(CORE TRUST) SEAL YOUR REPOSITORY!

von Doris Ernst, Gertraud Novotny und Eva Maria Schönher

Zusammenfassung: *Eine Arbeitsgruppe, die im Rahmen des Netzwerks für RepositorienmanagerInnen (RepManNet) entstanden ist, hat sich mit gängigen Zertifizierungen für Repositorien beschäftigt. Weiters wurden aktuelle Vorgaben der Forschungsförderer FWF und EU herangezogen. Das Core Trust Seal wurde genauer betrachtet. Hierfür wurde jenen Organisationen, die in Österreich bereits mit CTS zertifiziert sind, ein Fragebogen übermittelt. Die Antworten wurden anonymisiert zusammengefasst und ausgewertet. Plädiert wird für eine Zertifizierung von Repositorien und die Entwicklung einer DINI-Zertifizierung in Österreich.*

Schlagwörter: *Repositorium; Zertifikat; Zertifizierung; Core Trust Seal; CTS; Forschungsförderer; FWF; Europäische Union*

(CORE TRUST) SEAL YOUR REPOSITORY!

Abstract: *A working group, which was established within the Network of Repository Managers (RepManNet), has dealt with common certifications for repositories. In addition, current requirements of the research funding agencies FWF and EU were also taken into account. The Core Trust Seal was examined in more detail. For this purpose, a questionnaire was sent to those organizations that are already certified with CTS in Austria. The answers were summarized and evaluated anonymously. It is recommended to go for a repository certification. Moreover, the development of a DINI certificate in Austria is strongly suggested.*

Keywords: *repository; certificate; certification; Core Trust Seal; CTS; research funders; Austrian Science Fund; FWF; European Union*

DOI: *https://doi.org/10.31263/voebm.v73i1.3491*

1. Ausgangssituation

Im Rahmen des österreichischen Netzwerkes RepManNet[1] ist eine Arbeitsgruppe entstanden, die sich mit Zertifizierungen von Repositorien beschäftigt hat.

Die Auseinandersetzung mit einer Zertifizierung bietet die Möglichkeit, ein Repositorium entlang eines definierten Kriterienkataloges in Hinblick auf seine Funktionen und technischen Standards zu überprüfen. Dabei zeigt sich, ob Änderungen und Anpassungen vorgenommen werden müssen.

Vