Signing
- Anbindung an kommerziell erhältliche Mail-Gateways für die Verschlüsselung/Signatur von E-Mails.

Technische Eigenschaften von TCS

Die technische Basis der DFN-PKI wird bisher vom DFN-Verein komplett selbst betrieben. Im Gegensatz dazu wird der Trusted Certificate Service von einem kommerziellen Anbieter erbracht. Der DFN-Verein und das PKI-Team des DFN-CERT in Hamburg sind weiterhin direkte Ansprechpartner der Teilnehmer und beantworten über die bekannten Wege Fragen zur Organisation und zu technischen Details.

Die derzeitige Generation von GÉANT TCS wird seit Frühjahr 2020 durch Sectigo Limited, UK, betrieben. Sectigo ist ein internationaler PKI-Anbieter mit Niederlassungen in Großbritannien, Kanada, Spanien und den USA.

Teilnehmer erhalten vom PKI-Team des DFN-Vereins einen direkten Zugang zu dem von Sectigo betriebenen Portal, mit dem die Server- und Nutzerzertifikate ausgestellt werden. Voraussetzung ist selbstverständlich, dass der Teilnehmer die Kontrolle über alle Domains, die in die Zertifikate als E-Mail-Adressen oder Server-Namen aufgenommen werden sollen, in einem Domain Control Validation-Prozess nachweist. Dies geschieht wie in der DFN-PKI über eine E-Mail an einen Domain-Kontakt, alternativ über DNS- oder HTTP-basierte Mechanismen.

Es gibt verschiedene Wege, wie Zertifikate ausgestellt werden können. Das ACME-Interface ist das modernste Verfahren. Mit diesem API können Serverzertifikate mit auf vielen Systemen verfügbaren Werkzeugen, z. B. certbot oder Win-ACME, direkt ausgestellt und erneuert werden. Damit bietet TCS eine gute Möglichkeit, die Zertifikatausstellung zu automatisieren.

Einbindung in die DFN-AAI

Ein weiterer sehr interessanter Aspekt: Sectigo stellt einen Service Provider zur Verfügung, der den Nutzenden nach einer Authentifizierung an einem in der DFN-AAI eingebundenen Identity Provider direkt ein Zertifikat für E-Mail-Verschlüsselung/-Signatur oder Client-Authentisierung ausstellt. Hierbei ist keine weitere Interaktion eines Teilnehmerservices erforderlich, da die Anmeldung in der AAI und die dabei übertragenen Daten über den Nutzenden als Basis der Zertifikatausstellung herangezogen werden. Insbesondere ist keine PKI-spezifische Vor-Ort-Identifizierung mit separaten Dokumentationspflichten erforderlich, da schon vorhandene Identifizierungen z. B. im Rahmen der DFN-AAI „Advanced“ eingesetzt werden können. Die Nutzenden erhalten ihre Zertifikate direkt ohne weitere Verzögerung als Download.

Anträge für Serverzertifikate können ebenfalls über eine AAI-Authentifizierung erstellt werden, sodass die Registrierungsstelle beim Teilnehmer die Zuordnung zur einreichenden Person direkt feststellen kann.

BETRIEB VON SPEZIAL-PKIS

Browserverankerte PKIs wie TCS oder die DFN-PKI „Global“ müssen auf die Anforderungen der Browser- und Betriebssystemhersteller fokussiert sein. Damit gehen große Einschränkungen einher, sodass für abweichende Anwendungsszenarien Spezial-PKIs ohne Browserverankerung sehr sinnvoll sind. Mit einer solchen PKI können beispielsweise Zertifikate ausgestellt werden, die eine längere Laufzeit haben, als nach den externen Anforderungen möglich wäre. Auch interne Namen („*.local“) oder sonst nicht erhältliche Kombinationen aus Zertifikatsverwendungszwecken sind möglich.

Ein bekanntes Beispiel: Bei der Absicherung der SAML-Kommunikation in der DFN-AAI wird zunehmend auf Spezial-PKIs zurückgegriffen, da der Zertifikatswechsel in den Metadaten der AAI für eine Laufzeit von browserverankerten Zertifikaten von 398 Tagen zu aufwendig ist. Spezial-PKIs werden daher im Rahmen der DFN-PKI auch weiterhin langfristig zur Verfügung gestellt.

Migration der DFN-PKI „Global“

GÉANT TCS wird das Sicherheitsniveau „Global“ der DFN-PKI vollständig ablösen. Allerdings wird eine Umstellung der Prozesse zur Ausstellung von Zertifikaten bei den Teilnehmern eine gewisse Zeit benötigen. Die DFN-PKI „Global“ wird in sehr unterschiedlichen Szenarien genutzt. Für einfache Fälle wie die Ausstellung von Server- oder Nutzerzertifikaten in Einzelprozessen ist eine sehr schnelle Migration möglich. Einen technischen Zugang zu TCS hat jeder Teilnehmer bereits erhalten, sodass die Migration sehr leicht fallen sollte.

> GÉANT TCS wird das Sicherheitsniveau „Global“ der DFN-PKI vollständig ablösen.

Für komplizierte Fälle wie beispielsweise die tiefe Integration der Schnittstellen der DFN-PKI „Global“ in die automatisierte Zertifikatsproduktion ist eine Umstellung aufwendiger. Das Jahr 2022 sollte von jedem Teilnehmer, der umfangreiche Anwendungsszenarien hat, zur Planung der Migration genutzt werden. Es kann entweder ein Übergang zu TCS vorgenommen werden oder aber je nach Szenario ein Umstieg auf eine nicht im Browser verankerte Spezial-PKI. Beispielsweise kann eine reine Nutzerauthentifizierung auch problemlos mit Spezial-PKIs aufgebaut werden. Öffentlich betriebene Webserver oder E-Mail-Verschlüsselung und -Signatur erfordern aber in aller Regel einen Wechsel zu TCS.

Fazit

Mit der Bereitstellung von GÉANT TCS entwickelt der DFN-Verein den Dienst DFN-PKI weiter. TCS wird das Sicherheitsniveau DFN-PKI „Global“ in einer gestaffelten Übergangsperiode ablösen. Teilnehmer, die kompliziertere Anwendungsszenarien mit der bisherigen DFN-PKI „Global“ umgesetzt haben, sollten jetzt mit der Planung der Migration beginnen.

TCS bietet interessante Merkmale, die bisher nicht zur Verfügung standen: Insbesondere ist nun die DFN-AAI angebunden, sodass Personenzertifikate ohne lästige erneute persönliche Identifizierung nur für PKI-Zwecke ausgestellt werden können. Für die bessere Automatisierung von Serverzertifikaten steht das ACME-Protokoll zur Verfügung. Gleichzeitig kann das bestehende Angebot mit den bekannten Schnittstellen und Interfaces weiterhin mit Spezial-PKIs genutzt werden. ◆

Kontakt:

Bei Fragen zu TCS oder zur Migration der DFN-PKI wenden Sie sich bitte per E-Mail an: **dfnpca@dfn-cert.de**

Informationen zur TCS in der DFN-PKI finden Sie unter: **https://www.pki.dfn.de/geant-trusted-certificate-services/**

Informationen zu Spezial-PKIs in der DFN-PKI finden Sie hier: **https://www.pki.dfn.de/internelokale-cas/**

EasyRoam4Edu – der kurze Weg zu eduroam

Bei Studierenden, Forschenden und Beschäftigten der Hochschulen steht der Dienst eduroam hoch im Kurs. Auch die Authentifizierungs- und Autorisierungs-Infrastruktur (AAI) des DFN wird für immer mehr Bereiche eingesetzt, in denen Nutzende aus Wissenschaft und Forschung Zugang zu geschützten Ressourcen benötigen. Was liegt näher, als beide Dienste zu verknüpfen? Die neue Anwendung EasyRoam4Edu ermöglicht über DFN-AAI-Accounts den unkomplizierten, zertifikatsbasierten eduroam-Zugang.

Text: **Ralf Paffrath** (DFN-Verein)

DFN-AAI und eduroam gehören schon seit Langem zu den zentralen Diensten im DFN. So ist es nicht verwunderlich, dass fast alle Studierenden in Deutschland im Laufe ihres Studiums früher oder später mit diesen Diensten in Kontakt kommen. Die Kernkompetenzen der DFN-AAI und von eduroam sind sehr ähnlich. Beide Dienste authentifizieren und autorisieren Personen im DFN, um diesen beispielsweise Zugang zu Netzressourcen (LAN, WLAN) beziehungsweise Inhalten von Bibliotheken oder lizenzierten Webseiten zu ermöglichen. Daher ist es nachvollziehbar, dass diese beiden Dienste näher zusammenrücken. Unter anderem aus dieser Idee, die auf einen Vorschlag aus dem Betriebsausschuss des DFN-Vereins zurückzuführen ist, entstand EasyRoam4Edu. Aktuell wird EasyRoam4Edu im DFN pilotiert und ermöglicht über DFN-AAI-Accounts den unkomplizierten, zertifikatsbasierten eduroam-Zugang.

Wie funktioniert EasyRoam4Edu?

EasyRoam4Edu kann sowohl von Einrichtungen mit wenigen Nutzenden als auch von Einrichtungen mit vielen Nutzenden im DFN eingesetzt werden.

Im Pilotbetrieb gibt es den EasyRoam4Edu-Server https://get.eduroam.de, der eduroam-Profile in der Eigenschaft als DFN-AAI Basic Service Provider für die gängigen Betriebssysteme wie WINDOWS ≥ 10, MacOSX/iOS, ANDROID und LINUX-Derivate anbietet. Der EasyRoam4Edu-Server kann dabei in den Konfigurationsassistenten auf https://cat.eduroam.org eingebunden und im Rahmen des Pilotprojektes über den Eintrag EasyRoam4Edu (DFN-GS Pilot) angesteuert werden.

In eduroam gibt es neben anderen Verfahren zur Anmeldung die Authentifizierungsmethode EAP-TLS. Dabei kommen ausschließlich Client-Zertifikate zum Einsatz. Diese Zertifikate innerhalb eines eduroam-Profils erhalten die Nutzenden, wenn sie sich über ihren DFN-AAI-Basic-Account im System get.eduroam.de anmelden. Damit Nutzende sich erfolgreich am EasyRoam4Edu-Backend anmelden können, müssen sie zuvor auf dem DFN-AAI-Identity Provider (IdP) in den Einrichtungen im Rahmen eines Opt-in-Verfahrens von den Administrierenden für EasyRoam4Edu freigeschaltet werden. Während die DFN-AAI-IdP-Administrierenden in den Einrichtungen die Identitäten der Nutzenden kennen, wird dem EasyRoam4Edu-Server nur das Pseudonym der Nutzenden in Form des Attributs Pairwise ID mitgeteilt. Nach der Anmeldung am DFN-AAI-IdP wird auf der Grundlage der Pairwise ID ein pseudonymer Account auf dem EasyRoam4Edu-Server angelegt. Mit diesem Account können die Nutzenden eduroam-Zertifikate/-Profile für ihre Endgeräte generieren.

Eduroam-Föderation im DFN

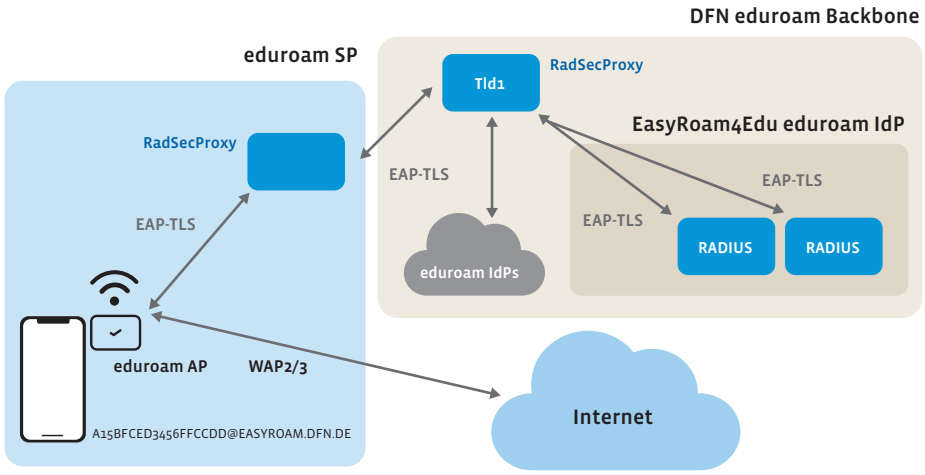


Abbildung 1: So funktioniert die Anmeldung in eduroam

Die eduroam-Client-Zertifikate sind Teil einer „Private CA“ und können nur für die Anmeldung in eduroam genutzt werden. Der EasyRoam4Edu-Server speichert ausschließlich die Pairwise ID, also das Pseudonym des DFN-AAI-IdP-Accounts, und verknüpft diese untrennbar mit den Seriennummern von Client-Zertifikaten. Die Seriennummer der Zertifikate ist Teil der Roaming-Indentität bei der Anmeldung in eduroam und kann nicht geändert werden.

Über die Verknüpfung der Pairwise ID und den Seriennummern in den Zertifikaten lässt sich die Identität der eduroam-Nutzenden beim DFN-AAI-IdP eindeutig zuordnen, während in EasyRoam4Edu und in eduroam die Nutzenden pseudonymisiert erscheinen. Somit ist der Nutzende generell nicht anonym in eduroam unterwegs.

Zusammensetzung und Aufbau der EasyRoam4Edu-Infrastruktur

Die EasyRoam4Edu-Infrastruktur setzt sich unter anderem zusammen aus einem Backend Server get.eduroam.de und zwei Authentifizierungsservern, easyroam.eduroam.de und easyroam2.eduroam.de. Die Serversoftware auf get.eduroam.de ist eine in C-Sharp geschriebene .NET-Entwicklung. Es wurde bewusst auf PHP verzichtet, da PHP nicht die Serversicherheit bietet, die in EasyRoam4Edu benötigt wird. Auf den Authentifizierungsservern wird jeweils ein FREERADIUS-Server betrieben. Die Realms für das Routing in eduroam werden aus dem Namen der DFN-AAI-IdPs und dem Präfix easyroam gewonnen. Beispiel: aus dem IdP-Namen dfn.de wird der eduroam Routing Realm: ‹seriennummer›@easyroam.dfn.de. Die eduroam Föderationsclient/-server filtern die Requests aus EasyRoam4Edu und leiten diese auf die beiden FREERADIUS-Server, die die EAP-TLS-Authentifizierung durchführen, weiter.

EasyRoam4Edu-Bootstrap

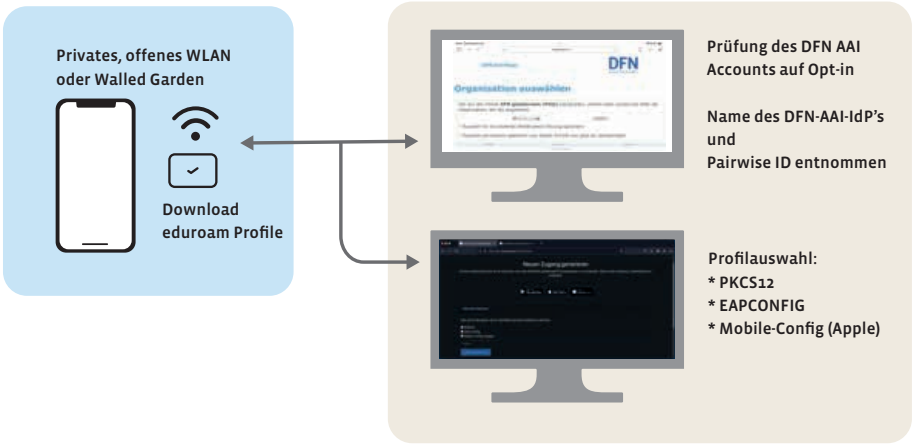


Abbildung 2: Die Profile werden mittels Bootstrapping auf den Endgeräten installiert

Erzeugung und Installation der Profile

Zunächst benötigen die Nutzenden einen Netzzugang. Das kann ein öffentliches oder ein privates WLAN sein. Aber auch ein „Walled Garden“, eine partiell offene Plattform, ist möglich. In diesem Walled Garden müssten dann der EasyRoam4Edu-Server get.eduroam.de, der WAYF (Where Are You From) und die DFN-AAI-IdPs in der Firewall in Form einer Whitelist freigeschaltet werden. Letzteres ist nicht ganz so trivial für Admins. Die IP-Adressen der DFN-AAI-IdPs können jedoch aus den DFN-AAI-Basic-Metadaten destilliert werden. Die Nutzenden haben in der Regel die Möglichkeit, die Profile auf einigen Geräten wie WINDOWS ≥ 10 oder ANDROID über die GETEDUROAM von GÉANT herunterzuladen oder auf macOS/iOS direkt vom EasyRoam4Edu-Server. EasyRoam4Edu ist so konzipiert, dass es nach Möglichkeit alle Varianten der Installation der Profile unterstützt.

Ausblick für das Pilotprojekt EasyRoam4Edu

Im Pilotprojekt stehen wir mitten im Prozess, den Piloten in den Regelbetrieb zu überführen. Wir werden den Service etwa ein Jahr lang erproben. Dabei gibt es rund um EasyRoam4Edu viele Ideen und Fragen, wie beispielsweise

- zur Laufzeit der Client-Zertifikate,
- zur Entscheidung Public CA und/oder Private CA für RADIUS-Server- und Client-Zertifikate,
- zum Umgang mit exmatrikulierten Studierenden,
- zu den Befugnissen und Verantwortlichkeiten der EasyRoam4Edu-Admins, z. B. bei Widerruf der Client-Zertifikate,
- zum einmaligen Einsatz eines QR-Codes zwecks Download der Profile,
- zur Anzahl der erlaubten Geräte,
- zur Einbettung von EasyRoam4Edu in Workflows und Umgebungen in den Einrichtungen oder
- ob ein Opt-in-Verfahren für die Freischaltung der Nutzenden ausreicht.

Die Aufzählung ist nur ein Ausschnitt der Themen, mit denen wir uns im Pilotprojekt befassen wollen. Wenn möglichst viele Einrichtungen an dem Pilotdienst teilnehmen, besteht eine gute Chance, viele dieser Punkte aufzugreifen und gemeinsam Lösungswege zu erarbeiten. ◆

Weitere Informationen finden Sie unter: **https://doku.tid.dfn.de/de:eduroam:start**
Für Fragen stehen wir jederzeit zur Verfügung: **easyroam4edu@dfn.de**

Sicherheit aktuell

Security Trainings powered by GN4-3

Im Januar 2019 startete GÉANT mit dem GN4-3-Projekt; das erste Mal ist ein komplettes Workpackage (WP8) ausschließlich mit Security-Themen besetzt worden. Während einige dieser Themen eine Fortführung früherer Arbeiten darstellen, konnten durch das erhöhte Budget auch neue Themenfelder angepackt werden. Dazu gehören auch die Security-Trainings, die primär vom DFN-CERT erarbeitet werden.

Mittels einer Gap-Analyse der für GÉANT-Mitglieder verfügbaren Trainingsprogramme und -materialien sowie nach der europaweiten Befragung 15 verschiedener NRENs wurde „Operational Network Security“ als unterrepräsentierter Trainingsbereich identifiziert. Dementsprechend entstand im Jahr 2020 ein Onlinekurs, der speziell auf die Bedürfnisse von System- und Netzwerkadministrierenden zugeschnitten war. In insgesamt 18 Webinaren wurden die Themen „Operating System Privacy & Security”, „Client Privacy & Security”, „Domain Name System (DNS) Protection” sowie „Distributet Denial of Service (DDoS) Protection” detailliert betrachtet.

In diesem Jahr wurde das Thema „Vulnerability Management“ in einem weiteren Trainingskurs für dieselbe Zielgruppe aufgearbeitet. Der dritte Kurs „IT Forensics for System Administrators“ wird ebenfalls online stattfinden. Er beginnt im November 2021 und endet im Januar 2022. Die Anmeldung zu den einzelnen Terminen ist kurzfristig möglich, die Aufzeichnungen und Materialien werden auf der DFN-CERT-Trainingswebseite zeitnah nach der Durchführung veröffentlicht. ◆

Alle im Rahmen des GN4-3-Projektes entwickelten Trainingsunterlagen sowie die aufgezeichneten Webinare finden Sie unter:
https://www.dfn-cert.de/en/Trainings.html
Zum Trainingskurs „IT Forensics for System Adminstrators“ können Sie sich hier anmelden:
https://events.geant.org/event/1073/
Weitere Informationen zum Kurs erhalten Sie hier:
https://learning.geant.org/it-forensics-for-system-administrators-new-for-2021-virtual-learning-with-experts/

Aufgrund der derzeitigen Pandemiesituation ist es möglich, wieder Onsite-Trainings zu organisieren und damit in einzelne Themenbereiche tiefer einzusteigen. Diesbezüglich bestehende Bedarfe können Sie direkt an das DFN-CERT melden unter: **veranstaltungen@dfn-cert.de**

ECSM 2021: Cyber Hero@Home

Erstmalig als Pilotprojekt im Jahr 2012 von der ENISA (European Network and Information Security Agency) gemeinsam mit acht teilnehmenden Ländern ausgerichtet und von der Europäischen Kommission unterstützt, beteiligt sich mittlerweile am European Cybersecurity Month (ECSM) europaweit eine Vielzahl von Hochschulen, Vereinen, Verbänden, Unternehmen, Behörden und Organisationen. In insgesamt 43 Ländern fanden im Jahr 2020 ECSM-Aktivitäten statt. Dabei wurde das Ziel, Teilnehmende aus ganz Europa zur Verbesserung der Cybersecurity – entsprechend dem Slogan „Cybersecurity is a shared responsibility" – zusammenzubringen, eindrucksvoll umgesetzt. Im vergangenen Jahr konnte die Anzahl der Nutzenden, die ECSM-Inhalte angeklickt haben, sogar auf 9,8 Millionen gesteigert und damit im Vergleich zum Vorjahr (2,7 Millionen) mehr als verdreifacht werden.

Foto: freepik

Der DFN-Verein beteiligt sich über das GN4-3-Projekt des europäischen Forschungsnetzes GÉANT regelmäßig am ECSM. Jedes Jahr stehen bestimmte Themengebiete der Cybersecurity im Fokus. Dieses Jahr konkretisierte GÉANT das ECSM-Motto zu „Cyber Hero @ Home" und spann damit das Motto aus 2020 „Become a Cyberhero" – das der Pandemiesituation und der aus ihr resultierenden veränderten Arbeitssituation geschuldet war – mit den Themen „Sicheres digitales Zuhause" und „Erste Hilfe für den digitalen Notfall" logisch weiter.

Mithilfe der Wochenschwerpunkte „Achtung Internetkriminalität", „Schützen Sie Ihr Netzwerk", „Schützen Sie Ihre Geräte" sowie „Schützen Sie Ihre Identität" wurde das zentrale Anliegen des ECSM im Aktionsmonat Oktober wirksam umgesetzt. Die dafür vorbereiteten Flyer wurden in 18 Sprachen übersetzt, um möglichst vielen Nutzenden den Zugang zu den Basisinformationen ohne etwaige sprachliche Hürden zu ermöglichen.

Einen Beitrag für die letzte Aktionswoche leistete das DFN-CERT gemeinsam mit einer Kollegin und einem Kollegen vom RUS-CERT und WWU-CERT. Der Artikel „Safe Videoconferencing" beleuchtet das Thema sowohl aus Sicht eines Teilnehmenden oder Ausrichtenden als auch von Administrationsseite aus. Die Initiative zu dem Beitrag entstand im EDUCV, dem Verbund operativer Informationssicherheitsteams deutscher Hochschulen, Lehr- und Forschungseinrichtungen.

Prinzipiell wird die Beteiligung aller Teilnehmer eines Forschungsnetzwerks am ECSM – sei es mit lokalen Aktionen oder globalen Angeboten sowie Veröffentlichungen – ausdrücklich begrüßt. Darum sei bereits an dieser Stelle darauf hingewiesen, dass der DFN-Verein auch im Oktober 2022 über GÉANT am ECSM teilnehmen wird. Schon Mitte kommenden Jahres soll das konkrete Thema feststehen, dann erfolgt auch der Aufruf zur Beteiligung – zeitnahe Informationen folgen. ◆

Den ECSM-Artikel zum Thema Videokonferenzen und viele weitere interessante Sicherheitsartikel finden Sie auf der Webseite des EDUCV unter:
https://www.educv.de/

MITARBEIT AN DIESER AUSGABE SICHERHEIT AKTUELL:

Christine Kahl (DFN-CERT)

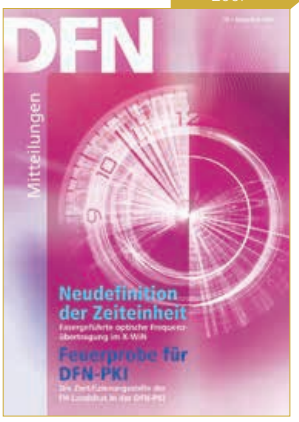
KONTAKT

Wenn Sie Fragen oder Kommentare zum Thema „Sicherheit im DFN" haben, schicken Sie bitte eine E-Mail an
sicherheit@dfn.de

DFM Mitteilungen I Ausgaben 69 - 80

70/2006 – DFN-AAI – kontrollierter Zugang zu geschützten Ressourcen
„Sesam öffne dich" hieß der Artikel: In Kooperation mit zahlreichen Wissenschaftseinrichtungen begann der DFN-Verein 2006 eine Infrastruktur für Authentifizierung und Autorisierung (AAI) aufzubauen, mit der die bisherigen Verfahren nicht nur extrem vereinfacht, sondern vor allem auch vereinheitlicht werden konnten. Damit sollte Nutzenden der Zugang zu geschützten Ressourcen ermöglicht werden. Heute ist die DFN-AAI eine der weltweit größten Föderationen, an der aktuell über 380 Heimateinrichtungen teilnehmen und deren Angehörige Zugriff auf weltweit über 4000 Dienste haben.

2007



2009

76/2009 – Jubiläum
25-jähriges Bestehen des DFN-Vereins: Conficker, Mebroot & Co wird der Garaus gemacht – als Reaktion auf die Schädlinge und neuen Bedrohungsszenarien baut das DFN-CERT seine Services inklusive der „Automatischen Warnmeldungen" in einem neuen Portal aus. Außerdem geht das GÉANT-Projekt GN3 an den Start.

2011

DFM Mitteilungen | Ausgaben 81 - 91

2013

86/2014 – Happy Birthday, DFN!
Mit 30 Lenzen ist der DFN-Verein auf dem Weg in die Cloud – und das per Superchannel durch das X-WiN: Mit dem neuen DFN-Terabit-Testbed erprobt der DFN-Verein Verbindungen mit einer Bandbreite von 1 Terabit/s. Ein erster erfolgreicher Test fand am 26. Februar 2014 auf einer Kernnetz-Strecke zwischen der Technischen Universität Dresden und der Bergakademie Freiberg statt.

2015

2017

91/2017 – Die Zukunft spricht IP
Der Dienst DFNFernsprechen steigt von ISDN auf rein IP-basierte Telekommunikation um. Die für Wissenschaft und Forschung konzipierten VoIP-Anschlussarten bilden die Grundlage für den Umstieg. Außerdem feiert die DFN-AAI ihren zehnten Geburtstag. Mit einer regen Nutzerschaft in den Heimateinrichtungen und in der internationalen Wissenschaftscommunity zählt sie zu den weltweit größten Föderationen. Mit der Initiative Eduroam off Campus (EoC) wird das Erfolgsmodell eduroam auch außerhalb des „Biotops Hochschule“ für reisende Forschende und Studierende zur Verfügung gestellt.

Proctored Exams – vom Piloten zur „neuen“ Normalität

Vor genau einem Jahr berichteten Mediendidaktiker Dr. Matthias Baume und die Studierenden Maximilian Frank und Lorenz Bayerlein von ihren Erfahrungen mit den Proctored Exams an der Technischen Universität München (TUM). Seitdem ist das Prüfungsformat gereift und hat sich etabliert. Um die Verwaltung von Online Proctored Exams auch im größeren Maßstab mit überschaubaren Kapazitäten und ohne größere Komplikationen zu organisieren, hat die TUM detaillierte Prüfungsverfahren für die Durchführung von beaufsichtigten Onlineprüfungen entwickelt.

Text: **Matthias Baume** und **Nina Muris-Wendt** (Technische Universität München, TUM)

Foto: Dabisik/photocase

Onlinebeaufsichtigte Prüfungen (Online Proctored Exams, Remote Invigilated Exams) erfahren seit einigen Jahren allgemein einen deutlichen Aufschwung in Bildungseinrichtungen und Unternehmen und auch im Hochschulkontext. Wichtigste Eigenschaft dieser Prüfungsform ist, dass die Prüflinge nicht nur auf dem Campus, sondern an jedem anderen Ort mit einer stabilen Internetverbindung ihren Test unter Aufsicht durchführen können. Die Gründe für den Einsatz dieses Formats sind vielfältig: Das Streben der Hochschulen nach Internationalisierung führt zur Notwendigkeit, Lerninhalte und Prüfungen für international verteilte Lernende anzubieten. Darüber hinaus ermöglichen Prüfungen von zu Hause eine Flexibilisierung und Individualisierung des Prüfens und schaffen für den Einzelnen häufig ein vertrautes Umfeld, verglichen mit den starren Rahmenbedingungen einer Prüfung im Hörsaal. Außerdem standen im Pandemiegeschehen der vergangenen Monate Prüfungen ohne aufwendigen Infektionsschutz zur Verfügung.

> Das Streben nach Internationalisierung führt zur Notwendigkeit, Prüfungen für international verteilte Lernende anzubieten.

Bereits ab dem Herbst 2018 hatte die Technische Universität München (TUM) aufgrund strategischer Überlegungen zur Internationalisierung das Projekt „Fernprüfungen“ gestartet mit dem Ziel, erste Erfahrungen mit Online Proctored Exams zu sammeln, geeignete Nutzungsszenarien auszuloten und Pilotanwendungen zu testen. Bis Ende 2019 wurden im Rahmen des Projektes auf der Basis einer breiten Literaturanalyse und einer Befragung von Prüfungsverantwortlichen in Europa bereits verschiedene Lösungen für Online Proctored Exams analysiert. Gleichzeitig wurden mithilfe von mehreren Pilotprüfungen grundlegende Prozesskonzepte und datenschutzrechtliche Rahmenbedingungen für die Nutzung erarbeitet.

VERGLEICH SOSE 2020, WISE 2020/21, SOSE 2021

	SoSe 2020	WiSe 2020/21	SoSe 2021
Anzahl der zentral verwalteten Fernprüfungen	**182**	**272**	**383**
davon E-Prüfungen (unbeaufs.)	49	55	108
davon Upload-Prüfungen	70	25	97
davon ZOOM-beaufsichtigte Prüfungen	15	27	18
davon Proctorio-Prüfungen	48	165	160
Teilnehmer*innen	**ca. 17 000**	**ca. 30 000**	**ca. 30 000**
größte Moodle-Prüfung (unbeaufs.)	1 139 TN	ca. 1 200 TN	1 037 TN
größte Proctorio-Prüfung (beaufs.)	1 060 TN	938 TN	1 268 TN

Bedingt durch die sich sehr dynamisch entwickelnde Pandemiesituation und die Schließung der Hörsäle an der TUM im März/April 2020 wurde ersichtlich, dass die Online Proctored Exams insbesondere für die zeitnahe Onlineverlagerung von geschlossenen (und damit betrugsanfälligen) Prüfungsformaten und Fragetypen (wie z. B. Multiple-Choice-Fragen, Kurztexte oder numerische Eingaben) einen wichtigen Beitrag zum Prüfungsgeschehen leisten könnten. Daher wurden ab dem Sommersemester 2020 auch Online Proctored Exams als eine mögliche Prüfungsvariante in der zentralen Lernplattform Moodle in Verbindung mit dem Anbieter Proctorio Deutschland ermöglicht.

Ein übergeordneter Prüfungsprozess für Online Proctored Exams an der TUM bündelt alle wichtigen Schritte

Um die Verwaltung von Online Proctored Exams auch im größeren Maßstab mit überschaubaren Kapazitäten und ohne größere Komplikationen zu organisieren, hat die TUM auf der Grundlage mehrerer Pilotversuche unterschiedlicher Größe detaillierte Prüfungsverfahren für die Durchführung von beaufsichtigten Onlineprüfungen entwickelt. Damit können alle notwendigen Schritte, Informationen und Aktivitäten des Prüfungsprozesses berücksichtigt werden, um Fehlerquellen bestmöglich zu minimieren.

Die wichtigsten Aspekte sind:

1. Information und Beratung: Insbesondere für Neueinsteiger in die beaufsichtigten Prüfungsformate ist es sehr wichtig, gute Informationen und Selbstlernangebote nutzen zu können.

2. Beantragung: Alle beaufsichtigten Prüfungsformate, die zentral verwaltet werden, müssen explizit über ein Onlineformular beantragt werden, um eine genaue und reibungslose Organisation zu bewerkstelligen. Die beantragten Prüfungen werden dann in einem gemeinsamen Prüfungskalender zusammengeführt.

3. Vorbereitung: Dozierende mit konkreter Prüfungsplanung erhalten einen spezifischen Prüfungskurs und bereiten darin sowohl ihre Demo-Prüfung (zum Ausprobieren) als auch die echte Prüfung vor. Die Prüfungskurse enthalten bereits alle notwendigen Informationen und Aktivitäten für die Prüflinge.

4. Beratung und Unterstützung: Während der Vorbereitung können Neueinsteiger von anderen Prüfungserfahrenen oder den TUM-Proctorio-Buddies Unterstützung bekommen. Auch individuelle Beratungen werden bei Bedarf organisiert.

5. Durchführung und Support: Während der Prüfung können sich die Prüflinge entweder an den Proctorio-Support, einen Prü-

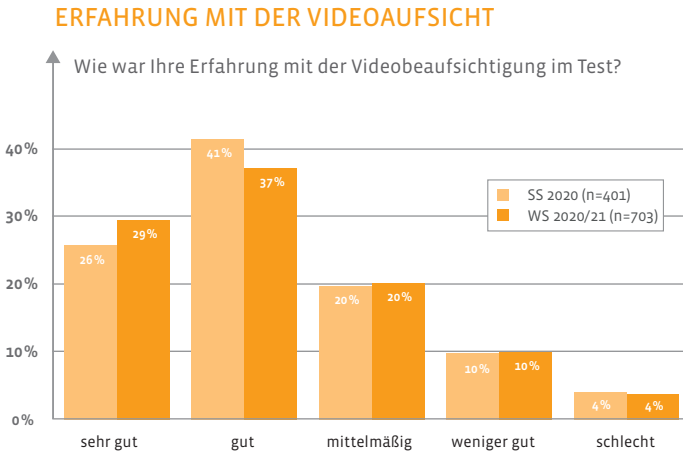


Abbildung 1

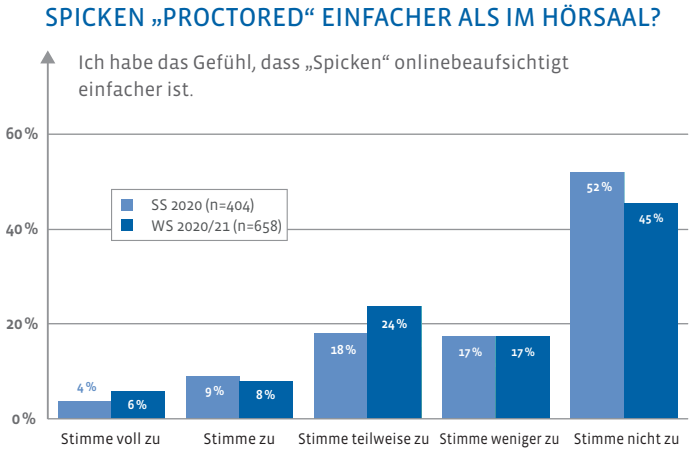


Abbildung 2

fungsverantwortlichen oder auch an die Proctorio-Buddies wenden, die häufig in einem Zoom-Meeting sofort erreichbar sind („Prüfungs-Standby“).

6. Abschluss: Nach der Prüfung sind Arbeiten wie das selektive Sichten der Prüfungsaufzeichnungen, das Löschen der sensiblen Daten und die Auswertung der Prüfungsergebnisse zu erledigen. Auch eine Prüfungseinsicht muss im weiteren Verlauf ermöglicht werden.

Was halten die Prüflinge von den onlinebeaufsichtigten Prüfungen?

In allen Proctorio-Prüfungskursen (das sind Moodle-Kurse, die speziell für Online Proctored Exams vorbereitet wurden) gibt es eine optionale Befragung der Prüflinge mittels Fragebogen. Diese kann direkt vor der Prüfung aktiviert werden. Die Befragung beinhaltet unterschiedliche Aspekte wie „Gemachte Erfahrungen“, „Wahrnehmung der Beaufsichtigung“, „Vorhandenes Informationsangebot“, „Technische Probleme“, „Datenschutz“, „Wunsch-Prüfungsvariante“ oder „Gesamteinschätzung der Prüfungsform“.

Nach mehreren evaluierten „Coronasemestern“ kann die Befragung Einblicke ermöglichen, welche Entwicklungen und Wahrnehmungsveränderungen sich bei Studierenden und Lehrenden bezüglich der beaufsichtigten Onlineprüfungen im Laufe der Zeit ergeben haben. Viele der international eingeschriebenen Studierenden haben noch nie in einem großen Hörsaal eine Vorlesung erlebt oder eine Prüfung geschrieben. Einige sind noch immer in ihren Heimatländern und kennen hauptsächlich Onlineveranstaltungen und Onlineprüfungen anstelle des über viele Jahre praktizierten Präsenzstudiums.

Um einen übergeordneten Blick auf die Entwicklung der Online Proctored Exams an der TUM zu erreichen, wurden die durchgeführten Befragungen einiger großer Prüfungskurse zusammengeführt und in Bezug gesetzt. Dadurch lassen sich mögliche Trends oder Meinungen der Studierenden deutlich seriöser einschätzen als die in den vergangenen Monaten häufig wahrgenommenen Einzelmeinungen. In den durchgeführten Befragungen wurden teils Rückläufe von bis zu 600 ausgefüllten Fragebögen in die Auswertung eingebracht.

> Insgesamt wird die Prüfungsform gut angenommen.

Die bisherigen Auswertungen über die vergangenen beiden Semester zeigen ein differenziertes Bild des Prüfungsgeschehens mit Online Proctored Exams an der TUM: Insgesamt wird die Prüfungsform gut angenommen und ein großer Teil der Studierenden bescheinigt gute bis sehr gute Erfahrungen (Abbildung 1).

Im Schnitt wählen ca. 95 Prozent der Teilnehmenden die Prüfungsvariante „zu Hause“. In den Hörsaal kommen auch bei sehr großen Prüfungen (400 – 1000 Teilnehmende) meist nur überschaubar viele Studierende. Diese lassen sich dann trotz Infektionsschutzbestimmungen gut handhaben.

Technische Probleme treten zwar vereinzelt auf, können aber von den an der TUM etablierten „Proctorio-Buddies“, den Prüfungsverantwortlichen oder dem zentralen TUM-Support in den allermeisten Fällen gelöst werden.

Im Gegensatz zu unbeaufsichtigten Prüfungen beurteilen viele Teilnehmende der beaufsichtigten Prüfungsformate die Möglichkeit zu betrügen als (deutlich) schwieriger als in vergleichbaren Prüfungen (Abbildung 2). Nur wenige sind der Meinung, dass „Spicken“ onlinebeaufsichtigt einfacher ist.

Beim Datenschutz ist möglicherweise eine Veränderung der Einstellung bei den Prüfungsteilnehmenden zu beobachten. Im letzten evaluierten Semester überwiegen für große Teile der Studierenden die Vor-

ÜBERWIEGEN DIE VORTEILE BEI GUTEM DATENSCHUTZ?

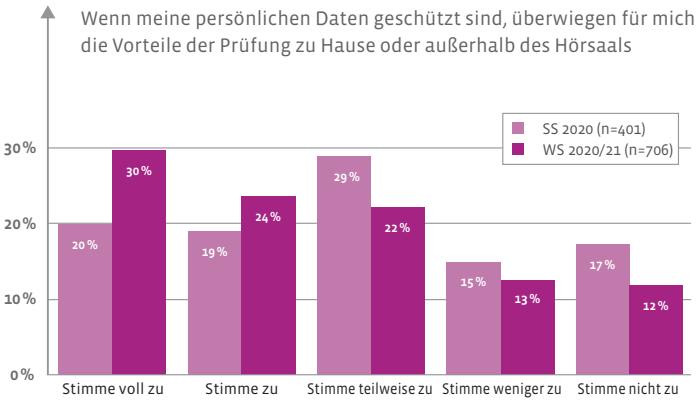


Abbildung 3

LIEBLINGSPRÜFUNGSFORM

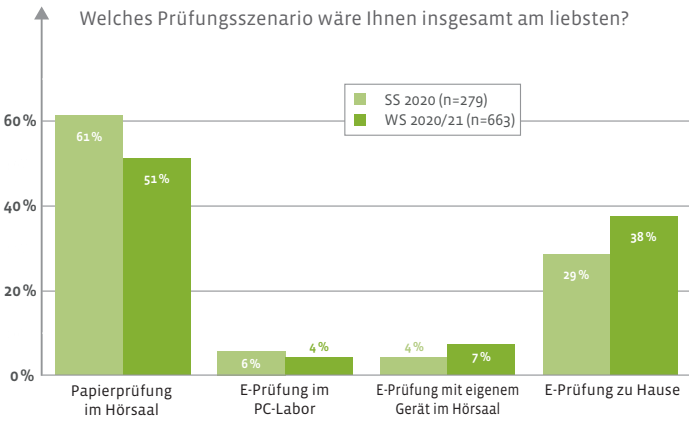


Abbildung 4

DAS SAGEN STUDIERENDE ZU DEN ONLINE-BEAUFSICHTIGTEN PRÜFUNGEN

PRO

„Man kann die Prüfung bequem von zu Hause aus schreiben. Man spart sich somit den Weg zur Prüfung und es ist auch stressfreier, wenn man am gleichen Tag noch eine andere Prüfung hat. Außerdem wird man normalerweise nicht von Geräuschen Anderer gestört. Ein weiterer Vorteil ist natürlich, dass man keinerlei Ansteckungsrisiko hat."

„Ich finde diese Prüfungsform sehr entspannt und für mich als Nicht-Münchner sehr angenehm. Ich spare mir aufwendige, kostspielige und lange Anfahrten und kann bequem von zu Hause meine Leistung erbringen."

CONTRA

„Es kommt keine Prüfungsatmosphäre auf, man fühlt sich sehr unter Druck gesetzt, auf keinen Fall irgendwohin zu schauen, damit es nicht als Spicken gewertet wird."

„Man muss sich von einem Programm beaufsichtigen lassen und weiß nicht, wo diese gesammelten Daten landen. Außerdem hat man neben der normalen Anspannung auch noch Angst, dass beispielsweise das Internet ausfällt oder irgendetwas am Laptop nicht funktioniert."

GESAMT

„Das Prüfungsformat an sich finde ich nicht schlecht. Allerdings kann ich nicht beurteilen, wie ich dieses Format in Kombination mit normalem Präsenzunterricht beurteilen würde. Mit ausschließlich Fernunterricht, wie ich ihn bisher nur kenne, würde ich dieses Format nicht noch einmal wählen, weil ich in der Prüfungsphase nicht mehr runterkomme, wenn alles in meinem Zimmer stattfindet."

„An sich bietet die Onlinebeaufsichtigung natürlich Vorteile, allerdings kann ich für meinen Teil sagen, dass ich es unglaublich schwer finde, zwei Stunden auf einen Bildschirm zu starren und sich dabei vollkommen zu konzentrieren."

„Es ist schwer, die E-Prüfung mit einer Hörsaalprüfung zu vergleichen, da ich ja noch nie eine Hörsaalprüfung hatte :D"

teile der Prüfung zu Hause. Das Bereitstellen von personenbezogenen Daten wird als weniger kritisch eingestuft (Abbildung 3).

Im zweiten evaluierten Semester geben insgesamt deutlich mehr Studierende als im Vorsemester an, als liebste Prüfungsform eine E-Prüfung zu Hause zu wählen (Abbildung 4).

> Der Wunsch nach reinen Hörsaalprüfungen scheint sich zu verringern.

Insgesamt sieht es danach aus, dass sich bei den Studierenden, die viele Monate hauptsächlich zu Hause gelernt haben, der Wunsch nach reinen Hörsaalprüfungen verringert und die Vorteile der Prüfung zu Hause im Laufe der Zeit im Vergleich zu den technischen und datenschutzrechtlichen Nachteilen deutlicher wahrgenommen werden. Letztlich wird der Studienmittelpunkt bei vielen Studierenden durch das Onlinestudium und die Onlineprüfungen auf die häuslichen Räumlichkeiten fokussiert.

Genauere Tendenzen werden die aktuell noch ausstehenden Auswertungen der Prüfungszeit des Sommersemesters 2021 klarer aufzeigen. Sollten sich jedoch aufgrund des anhaltenden Pandemiegeschehens die kommenden Semester weiter hauptsächlich

auf Onlinelehre und auch Onlineprüfungen beschränken, könnte dies aufgrund der in der Evaluation erhaltenen Einsichten deutliche Veränderungen in der Wahrnehmung von Studium und Lehre durch die Studierenden an der TUM haben.

Wie werden die Prüfungsverantwortlichen unterstützt und was ist ein Proctorio-Buddy?

Im Herbst 2020 nach der ersten „Corona-Prüfungszeit“ wurde ersichtlich, dass die onlinebeaufsichtigten Prüfungen mit Moodle und Proctorio gut angenommen werden. Jedoch war der zu leistende Vorbereitungs-, Betreuungs- und Organisationsaufwand für die ca. 50 im Sommer geplanten und durchgeführten Proctorio-Prüfungen um ein Vielfaches höher als die ursprünglich im Projekt „Fernprüfungen“ angedachten Personalkapazitäten hergaben. Um für die nahende nächste Prüfungszeit den Vorbereitungs- und Betreuungsaufwand besser zu verteilen, entstand die Idee, erfahrene Prüfungsverantwortliche zu gewinnen, um andere, noch unerfahrenere Kolleginnen und Kollegen zu unterstützen und auch während der Prüfungsdurchführung zu begleiten.

Da der Prüfungsprozess ein hohes Maß an Verantwortung und Vertrauen der Kollegen erfordert, sollte auch der Name für dieses Vorhaben die entsprechenden Rahmenqualitäten verinnerlichen. Darum fiel die Wahl auf: „Proctorio-Buddy“

Nachfolgend schildert Proctorio-Buddy Mizuki Ando ihre Erfahrungen aus mittlerweile zwei Semestern mit vielen unterschiedlichen, begleiteten Proctorio-Prüfungen.

Durch dick und dünn – mit den Proctorio-Buddies

Proctorio-Buddies sind erfahrene Dozierende, Prüfungsverantwortliche und Mitarbeitende der TUM, die sich weiterqualifiziert haben, um die onlinebeaufsichtigten Prüfungen von weniger erfahrenen Kolleginnen und Kollegen zu unterstützen und zu begleiten. Die Sachbearbeiterin für Studium und Lehre an der TUM-Fakultät für Sport- und Gesundheitswissenschaften Mizuki Ando berichtet, welche Erfahrungen sie als Proctorio-Buddy im Winter- und Sommersemester 2020/21 gemacht hat.

Text: **Mizuki Ando** (Technische Universität München, TUM)

Pädagogin mit Schwerpunkt Bildungsforschung und Bildungsmanagement: Proctorio-Buddy Mizuki Ando hat zum Erfolg der digitalen Prüfungsformate an der TUM beigetragen. *Foto: Andreas Heddergott*

Im Wintersemester 2020/2021 sollten pandemiebedingt alle Prüfungen unserer Fakultät auf digitale Formate umgestellt werden. Die Dozierenden standen plötzlich vor der großen Herausforderung, ihre bisherigen Papierklausuren auf der Onlineplattform Moodle mit der Browsererweiterung Proctorio zu realisieren. Das stresste alle Mitarbeitenden unserer Fakultät ungemein.

Ich war zuvor für die Organisation der Papierklausuren zuständig, als ich gefragt wurde, ob ich Lust hätte, im Support der Proctorio-Prüfungen mitzuwirken. Als ausgebildete Pädagogin mit Schwerpunkt Bildungsforschung und Bildungsmanagement brachte ich schon ein großes persönliches Interesse für die Digitalisierung von Lehr-Lern-Situationen mit und freute mich darauf, die verschiedenen Funktionen und Möglichkeiten von Moodle und Proctorio kennenzulernen. Zur Vorbereitung nahm ich an einer „MasterClass" für Proctorio-Buddies unserer Universität teil.

Nachdem in der Anfangszeit der Proctorio-Prüfungen etliche Fragen auftauchten, erstellten wir aus der Verwaltung einen Moodle-Kurs für die Dozierenden unserer Fakultät, um sie auf die digitalen Prüfungen vorzubereiten. Aus den vielen einzelnen Anfragen stellte ich außerdem FAQs mit allen nützlichen Links zusammen.

Eine Situation ist mir besonders in Erinnerung geblieben: Bei einer meiner ersten Prüfungen saß ich mit den Dozierenden in einem Zoom-Meeting, während die Studierenden die Prüfung schrieben. Als wir den Bearbeitungsstand der Studierenden überprüften, ist einem Dozenten aufgefallen, dass Moodle bestimmte Zeichenfolgen automatisch als Emoticon ausgibt. Darüber mussten wir herzhaft lachen, da in den Antworten lauter Smileys und Herzchen zu sehen waren. Zum Glück fand ich im Internet eine Lösung für das Problem und konnte die Einstellung schnell deaktivieren.

Die Aufgaben der Proctorio-Buddies sind vielfältig. Sie erstrecken sich von der Beratung der Prüfungsverantwortlichen zu den passenden Prüfungseinstellungen bis hin zum begleitenden „Prüfungs-Stand-by", falls während der Prüfung technische Probleme auftreten. Am wichtigsten ist der mehrstufige, vorbereitende Prüfungscheck vor den Klausuren, da dem geschulten Auge eines Proctorio-Buddys mehr mögliche Fehlerquellen auffallen.

Die Prüfung wird zu einer fest eingestellten Zeit freigeschaltet und wieder geschlossen. Nur für technische Probleme und Fragen sitze ich auf Stand-by in einem Zoom-Meeting oder an der Hotline entweder im Büro oder zu Hause. Bei einem parallel laufenden Zoom-Meeting kann ich mich während der Prüfung mit den anderen Aufsichtspersonen unterhalten. Gerade in der Anfangszeit hat das unheimlich geholfen, aufgeregte Kolleginnen und Kollegen während der Prüfung zu beruhigen und die Stimmung aufzulockern. Drei Prüfungen am Tag zu betreuen ist somit kein Problem im Gegensatz zu einer Prüfungsaufsicht im Hörsaal.

> Während der Prüfung werden Video- und Audioaufnahmen der Teilnehmenden erstellt.

Zuvor hatte ich schon des Öfteren klassische Prüfungsaufsichten im Hörsaal gemacht. Das fand ich nicht sonderlich spannend und jeder, der das schon einmal gemacht hat, kann das sicher bestätigen. Man geht durch die Reihen und wartet, bis die Zeit vergeht. Bei der „Aufsicht" einer Proctorio-Prüfung ist das anders. Während der Prüfung werden Video- und Audioaufnahmen der Teilnehmenden erstellt, um im Nachhinein mögliche Betrugsversuche zu untersuchen. Proctorio kann je nach Einstellung Verdachtsmomente markieren, die ich mir dann anschauen kann. So muss ich nicht die gesamte Aufzeichnung durchsuchen. Menschen dabei zu beobachten, wie sie auf ihren Bildschirm starren, ist schon irgendwie komisch.

Wenn Studierende nicht an einer fernbeaufsichtigten Prüfung von zu Hause aus teilnehmen wollen, gibt es alternativ die Möglichkeit, am eigenen Laptop die Prüfung in einem Hörsaal zu schreiben. Dabei werden keine Video- oder Audioaufnahmen gemacht, dafür gibt es aber eine Aufsichtsperson vor Ort. In der Regel müssen Studierende vor der tatsächlichen Prüfung eine DEMO-Prüfung absolvieren, um die Prüfungssituation an ihrem Endgerät auszutesten. Dabei sind dann auch Kamera und Mikrofon eingeschaltet, damit die Studierenden unter Realbedingungen testen können.

Einige Studierende haben sehr schlechte Internetverbindungen oder ganz alte Rechner. Und da können wir als Proctorio-Buddies auch nicht viel machen. Bei einer Prüfung zum Beispiel rief ein Student während der 90 Minuten ungefähr acht Mal an. Ständig hing die Seite. Mittlerweile erkannte ich schon seine Stimme. Bei einem der Anrufe kam dann aber sehr aufgeregt die Frage: „Muss ich Sie jetzt mit ins Bad nehmen, wenn ich auf Toilette gehen möchte?" Ich habe höflich verneint, musste aber hinterher ganz schön lachen. Die Toilettengänge wurden sogar schon unter den Dozierenden an unserer Fakultät stark diskutiert, da man nicht kontrollieren kann, ob jemand Spickzettel im Bad aufgehängt hat. Andererseits können wir natürlich niemandem verbieten, seine Notdurft zu stillen – vor allem nicht in so stressigen Situationen. Womit man sich alles auseinandersetzen muss als Proctorio-Buddy!

Ich fand es sehr spannend, die technischen Möglichkeiten, aber auch die Grenzen der onlinebeaufsichtigten Prüfungen kennenzulernen. Proctorio kann sehr viel, aber eben auch nicht alles. Dennoch das Optimum aus dieser Prüfungsart zu ziehen, hat mir unglaublich Spaß gemacht.

Auch der Austausch mit Mitarbeitenden anderer Fakultäten ist sehr bereichernd. Als Proctorio-Buddy bin ich mittlerweile an der Fakultät bekannt und bekomme viele Fragen weitergeleitet. Ich freue mich jedes Mal, wenn ich einem Studierenden oder Dozierenden helfen kann. Ich bin gespannt, wie sich digitale Prüfungsformate weiterentwickeln und den Universitätsalltag für Studierende und Dozierende verändern werden. ◆

Habemus Reform

Größte Reform des Urheberrechts seit zwei Jahrzehnten teilweise in Kraft getreten

Die seit Beginn des Gesetzgebungsverfahrens kontrovers und medienwirksam diskutierte EU-Urheberrechtsreform hat nun ihren vorläufigen Abschluss gefunden. Ende Mai passierte das „Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des Digitalen Binnenmarktes“ den Deutschen Bundestag.[1] Am 7. Juni 2021 traten weite Teile des Gesetzes in Kraft, die übrigen Regelungen folgen am 1. August 2021. Wir geben einen Überblick über die Neuregelungen und Änderungen, die Hochschulen besonders betreffen.

Text: **Justin Rennert** (Forschungsstelle Recht im DFN)

Foto: Marco2811/Adobe Stock

I. Hintergrund und Gesetzgebungsverfahren

Die Europäische Kommission hatte bereits im September 2016 im Rahmen ihrer Strategie für einen digitalen Binnenmarkt einen Vorschlag für eine „Richtlinie über das Urheberrecht im digitalen Binnenmarkt“ (kurz: DSM-RL) gemacht. Der Vorschlag war sodann Gegenstand intensiver Diskussionen im Europäischen Parlament und im Rat der Europäischen Union. Der aus Mitgliedern des Rates und des Parlamentes bestehende Vermittlungsausschuss musste einberufen werden und verhandelte ab Oktober 2018 bis zum Februar 2019. Erst am 26. März 2019, mehr als zwei Jahre nach der erstmaligen Befassung des Europäischen Parlamentes mit dem Gesetzesvorschlag, nahm das Parlament den Vorschlag schließlich an. Zwischenzeitlich gingen in Deutschland zehntausende Menschen auf die Straßen, um gegen das geplante Gesetz zu demonstrieren. Bei der bundesweit größten Demonstration im März 2019 in München meldete die Polizei eine Teilnehmerzahl von 40 000 Menschen.[2] Der Protest richtete sich vor allem gegen den geplanten Artikel 13 des Kommissionsvorschlags (in der schließlich verabschiedeten Richtlinie Artikel 17), der eine urheberrechtliche Verantwortlichkeit für Uploadplattformen wie YouTube vorsah, wenn auf ihren Plattformen urheberrechtlich geschützte Inhalte hochgeladen werden. Kritiker und Demonstrierende befürchteten als Konsequenz der Regelung ein sog. Overblocking von Inhalten durch die Uploadplattformen, mithin eine versehentliche Blockierung auch von Inhalten, die gar nicht urheberrechtlich geschützt sind. Dies würde die Ausübung des Rechtes auf freie Meinungsäußerung im Internet gefährden.

Mit dem Beschluss des Rates der Europäischen Union wurde die Richtlinie gleichwohl im April 2019 verabschiedet. Die Mitgliedstaaten hatten daraufhin bis zum 7. Juni 2021 Zeit, um die nicht unmittelbar in den Mitgliedstaaten geltende Richtlinie in bindendes nationales Recht umzusetzen. Die Bundesrepublik Deutschland setzte die Richtlinie nun in Gestalt des „Gesetzes zur Anpassung des Urheberrechtes an die Erfordernisse des Digitalen Binnenmarktes“ (nachfolgend: Umsetzungsgesetz) um. Das Gesetzespaket bringt Änderungen am Urheberrechtsgesetz (UrhG) und am Verwertungsgesellschaftengesetz (VGG) mit sich. Zudem wird mit dem Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) ein gänzlich neues, eigenständiges Gesetz geschaffen, das die urheberrechtliche Verantwortlichkeit von Uploadplattformen regelt und Artikel 17 der DSM-Richtlinie umsetzt. Nachfolgend stellen wir die Änderungen mit besonderem Hochschulbezug überblicksweise dar.

II. Überblick über die einzelnen Regelungen der Reform

Die Einzelregelungen des Umsetzungsgesetzes unterscheiden sich zunächst nach dem Datum ihres Inkrafttretens. Während viele Einzelregelungen bereits am 7. Juni 2021 in Kraft getreten sind, gilt das neue UrhDaG erst ab dem 1. August 2021. Zunächst wird hier auf die ab dem 7. Juni geltenden Vorschriften eingegangen, ein Überblick über das UrhDaG folgt zuletzt.

1. Text- und Data-Mining

Das Umsetzungsgesetz ergänzt die bisherigen Regelungen zum Text- und Data-Mining.[3] Seit März 2018 bestand in Gestalt des § 60d UrhG aF bereits eine gesetzliche Erlaubnis für das Text- und Data-Mining zu Zwecken der wissenschaftlichen Forschung. Beim Text- und Data-Mining werden große Mengen von Informationen, die in digitaler Form vorliegen (also z. B. Texte, Töne, Statistiken oder Bilder) mithilfe von Computern automatisiert ausgewertet. Dies geschieht in der Regel unter Verwendung von algorithmusbasierten Analyseverfahren und erlaubt die Aufdeckung von Strukturen, Trends und Korrelationen innerhalb großer Datensätze. So setzen beispielsweise Versicherungen das Data-Mining ein, um die Häufigkeit und die Wahrscheinlichkeit spezifischer Schadensfälle auszuwerten und so die Versicherungsprämie intelligent anpassen zu können.[4]

Der neue § 44b UrhG führt eine Erlaubnisnorm für das Text- und Data-Mining ein, bei der die Verfolgung von Forschungszwecken nicht mehr erforderlich ist. Gemäß § 44b UrhG ist es nunmehr für jedermann zulässig, Vervielfältigungen von rechtmäßig zugänglichen digitalen oder digitalisierten Werken für das Text- und Data-Mining zu erstellen. Die Daten dürfen beispielsweise auf einer Festplatte gespeichert und kopiert werden, um sie für die Bearbeitung durch den Algorithmus vorzubereiten. Es ist dabei stets Voraussetzung, dass die Werke bereits rechtmäßig zugänglich sind, d. h. beispielsweise frei im Internet verfügbar. Dem Inhaber des Urheberrechts an den in den Daten enthaltenen Werken bleibt allerdings die Möglichkeit, die Vervielfältigung zu untersagen, indem er einen Nutzungsvorbehalt erklärt. Dies kann beispielsweise in den AGB oder im Impressum der eigenen Webseite erfolgen.

Nach wie vor gibt es in Gestalt des § 60d UrhG jedoch eine Spezialregelung für Forschungsorganisationen. Für die wissenschaftliche Forschung erlaubt sie Vervielfältigungen der in den Daten enthaltenen Werke. Zusätzlich erlaubt sie jedoch, die Vervielfäl-

1 https://www.bundestag.de/dokumente/textarchiv/2021/kw20-de-urheberrecht-binnenmarkt-842596
2 https://www.sueddeutsche.de/muenchen/demo-muenchen-urheberrecht-1.4380419
3 Vertiefend Gielen: „Die neue urheberrechtliche Schranke zum Text- und Data-Mining“, DFN-Infobrief Recht 12/2019
4 Bitter in Hoeren/Sieber/Holznagel MMR-HdB, Teil 15.4 Big Data im Finanz- und Versicherungswesen Rn. 2

tigungen im Anschluss an die Aufbereitung für die Analyse einem abgegrenzten Personenkreis oder einzelnen Dritten auch öffentlich zugänglich zu machen. Privilegiert ist mithin die Bereitstellung der Daten innerhalb eines Teams von Forschenden (also z. B. im Intranet eines universitären Instituts) oder die Begutachtung von Forschungsergebnissen im Rahmen sog. Peer-Review-Verfahren.

Das Umsetzungsgesetz nimmt einige Änderungen an dieser Vorschrift vor. Die wohl wichtigste Änderung ist der Entfall der Vergütungspflicht. Vor dem 7. Juni hatte der Rechteinhaber gegen denjenigen, der Vervielfältigungen oder öffentliche Zugänglichmachungen im Rahmen des Text- oder Data-Mining vornahm, nach Gesetz einen Anspruch auf Zahlung einer angemessenen Vergütung. Nach neuer Rechtslage besteht ein solcher Anspruch nicht mehr. Der nationale Gesetzgeber hat sich sonach an die (unverbindliche) Vorgabe in Erwägungsgrund 17 Satz 2 der DSM-RL gehalten. Weiterhin entfällt die Pflicht, nach erfolgter Vervielfältigung für die einzelnen Werke innerhalb des Datenbestandes eine Quelle angeben zu müssen. Nach alter Rechtslage musste beispielsweise nach der Digitalisierung eines Datensatzes innerhalb der elektronischen Datei der Urheber genannt werden. Schließlich wurde die sehr strenge Beschränkung der Vorschrift auf nichtkommerzielle Nutzungszwecke aufgelockert. Bislang durften Forscher, die von der Erlaubnisnorm Gebrauch machen wollten, ausschließlich nichtkommerzielle Zwecke verfolgen, d. h. keine Gewinne erzielen. Nunmehr ist es ausreichend, wenn zwar Gewinne erzielt werden, diese allerdings sämtlich in die wissenschaftliche Forschung reinvestiert werden. Alternativ reicht es aus, wenn eine Forschungseinrichtung im Rahmen eines staatlich anerkannten Auftrages im öffentlichen Interesse tätig ist. Ist eine Einrichtung gänzlich kommerziell tätig, kann sie sich – wie schon beschrieben – allerdings auf den neuen § 44b UrhG berufen. Ausdrücklich sei an dieser Stelle erwähnt, dass die Spezialregelung für Forschungsorganisationen des § 60d UrhG den neuen § 44b UrhG in ihrem Anwendungsbereich nicht verdrängt. Für reine Vervielfältigungen (nicht jedoch für öffentliche Zugänglichmachungen) kann sich auch ein Forscher auf den § 44b UrhG berufen.[5] Insofern werden die Risiken für Forschende abgemildert, wenn nicht eindeutig geklärt ist, ob diese im rechtlichen Sinne kommerziell oder nichtkommerziell tätig sind.

2. Digitale Lehre

Eine geringfügige Änderung bewirkt das Umsetzungsgesetz im Rechtsregime zur digitalen Lehre. Nach § 60a UrhG aF war es schon bisher erlaubt, zur Veranschaulichung des Unterrichts und der Lehre an Bildungseinrichtungen zu nichtkommerziellen Zwecken bis zu 15 Prozent eines veröffentlichten Werkes zu vervielfältigen, zu verbreiten, öffentlich zugänglich zu machen oder in sonstiger Weise öffentlich wiederzugeben. Aus Sicht des europäischen Gesetzgebers bestand allerdings ein Mangel an Rechtssicherheit bei grenzüberschreitenden Nutzungen. Wenn also zum Beispiel eine italienische Studentin an einer deutschen Fernuniversität eingeschrieben war und von Italien online die Vorlesungen und Seminare verfolgte, bestand für die Universität die Gefahr, wegen einer Urheberrechtsverletzung nach italienischem Recht in Anspruch genommen zu werden.

Nunmehr schreibt der neue § 60a UrhG in einem neu eingefügten Absatz 3a vor, dass bei Nutzung eines Werkes zur Veranschaulichung des Unterrichts oder der Lehre an Bildungseinrichtungen nur das Recht des Staates am Sitz der Bildungseinrichtung anwendbar ist. Die deutsche Fernuniversität im oben genannten Beispiel kann sich nun also sicher sein, dass sich die urheberrechtliche Zulässigkeit der Werknutzung im Rahmen von Onlinevorlesungen ausschließlich nach deutschem Recht richtet.

3. Nicht verfügbare und vergriffene Werke

Erhebliche Änderungen bewirkt das Umsetzungsgesetz innerhalb der Vorschriften zu vergriffenen Werken. Vergriffene Werke sind solche, die nicht mehr im Handel erhältlich sind, für die aber gleichwohl noch urheberrechtlicher Schutz besteht. Oft befinden sich diese Werke im Bestand von Hochschulen, Bibliotheken, Museen oder Archiven. Im Zuge der fortschreitenden Digitalisierung dieser Einrichtungen gab und gibt es das erhebliche Bedürfnis, auch vergriffene Werke digital (insb. online) verfügbar zu machen, um das darin enthaltene Wissen nicht in Vergessenheit geraten zu lassen. Problematisch ist dabei, dass die Digitalisierung von Werken in die Rechte des Urhebers eingreift und deswegen eigentlich die Einholung einer Nutzungserlaubnis erforderlich wäre.[6] Bei vergriffenen Werken gestaltet sich das Ausfindigmachen des Rechteinhabers zur Einholung der Nutzungserlaubnis allerdings häufig schwierig. Beispielsweise kann es sein, dass der Verlag, der das Werk veröffentlicht hat, gar nicht mehr existiert oder die Anschrift des Urhebers inzwischen unauffindbar ist.

Seit 2014 existierten daher in Deutschland mit den §§ 51 ff. VGG aF Regelungen, die mittels einer gesetzlichen Vermutungsregelung de facto ermöglichten, dass Verwertungsgesellschaften Nutzungsrechte an Printwerken einräumen, obwohl ihnen die Befugnis hierzu vom Rechtsinhaber nicht übertragen wurde. Bibliotheken oder Archive mussten sich seither statt mit einer Vielzahl potenziell unauffindbarer Rechtsinhaber nur mit einigen wenigen Verwertungsgesellschaften auseinandersetzen.

5 amtl. Begr. BT-Drs. S. 110

6 Vertiefend Tiessen: „Vergriffen heißt nicht vergessen“, DFN-Infobrief Recht 01/2020

Dieses Rechtsregime weitet das Umsetzungsgesetz nunmehr erheblich aus. Zunächst fällt die Beschränkung auf Printwerke weg. Gemäß dem neu eingefügten § 52b VGG ist nun jede Werkart (insb. Film- und Musikwerke) erfasst, ohne Rücksicht darauf, ob das Werk in einer Printpublikation veröffentlicht wurde. So könnten z. B. in Zukunft auch für Werke, die auf Videokassetten im veralteten Format gespeichert sind, Nutzungsrechte vereinfacht erteilt werden. Gleiches gilt für Fotografien, die im Analogformat vorliegen, oder für auf CDs oder Schallplatten gespeicherte Musik- oder Tonaufnahmen.

Weiterhin ersetzt das Umsetzungsgesetz den Begriff der „vergriffenen Werke" durch den Begriff der „nicht verfügbaren Werke". Nicht verfügbar ist ein Werk nach dem neuen § 52b Abs. 1 VGG, wenn es der Allgemeinheit auf keinem üblichen Vertriebsweg in einer vollständigen Fassung angeboten wird. Darunter fallen zunächst alle Werke, die schon nach alter Rechtslage als vergriffen galten, d. h. nicht mehr im Handel verfügbar sind. Zudem sind unter der neuen Terminologie aber nun auch Werke erfasst, die zwar irgendwann einmal durch den Urheber veröffentlicht wurden, aber noch nie im Handel erhältlich waren. Hat die jeweilige Einrichtung mit einem vertretbaren Aufwand ohne Erfolg versucht, ein Angebot des Werkes am Markt aufzufinden, so wird unwiderleglich vermutet, dass dieses vergriffen ist.

Nach wie vor besteht ein Widerspruchsrecht des Rechtsinhabers. Der Widerspruch führt zur Unwirksamkeit der Rechtseinräumung. Anders als bisher muss der Widerspruch nicht gegenüber dem Deutschen Patent- und Markenamt (DPMA), sondern gegenüber dem Amt der Europäischen Union für geistiges Eigentum (EUIPO) erfolgen. In diesem Zuge wird auch das bisher gem. § 52 VGG aF beim DPMA geführte Register vergriffener Werke Ende 2025 geschlossen. Auf einem neuen europaweiten Onlineinformationsportal des EUIPO müssen Verwertungsgesellschaften gem. § 52 Abs. 1 S. 1 Nr. 4 VGG nun sechs Monate vor Wirksamwerden der Rechtseinräumung über das betreffende Werk und die Rechtseinräumung an selbigem informieren. Rechtsinhaber können so ihr Werk identifizieren und der Rechtseinräumung im Anschluss ggf. widersprechen oder Ansprüche auf Zahlung von anteiligen Einnahmen geltend machen.

Der neue § 52 VGG weist lediglich Kulturerbeeinrichtungen (also Bibliotheken, Museen und Archive sowie Einrichtungen im Bereich des Tonerbes) als mögliche Profiteure der vereinfachten Nutzungsrechtseinräumung aus. Unter der bisherigen Rechtslage waren Bildungseinrichtungen wie Hochschulen im Gesetz ausdrücklich genannt. Vieles spricht jedoch dafür, dass Hochschulen auch nach wie vor erfasst sind, da diese in der Regel über eingegliederte Bibliotheken oder zumindest Archive verfügen.

Für Hochschulangestellte in Bibliotheken oder Archiven ergibt sich im Ergebnis durch das Umsetzungsgesetz folgende Regel: Haben sie mit einigem Aufwand den Markt nach Angeboten des jeweiligen Werks durchsucht, so dürfen sie sich bis zu einem etwaigen Widerspruch des Rechtsinhabers sicher sein, dass die Verwertungsgesellschaft die richtige Stelle für die Rechtseinräumung ist.

4. Verantwortlichkeit von Uploadplattformen

Im Januar 2020 informierten wir bereits umfassend über die durch die DSM-RL vorgesehene urheberrechtliche Verantwortlichkeit von Uploadplattformen. Insbesondere setzten wir uns mit der Problematik von Uploadfiltern auseinander.[7] An dieser Stelle soll zunächst ein kurzer Überblick über die Umsetzung der europäischen Regelungen durch das UrhDaG erfolgen. Eine detaillierte Aus- und Bewertung der neuen Vorschriften werden wir im Infobrief vornehmen, nachdem das Gesetz am 1. August 2021 in Kraft getreten ist und die praktischen Auswirkungen spürbar geworden sind. Zwar sind Hochschulen, sofern sie selbst Uploadplattformen betreiben (beispielsweise ein universitätseigenes Videoportal, auf das Studierende Inhalte hochladen können), gem. Art. 2 Nr. 6 der DSM-RL (umgesetzt in § 3 Nr. 2 UrhDaG) von den Änderungen der DSM-RL ausgenommen, gleichwohl sind sie wie jeder andere Internetnutzer von den Regelungen im praktischen Umgang mit dem Internet betroffen (beispielsweise bei der Nutzung der Plattform „YouTube" durch die Hochschule zu Zwecken der Öffentlichkeitsarbeit).

Mit Inkrafttreten des UrhDaG am 1. August 2021 werden Uploadplattformen wie YouTube (nach der Terminologie des UrhDaG „Diensteanbieter") für von Nutzern hochgeladene Inhalte gem. § 1 Abs. 1 UrhDaG verantwortlich sein. Sie können dementsprechend künftig bei einer Verletzung des Urheberrechts von Rechtsinhabern auf Unterlassung und Schadensersatz in Anspruch genommen werden. Bisher war eine Inanspruchnahme nur möglich, wenn sie Kenntnis von der Rechtsverletzung hatten und trotzdem untätig geblieben sind (d. h. die betreffenden Inhalte nicht von ihrer Plattform entfernt haben).

Die Befreiung der Diensteanbieter von der Möglichkeit zur Inanspruchnahme ist für Diensteanbieter zwar nach wie vor möglich, aber an weitaus strengere Voraussetzungen geknüpft als bisher. Insbesondere müssen sich Diensteanbieter nun laufend darum bemühen, die vertraglichen Nutzungsrechte für geschützte Inhalte zu erwerben. Der nationale Gesetzgeber sieht vor, dass „bestmögliche Anstrengungen" zum Erwerb der Nutzungsrechte unternommen werden müssen. Insofern ist die Formulierung gegenüber der deutschen Fassung der DSM-RL („alle Anstrengungen") abgemildert. Zu den bestmöglichen Anstrengungen gehört insbesondere

7 Gielen: „First Rule: You Do Not Talk About Uploadfilter", DFN-Infobrief Recht 01/2020

die Zusammenarbeit mit Verwertungsgesellschaften, die in der Regel Urheberrechte einer Mehrzahl von Urhebern wahrnehmen.

Weiterhin müssen Diensteanbieter Inhalte umgehend blockieren, sobald der Rechtsinhaber dies verlangt. Unter gewissen Voraussetzungen müssen sie auch dafür sorgen, dass die geschützten Inhalte in Zukunft nicht mehr hochgeladen werden.

Der dadurch entstehenden Gefahr des Overblockings von Inhalten durch den Einsatz automatisierter Identifikations- und Blockierungsverfahren (insb. durch den Einsatz von Uploadfiltern) versucht der deutsche Gesetzgeber auf zweierlei Weise beizukommen: Erstens wird durch Einführung eines Beschwerdeverfahrens sowohl für Nutzer als auch für Rechtsinhaber die Möglichkeit geschaffen, sich (auf Nutzerseite) gegen die Blockierung und (auf Rechtsinhaberseite) gegen die öffentliche Wiedergabe zur Wehr zu setzen. Zweitens werden durch das neu eingeführte Rechtsinstrument der mutmaßlich erlaubten Nutzungen bestimmte Fälle geschaffen, in denen die Diensteanbieter die Inhalte trotz Blockierungsverlangen der Rechtsinhaber zunächst nicht blockieren müssen. Erst nach Einlegung einer Beschwerde durch den Rechtsinhaber kann es dann zur Löschung kommen. Zu diesen Fällen gehört insbesondere die nichtkommerzielle Nutzung kleinster Auszüge von Werken (beispielsweise im Rahmen von Parodien oder Internet-Memes). Wie wirksam die genannten Rechtsinstrumente sind, kann gegenwärtig noch nicht gesagt werden. Ob sie einem aggressiven Overblocking vorbeugen, muss Gegenstand einer Evaluierung nach Inkrafttreten des Gesetzes sein. Jedenfalls hat der deutsche Gesetzgeber den Spielraum der DSM-RL genutzt, die lediglich abstrakt vorgab, dass die neu eingeführte Verantwortlichkeit von Diensteanbietern nicht dazu führen darf, dass Inhalte, die nicht gegen das Urheberrecht verstoßen, blockiert werden.

Bemerkenswert ist schließlich der durch § 4 Abs. 3 UrhDaG vorgesehene Direktvergütungsanspruch von Urhebern gegen den Diensteanbieter. Gerade bei komplexen digitalen Verwertungen gewährleistet das Urhebervertragsrecht nicht automatisch, dass Kreative auch an den Einnahmen beteiligt werden, die verwertende Unternehmen (z. B. Musikverlage) mit der Lizenzierung an Diensteanbieter erzielen. Hat der Urheber das Recht der öffentlichen Wiedergabe einem Dritten eingeräumt, so hat der Diensteanbieter für die Nutzung des Werkes dem Urheber künftig gleichwohl eine angemessene Vergütung zu zahlen. Diensteanbieter können also in die Situation geraten, dass sie dem Dritten (zum Beispiel einem Musikverlag) zunächst Lizenzgebühren für die Einräumung von Nutzungsrechten bezahlen und zusätzlich dem Urheber direkt eine angemessene Vergütung zahlen müssen. Nach alter Rechtslage genügte die Entrichtung von Lizenzgebühren an den Dritten.

III. Fazit und Auswirkungen für Hochschulen

Die praktischen Auswirkungen der nationalen Umsetzung der DSM-RL durch das Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des Digitalen Binnenmarktes sind immens. Viele Regelungen betreffen Hochschulen unmittelbar. Dazu gehören insbesondere die geänderten Vorschriften zum Text- und Data-Mining und zu nicht verfügbaren Werken. Hier sind sogar kombinierte Anwendungsmöglichkeiten denkbar. Beispielsweise kann es sein, dass eine Hochschulbibliothek ihren Bestand an nicht verfügbaren Werken digitalisieren und dabei gleichzeitig gewisse Muster innerhalb dieses Bestandes erkennen möchte. Die reine Vervielfältigung kann ihr in so einem Fall nach § 60d UrhG erlaubt sein. Für eine anschließende Zugänglichmachung des Bestandes gegenüber der Allgemeinheit kann sie sich für die vereinfachte Lizenzierung an die zuständige Verwertungsgesellschaft wenden. Sofern kein unmittelbarer Hochschulbezug gegeben ist, besteht er jedenfalls mittelbar. Die Vorschriften des UrhDaG zur Verantwortlichkeit von Uploadplattformen betreffen praktisch jeden Nutzer dieser Plattformen. Immer öfter verwenden auch Universitäten oder universitätseigene Institute Plattformen wie YouTube zur Öffentlichkeitsarbeit oder gar zur Vermittlung von Wissen. Eine hochschulinterne Auseinandersetzung mit den Änderungen durch das Umsetzungsgesetz bietet Chancen und kann insbesondere neue Möglichkeiten der Benutzung geschützter Werke für wissenschaftliche Zwecke aufzeigen. ◆

Lass' das mal die Forscher machen!

Zur neuesten Änderung des Netzwerkdurchsetzungsgesetzes

Straftaten im Netz sind längst keine Seltenheit mehr. Besonders die Verbreitung von Hassinhalten hat in den letzten Jahren stark zugenommen. Mit dem Netzwerkdurchsetzungsgesetz (NetzDG) startete der deutsche Gesetzgeber eine erste Offensive gegen Hass im Netz.[1] Mit der aktuellen Änderung dieses Gesetzes ergeben sich für Forschungseinrichtungen neue Möglichkeiten zur Analyse der Maßnahmen der Anbieter sozialer Netzwerke gegen strafbare Inhalte.

Text: **Owen Mc Grath** (Forschungsstelle Recht im DFN)

Foto: Lisa-S/Shutterstock

I. Grundlagen

Erstmalig in Kraft getreten im Oktober 2017 regelt das NetzDG Ansprüche und Pflichten sowohl von Anbietern sozialer Netzwerke als auch Opfern und Tätern von Hasskriminalität und anderer Straftaten im Netz. So soll der zu beobachtenden Zunahme dieser Delikte in den letzten Jahren entgegengetreten werden.

Besonders stark wurde der Ruf nach einem solchen Gesetz erstmals im Zuge der vielen Debatten um Fake News[2] im Rahmen der US-Wahlen im Jahr 2016. Die hierdurch infrage gestellte Regulierung von rechtswidrigen Beiträgen auf sozialen Netzwerken bestätigte sich zwar nicht bei allen Netzwerken. Manch großes Unternehmen ging jedoch bisher unzureichend auf beleidigende Kommentare und strafbare Inhalte ein. Auch in Deutschland hat sich in den letzten Jahren gezeigt, welch starken Nährboden Hassinhalte im Netz für tätliche Angriffe bieten. Der Anschlag in Hanau im vergangenen Jahr, die Attentate im Umfeld der Synagoge in Halle sowie die Ermordung des Kasseler Regierungspräsidenten Walter Lübcke sind die tragische Spitze des Eisberges.

Das NetzDG betrifft nur solche Netzwerke, die im Inland mindestens zwei Millionen registrierte Benutzer haben (§ 1 Abs. 2 NetzDG). So werden kleinere Netzwerke nicht mit der Vorgabe der komplexen Beschwerdebearbeitung belastet. Das Gesetz verlangt von den Anbietern sozialer Netzwerke die zügige Bearbeitung von Nutzerbeschwerden, welche sich auf rechtswidrige Inhalte beziehen (§ 3 NetzDG). Bei über 100 Beschwerden in einem Jahr sind die Anbieter darüber hinaus verpflichtet, halbjährlich einen Bericht über den Umgang mit Beschwerden zu verfassen (§ 2 NetzDG). Bei Missachtung dieser Vorgaben drohen Bußgelder (§ 4 NetzDG).

II. Kritik

Seit dem ersten Entwurf sieht sich das NetzDG starker Kritik ausgesetzt. Dem Ruf nach Regulierung der in sozialen Medien geteilten Inhalte steht die Angst vor Zensur und Meinungsmanipulation gegenüber. Allem voran wird bemängelt, dass das Gesetz die grundgesetzlich verankerte Meinungsfreiheit (Art. 5 Abs. 1 Grundgesetz (GG)) über ein hinnehmbares Maß hinaus einschränken würde. Nach § 3 NetzDG sind Anbieter sozialer Netzwerke verpflichtet, ein passendes Beschwerdeverfahren für rechtswidrige Inhalte einzurichten und entsprechend auf die Beschwerden der Nutzer zu reagieren. Für den Fall, dass beispielsweise ein Beitrag mit offensichtlich rechtswidrigem Inhalt vorliegt, ist dieser innerhalb von 24 Stunden zu entfernen oder der Zugang zu diesem zu sperren. Handelt der Anbieter eines sozialen Netzwerkes nicht entsprechend diesen Vorgaben, drohen hohe Bußgelder.

Das Bundesverfassungsgericht definiert eine Meinung über „das Element der Stellungnahme, des Dafürhaltens, des Meinens im Rahmen einer geistigen Auseinandersetzung“[3]. Beiträge in sozialen Medien stellen danach regelmäßig eine Meinung des Verfassers dar. Der Schutz der Meinungsfreiheit endet dort, wo die Meinung zur reinen Schmähkritik verkommt. Hassinhalten ist eben dieser Vorwurf regelmäßig zu machen. Die staatliche Beeinträchtigung von Beiträgen aus dem Netz, welche eine Meinung darstellen, bedeutet allerdings einen Eingriff in die Meinungsfreiheit. Diese ist nicht schrankenlos gewährt. Sie kann durch Gesetz (Art. 5 Abs. 2 GG) oder kollidierende Verfassungsgüter eingeschränkt werden. In diesem Zusammenhang ist allerdings auf die Verhältnismäßigkeit der Einschränkung zu achten. Im konkreten Fall bedeutet das, dass der Schutz vor Straftaten im Netz und das Persönlichkeitsrecht der betroffenen Personen dem bedrohten Rechtsgut der Meinungsfreiheit gegenüberzustellen und abzuwägen ist.

Eine unverhältnismäßige Einschränkung der Meinungsfreiheit kann besonders das sogenannte Overblocking[4] bedeuten. Hierbei werden mehr Inhalte gesperrt und gelöscht, als es nötig wäre – potenziell auch rechtmäßige Beiträge. Diese Überkorrektur aufseiten der Anbieter sozialer Netzwerke schützt sie selbst vor drohenden Bußgeldern. Dass dabei auch Beiträge gelöscht werden, die nicht als rechtswidrig einzuordnen sind, wird durch das NetzDG nicht unmittelbar unterbunden. So setzt das NetzDG einen asymmetrischen Anreiz zum Overblocking.

In Fällen des Overblockings wird regelmäßig die Meinungsfreiheit der Beitragsverfasser beschränkt, ohne eine ausreichende Rechtfertigung als Gegengewicht zu haben. Eine trennscharfe Unterscheidung zwischen Beiträgen, welche trotz Eingriff in die Meinungsfreiheit zu löschen sind, und solchen Inhalten, bei denen ein Eingriff in die Meinungsfreiheit nicht hinzunehmen ist, ist nicht einfach zu treffen. Die Bußgeldbewehrung unzureichender Bearbeitungen von Beschwerden und die mitunter knappe Handlungsfrist vermögen in solchen Grenzfällen schnell zur Löschung oder Sperrung der Beiträge zu führen, obwohl dies nicht im Einklang mit der Meinungsfreiheit der Betroffenen steht. Die gleichen Sorgen ergeben sich auch dann, wenn Anbieter sozialer Netzwerke zur Vereinfachung des Prozesses und zur Beschwerdeprävention automatisierte Verfahren zur Erkennung und Entfernung rechtswidriger Inhalte einsetzen.

1 S. zu einer potenziellen europäischen Lösung: Gielen, Digital Services Act: Das Plattformgrundgesetz?, Infobrief Recht 3/2021.
2 Auch zu Coronazeiten ein großes Thema: Tiessen, No news is better news, Infobrief Recht 7/2020.
3 BVerfGE 61, 1, 8.
4 Ähnlich bei Urherberrechtsverstößen: Gielen, First Rule: You Do Not Talk About Uploadfilter! Infobrief Recht 1/2020.

Neben dem befürchteten Overblocking sehen viele auch gerade die mit der Aufgabenübertragung der Regulierung einhergehende Machtkonzentration bei den Anbietern sozialer Netzwerke als problematisch an.

III. Reaktion des Gesetzgebers

Die jüngst im Bundestag beschlossene Gesetzesänderung des NetzDG hat vor allem den Anspruch, der Sorge vor Overblocking und der zunehmenden Machtkonzentration von Anbietern sozialer Netzwerke entgegenzutreten. Bewältigt werden soll das unter anderem durch ein Gegenvorstellungsverfahren, in welchem die Teilnahme der durch eine Löschung betroffenen Nutzer und der sich beschwerenden Nutzer ermöglicht wird. So besteht für das einschlägige Netzwerk eine weitere, zumindest mittelbare Hürde zur pauschalen Entfernung von Inhalten, welche nicht schlichtweg als rechtswidrig eingeordnet werden können. Ferner sollen Schlichtungsstellen etabliert werden und die Aufsicht über die Verfahren fällt zukünftig dem Bundesamt für Justiz zu.

Für wissenschaftliche Einrichtungen ist der § 5a NetzDG die wesentlich bedeutendere Neuerung. Mit diesem steht Forschern ein Anspruch auf Auskunft über „den Einsatz und die konkrete Wirkweise von Verfahren zur automatisierten Erkennung von Inhalten, die entfernt oder gesperrt werden sollen, insbesondere zu Art und Umfang eingesetzter Technologien und den Zwecken, Kriterien und Parametern für deren Programmierung sowie zu den eingesetzten Daten“ und „die Verbreitung von Inhalten, die Gegenstand von Beschwerden über rechtswidrige Inhalte waren oder die vom Anbieter entfernt oder gesperrt worden sind, insbesondere die entsprechenden Inhalte sowie Informationen darüber, welche Nutzer in welcher Weise mit den Inhalten interagiert haben“ gegen die Anbieter sozialer Netzwerke zu.

Wenn Forscher diesen Anspruch geltend machen wollen, muss ein Schutzkonzept vorgelegt werden, welches unter anderem die Absichten und ein berechtigtes Interesse der Untersuchung sowie eine Übersicht der datenschützenden Maßnahmen darlegt. Die Auskunft kann verweigert werden, wenn aufseiten des Netzwerks oder der von dem Verfahren betroffenen Personen ein schutzwürdiges Interesse das öffentliche Interesse an der Erforschung des Falles überwiegt.[5] Ferner hat der Anbieter eines sozialen Netzwerkes Anspruch auf Ersatz der ihm durch die Erteilung der Auskunft entstehenden Kosten gegen den Forscher. Diese Kosten sind allerdings im Regelfall auf 5.000 € begrenzt.

Ziel der Vorschrift ist die Schaffung von Transparenz über die Arbeitsweise von Anbietern sozialer Netzwerke. So soll die Bearbeitung von Beschwerden und die eventuelle Löschung von Beiträgen für die Öffentlichkeit nachvollziehbar werden und mittelbar ein pauschaler Umgang mit Löschungen verhindert werden. Starke Relevanz hat dieses Vorhaben bei komplexen automatisierten Verfahren zur Entfernung von Hassinhalten. Diese Verfahren erschließen sich regelmäßig kaum für Laien und der allgemein zugängliche Transparenzbericht (§ 2 NetzDG) schafft zumeist auch keine Klarheit. Forschungseinrichtungen haben in der Theorie durch die zu erhaltenden Auskünfte und die eigene Expertise einen besseren und vor allem vertiefteren Zugang zu der infrage stehenden Thematik. Die erarbeiteten Ergebnisse stehen dann der Öffentlichkeit und der weiteren wissenschaftlichen Auseinandersetzung zur Verfügung.

IV. Fazit und Auswirkungen für wissenschaftliche Einrichtungen

Die Themen Hasskriminalität im Netz und die Macht sozialer Medien sind aktueller denn je. Mit dem neuen § 5a NetzDG haben Forscher die Möglichkeit, einen Beitrag zur Bekämpfung beider Problematiken zu leisten. Ob die Einbindung der Wissenschaft in die Bewältigung von strafbaren Netzinhalten tatsächlich für mehr Transparenz und im Ergebnis für eine differenzierte Auseinandersetzung mit möglicherweise rechtwidrigen Beiträgen aufseiten der sozialen Netzwerke sorgt oder ob die Hürden für die wissenschaftliche Beteiligung zu hoch gesetzt sind, wird sich zeigen. ◆

5 Zum Schutz des Geschäftsgeheimnisses in diesem Zusammenhang: Gielen, Digital Services Act: Das Plattformgrundgesetz?, Infobrief Recht 3/2021.

DFN Live: Wissen teilen, Erfahrungen weitergeben

Der DFN-Verein lebt von der Expertise und Erfahrung seiner Mitglieder und Teilnehmer am Deutschen Forschungsnetz. Mit zahlreichen Veranstaltungen, Tutorien, Tagungen und Workshops bietet der DFN-Verein ein Forum für einen lebendigen Dialog und Wissenstransfer. Gerade in Covid-19-Zeiten erhält der Austausch innerhalb der Netz-Community – egal ob digital oder physisch – eine besondere Bedeutung. In welchem Format die jeweiligen Veranstaltungen abhängig vom künftigen Pandemiegeschehen stattfinden, geben wir rechtzeitig über unsere etablierten Informationskanäle bekannt.

82. DFN-Mitgliederversammlung

Aufgrund des Pandemiegeschehens fand die 82. Mitgliederversammlung am Dienstag, 8. Juni 2021, erneut virtuell statt. Mitgliedsvertretende aus ganz Deutschland nahmen teil. Auf der Tagesordnung standen wieder viele spannende Themen. So berichtete der Vorstand über die Projektbeteiligungen des DFN-Vereins, unter anderem über das Projekt GN4-3, das ab Januar 2023 nahtlos als GN5 weitergeführt werden soll, sowie über die Beteiligung an EOSC Future. Ein weiterer Punkt war auch der Aufbau des Dienstes Security Operations. Prävention, Detektion und Reaktion werden im neuen DFN-Dienst intensiv miteinander verzahnt.

Weitere Themen waren unter anderem die künftige Entwicklung des Dienstes DFNconf sowie der aktuelle Stand von edu-ID.

TERMIN

Die 83. Mitgliederversammlung findet am **Mittwoch, 15.12.2021**, online statt.

29. DFN-Konferenz „Sicherheit in vernetzten Systemen“

Im Auftrag des DFN-Vereins veranstaltet das DFN-CERT jedes Jahr die Konferenz „Sicherheit in vernetzten Systemen“. Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung, einer großen Vielfalt an Beiträgen und Diskussionen sowie durchschnittlich 350 Teilnehmenden hat sich die DFN-Konferenz als eine der größten deutschen Tagungen für Informationssicherheit etabliert.

TERMIN

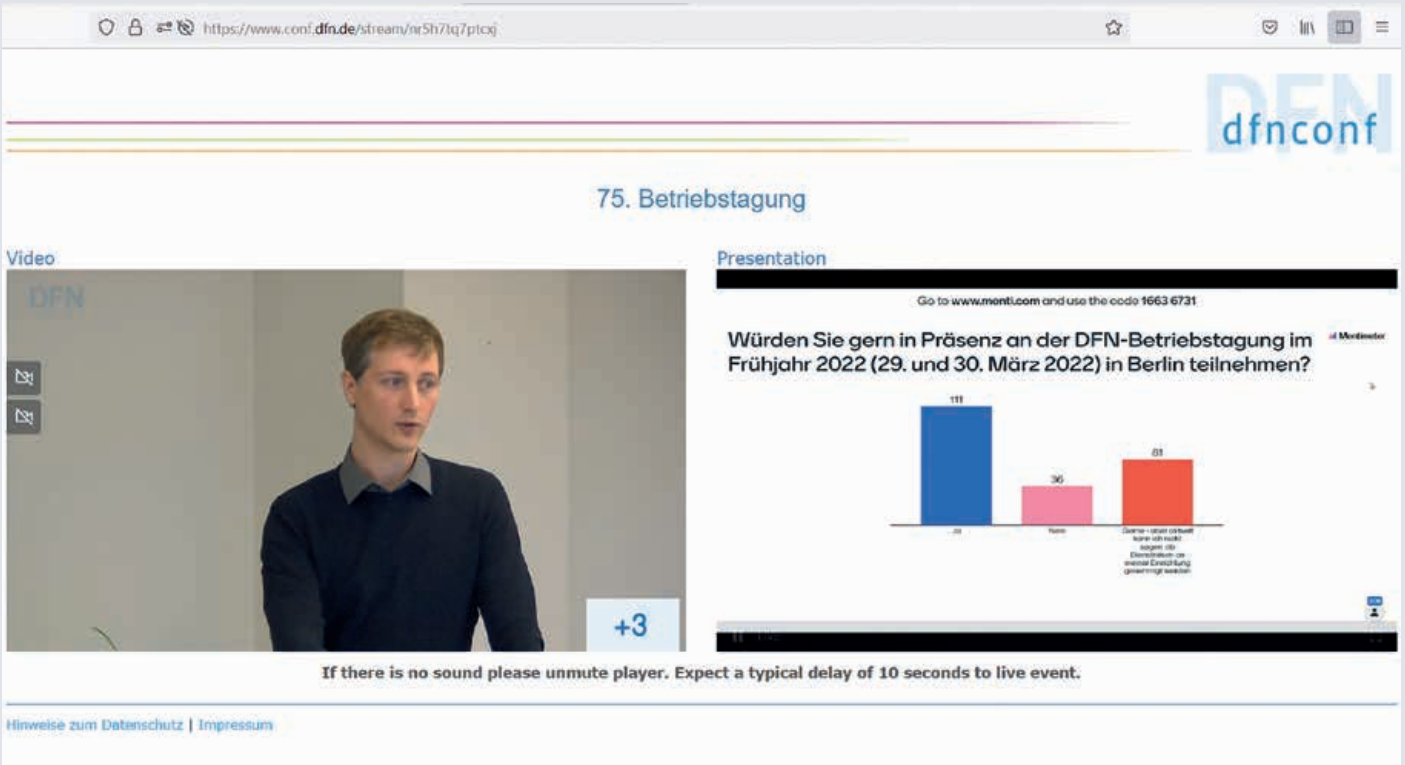
Die 29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **Donnerstag und Freitag, 3. und 4. Februar 2022**, statt.

75. DFN-Betriebstagung

Rendezvous im Herbst: Am Dienstag und Mittwoch, 26. und 27. Oktober 2021, traf sich die DFN-Community erneut online zur 75. DFN-Betriebstagung (BT) und informierte sich über die neuen Entwicklungen rund um das Deutsche Forschungsnetz und seine Dienste. Rund 400 Teilnehmende zählte das gemeinsame Plenum, das über die DFNconf-Plattform gestreamt wurde. Und auch die Fachforen von AAI über Sicherheit bis Cloud waren mit bis zu 305 Gästen sehr gut besucht und boten viele spannende Vorträge wie zum Beispiel die Präsentation im Multimedia-Forum „Von der automatisierten Veranstaltungsaufzeichnung zur hybriden Veranstaltung“. Dieses Thema dürfte derzeit viele Einrichtungen beschäftigen. Und auch beim DFN-Verein wird das hybride Format wegen der aktuell fehlenden Planungssicherheit ins Auge gefasst, denn trotz der regen Beteiligung ist bei vielen Teilnehmenden der Wunsch groß, sich endlich auch wieder in Präsenz austauschen zu können. Das zeigte das Ergebnis der Umfrage, die im Anschluss an das Plenum durchgeführt wurde. Ein Großteil der Befragten gab an, im Frühjahr gerne in Präsenz an der DFN-Betriebstagung teilnehmen zu wollen. Das DFN-Orga-Team hat bereits mit den Vorbereitungen begonnen. Eine gute Nachricht vorab: Wenn das Pandemiegeschehen Präsenzveranstaltungen im Frühjahr wieder zulässt, darf sich die DFN-Community auf einen neuen Treffpunkt freuen – nämlich ganz zentral in Berlin-Mitte, nahe dem Alexanderplatz.

TERMIN

Die 76. DFN-Betriebstagung findet am Dienstag und Mittwoch, **29. und 30. März 2022**, statt. Sie ist als Hybridveranstaltung geplant.



Eindeutiges Votum: Den Wunsch, sich wieder mal in die Augen schauen zu können, teilen nicht nur die Mitgliedsvertretenden, sondern auch DFN-Moderator Michael Röder sowie der Rest der DFN-Geschäftsstelle.

16. Tagung der DFN-Nutzergruppe Hochschulverwaltung

Unter dem Motto „Campus transformieren – Surfen auf der Digitalisierungswelle“ findet vom 9. bis 11. Mai 2022 die Tagung der DFN-Nutzergruppe Hochschulverwaltung in Wismar statt. Organisiert wird sie in Zusammenarbeit mit der Hochschule Wismar vom DFN-Verein. Vortragende aus Rechenzentren sowie aus Forschung, Verwaltung und Wirtschaft beschäftigen sich mit hochaktuellen Fragen zur Informationssicherheit, Datenhaltung und Softwarebeschaffung sowie zum Softwaremanagement.

Schwerpunkte der 16. Tagung sind: Cloudnutzung, „Die digitale Hochschule“ und E-Government.

In der 1991 gegründeten DFN-Nutzergruppe Hochschulverwaltung werden Entwicklungen der Informations-, Kommunikations- und Medientechnik in direkten Bezug zu Themen der Hochschuladministration gesetzt. Die Ergebnisse werden den Vertretenden der Hochschulen in der Regel alle zwei Jahre auf einer Tagung vorgestellt. Corona-bedingt gab es 2021 eine Onlinetagung. Die übernächste Tagung wird, im ursprünglichen Zweijahresrhythmus, 2023 in Bamberg stattfinden.

Weitere Informationen zur Arbeit der Nutzergruppe und zu ihren Tagungen finden Sie unter: www.hochschulverwaltung.de.

Hafen von Wismar mit Blick auf die Altstadt *Foto: DR pics24/ iStock*

TERMIN

Die 16. Tagung der DFN-Nutzergruppe Hochschulverwaltung findet vom **9. bis 11. Mai 2022** in Wismar statt.

Forum Hochschulkanzler 2022

Das Diskussionsforum der Kanzlerinnen und Kanzler der Hochschulen im DFN-Verein (kurz „DFN-Kanzlerforum“) richtet sich an alle Personen, die auf Ebene der Hochschulleitung eine strategische Verantwortung für Informationsverarbeitung und datentechnische Kommunikation (IuK) tragen.

In einem Abstand von zwei Jahren bietet das DFN-Kanzlerforum die Gelegenheit, sich auf Ebene der Hochschulleitungen über aktuelle Themen rund um die sich schnell wandelnden Herausforderungen der Nutzung von netzbasierten Informations- und Kommunikationsdiensten zu informieren und sich untereinander sowie mit Vertretenden des DFN-Vereins auszutauschen.

TERMIN

Das Forum Hochschulkanzler 2022 ist für **Montag und Dienstag, 23. und 24. Mai 2022**, geplant.

DFM Mitteilungen | Ausgaben 92 - 99

2019

97/2020 – Abstand, bitte! – heißt es von nun an

Die erste Welle der COVID-19-Pandemie stellt die ganze Welt vor besondere Herausforderungen. Und auch der DFN-Verein ist davon nicht ausgenommen. Die Arbeit wird in das Homeoffice verlagert. Auch die 80. DFN-Mitgliederversammlung findet online statt – zum ersten Mal. Insbesondere der Dienst DFNconf wird arg auf die Probe gestellt. Die Meeting- und Teilnehmerzahlen gehen über Nacht auf allen Plattformen durch die Decke. In einem Kraftakt gelingt es dem DFNconf-Team den Dienst auf mehreren Ebenen zu stabilisieren. Fazit: die COVID-19-Pandemie hat gezeigt, wie stark die DFN-Gemeinschaft in Krisenzeiten und wie stabil das Kernnetz des X-WiN ist.

2021

Überblick DFN-Verein

(Stand: 11/2021)

Fotos: jackijack / fotolia

Laut Satzung fördert der DFN-Verein die Schaffung der Voraussetzungen für die Errichtung, den Betrieb und die Nutzung eines rechnergestützten Informations- und Kommunikationssystems für die öffentlich geförderte und gemeinnützige Forschung in der Bundesrepublik Deutschland. Der Satzungszweck wird insbesondere verwirklicht durch Vergabe von Forschungsaufträgen und Organisation von Dienstleistungen zur Nutzung des Deutschen Forschungsnetzes.

Als Mitglieder werden juristische Personen aufgenommen, von denen ein wesentlicher Beitrag zum Vereinszweck zu erwarten ist oder die dem Bereich der institutionell oder sonst aus öffentlichen Mitteln geförderten Forschung zuzurechnen sind. Sitz des Vereins ist Berlin.

Die Geschäftsstelle

Standort Berlin (Sitz des Vereins)
DFN-Verein e. V.
Alexanderplatz 1
10178 Berlin
Telefon: +49 30 884299-0

Standort Stuttgart
DFN-Verein e. V.
Lindenspürstraße 32
70176 Stuttgart
Telefon: +49 711 63314-0

Die Organe

Mitgliederversammlung
Die Mitgliederversammlung ist u. a. zuständig für die Wahl der Mitglieder des Verwaltungsrates, für die Genehmigung des Jahreswirtschaftsplanes, für die Entlastung des Vorstandes und für die Festlegung der Mitgliedsbeiträge. Derzeitiger Vorsitzender der Mitgliederversammlung ist Prof. Dr. Gerhard Peter, Hochschule Heilbronn.

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten, und berät den Jahreswirtschaftsplan. Für die 13. Wahlperiode sind Mitglieder des Verwaltungsrates:

Dr. Rainer Bockholt
(Rheinische Friedrich-Wilhelms-Universität Bonn)

Franziska Broer
(Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.)

Prof. Dr. Frank Jenko
(Technische Universität München)

Prof. Dr. Sabina Jeschke
(Arctic Brains AB, Schweden)

Prof. Dr. Odej Kao
(Technische Universität Berlin)

Dr. Holger Marten
(Christian-Albrechts-Universität zu Kiel)

Dr. Karl Molter
(Hochschule Trier)

Prof. Dr.-Ing. Stephan Olbrich
(Universität Hamburg)

Dr. Hartmut Plehn
(Otto-Friedrich-Universität Bamberg)

Prof. Dr.-Ing. Dr. h.c. Stefan Wesner
(Universität Ulm)

Prof. Dr.-Ing. Ramin Yahyapour
(Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen)

Christian Zens
(Friedrich-Alexander-Universität Erlangen-Nürnberg)

Prof. Dr. Harald Ziegler
(Ruhr-Universität Bochum)

Der Verwaltungsrat hat als ständige Gäste

eine Vertreterin der Hochschulrektorenkonferenz:
Prof. Dr. Monika Gross
(Berliner Hochschule für Technik)

eine Vertreterin der Hochschulkanzlerinnen und -kanzler:
Dr. Andrea Bör
(Kanzlerin der Freien Universität Berlin)

einen Vertreter der Kultusministerkonferenz:
Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:
Prof. Dr. Gerhard Peter
(Hochschule Heilbronn)

den Vorsitzenden des ZKI:
Hartmut Hotzel
(Bauhaus-Universität Weimar)

Vorstand
Der Vorstand des DFN-Vereins im Sinne des Gesetzes wird aus dem Vorsitzenden und den beiden stellvertretenden Vorsitzenden des Verwaltungsrates gebildet. Derzeit sind dies:

Prof. Dr. Odej Kao
Vorsitz

Dr. Rainer Bockholt
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

Der Vorstand wird beraten vom Strategischen Beirat, einem Betriebsausschuss (BA) und einem Ausschuss für Recht und Sicherheit (ARuS).

Der Vorstand bedient sich zur Erledigung laufender Aufgaben einer Geschäftsstelle mit Standorten in Berlin und Stuttgart. Sie wird von einer Geschäftsführung geleitet. Als Geschäftsführer wurden vom Vorstand Dr. Christian Grimm und Jochem Pattloch bestellt.

Die Mitgliedseinrichtungen

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Technische Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
Bad Homburg	NTT Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berlin-Brandenburgische Akademie der Wissenschaften
	Berliner Institut für Gesundheitsforschung/Berlin Institute of Health
	Berliner Hochschule für Technik (BHT)
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Campus Berlin-Buch GmbH
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hertie School gGmbH
	Hochschule für Technik und Wirtschaft – University of Applied Sciences
	Hochschule für Wirtschaft und Recht
	Humboldt-Universität zu Berlin (HUB)
	International Psychoanalytic University Berlin
	IT-Dienstleistungszentrum
	Museum für Naturkunde
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB)
	Zuse-Institut Berlin (ZIB)
Biberach	Hochschule Biberach
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern, für Bau und Heimat
	BundesminIsterium für Umwelt, Naturschutz und nukleare Sicherheit
	Deutsche Forschungsgemeinschaft (DFG)
	Deutscher Akademischer Austauschdienst e. V. (DAAD)
	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	ITZ Bund
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	FZB, Forschungszentrum Borstel – Leibniz Lungenzentrum
Brandenburg	Technische Hochschule Brandenburg
Braunschweig	Leibniz-Institut DSMZ – Deutsche Sammlung von Mikroorganismen und Zellkulturen GmbH
	Helmholtz-Zentrum für Infektionsforschung GmbH
	Hochschule für Bildende Künste Braunschweig
	Johann Heinrich von Thünen-Institut, Bundesforschungs-institut für Ländliche Räume, Wald und Fischerei
	Julius Kühn-Institut, Bundesforschungsinstitut für Kulturpflanzen
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Carolo-Wilhelmina zu Braunschweig
Bremen	Hochschule Bremen
	Hochschule für Künste Bremen
	Jacobs University Bremen gGmbH
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung (AWI)
	Hochschule Bremerhaven
Chemnitz	Technische Universität Chemnitz
	TUCed – Institut für Weiterbildung GmbH
Clausthal	Technische Universität Clausthal
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg
Darmstadt	Deutsche Telekom IT GmbH
	European Space Agency (ESA)
	Evangelische Hochschule Darmstadt
	GSI Helmholtzzentrum für Schwerionenforschung GmbH
	Hochschule Darmstadt
	Merck KGaA
	Technische Universität Darmstadt
Deggendorf	Technische Hochschule
Dortmund	Fachhochschule Dortmund

	Technische Universität Dortmund
Dresden	Evangelische Hochschule Dresden
	Helmholtz-Zentrum Dresden-Rossendorf e. V.
	Hannah-Arendt-Institut für Totalitarismusforschung e. V.
	Hochschule für Bildende Künste Dresden
	Hochschule für Technik und Wirtschaft
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Dummersdorf	Forschungsinstitut für Nutztierbiologie (FBN)
Düsseldorf	Hochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
	Robert-Schumann-Hochschule
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	RWI – Leibniz-Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Hochschule Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	Deutsches Institut für Internationale Pädagogische Forschung
	Frankfurt University of Applied Science
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	Philosophisch-Theologische Hochschule St. Georgen e. V.
	Senckenberg Gesellschaft für Naturforschung
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
	Evangelische Hochschule Freiburg
	Katholische Hochschule Freiburg
Freising	Hochschule Weihenstephan
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen – Informatik, Technik, Wirtschaft, Medien
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum d. Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum Geesthacht Zentrum für Material- und Küstenforschung GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GWDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen, Hochschule für Technik und Wirtschaft
	FernUniversität in Hagen
Halle/Saale	Leibniz-Institut für Wirtschaftsforschung Halle e. V.
	Martin-Luther-Universität Halle-Wittenberg
	Burg Giebichenstein Kunsthochschule Halle
Hamburg	Bundesamt für Seeschifffahrt und Hydrographie
	Deutsches Elektronen-Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für Bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg
	Universität Hamburg
Hameln	Hochschule Weserbergland
Hamm	Hochschule Hamm-Lippstadt
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe
	Hochschule Hannover
	Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek
	Gottfried Wilhelm Leibniz Universität Hannover
	HIS Hochschul-Informations-System eG
	Hochschule für Musik, Theater und Medien
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek
	Stiftung Tierärztliche Hochschule
Heide	Fachhochschule Westküste, Hochschule für Wirtschaft und Technik
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	NEC Laboratories Europe GmbH
	Ruprecht-Karls-Universität Heidelberg
Heilbronn	Hochschule für Technik, Wirtschaft und Informatik Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Fachhochschule Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof – FH
Idstein	Hochschule Fresenius gGmbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	DiZ – Zentrum für Hochschuldidaktik d. bayerischen Fachhochschulen
	Hochschule für angewandte Wissenschaften FH Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena

	Leibniz-Institut für Photonische Technologien e. V.
	Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Hochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibnitz-Institut für Informationsinfrastruktur
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Karlshochschule International University
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Fachhochschule Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	Technische Hochschule Köln
	Universität zu Köln
Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut – Hochschule für angewandte Wissenschaften
Leipzig	Deutsche Telekom, Hochschule für Telekommunikation Leipzig
	Helmholtz-Zentrum für Umweltforschung – UFZ GmbH
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	Technische Hochschule Ostwestfalen-Lippe
Lübeck	Technische Hochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Hochschule für Wirtschaft und Gesellschaft Ludwigshafen
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
	Universität Koblenz-Landau
Mannheim	Hochschule Mannheim
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	TÜV SÜD Energietechnik GmbH Baden-Württemberg
	Universität Mannheim
	ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
Meißen	Hochschule Meißen (FH) und Fortbildungszentrum
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschafts- u. Landnutzungsforschung e. V.
München	Bayerische Staatsbibliothek
	Hochschule für angewandte Wissenschaften München
	Hochschule für Philosophie München
	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Katholische Stiftungshochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	Fachhochschule Münster
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Bundesgesellschaft für Endlagerung mbH (BGE)

Pforzheim	Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Potsdam	Fachhochschule Potsdam
	Helmholtz-Zentrum, Deutsches GeoForschungsZentrum – GFZ
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Reutlingen	Hochschule Reutlingen
Rosenheim	Technische Hochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	CISPA – Helmholtz-Zentrum für Informationssicherheit gGmbH
	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schenefeld	European X-Ray Free-Electron Laser Facility GmbH
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Sigmaringen	Hochschule Albstadt-Sigmaringen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Hochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	Technische Hochschule Ulm
	Universität Ulm
Vechta	Universität Vechta
	Private Hochschule für Wirtschaft und Technik gGmbH
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH (LZI)
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz
Weßling	T-Systems Information Services GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau
Wilhelmshaven	Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth
Wismar	Hochschule Wismar
Witten	Private Universität Witten/Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
	Kirchliche Hochschule Wuppertal/Bethel
Würzburg	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität Würzburg
	Universitätsklinikum Würzburg
Zittau	Hochschule Zittau/Görlitz
Zwickau	Westsächsische Hochschule Zwickau

DFN mitteilungen
bieten Hintergrundwissen zu Themen aus der Welt der Kommunikationsnetze und des DFN-Vereins

DFN infobrief recht
informiert über aktuelle Entwicklungen und Fragen des Medien- und Informationsrechts

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

DFN auf twitter
postet und teilt spannende News zum Deutschen Forschungsnetz

Alle Publikationen können Sie hier abonnieren:
https://www.dfn.de/publikationen/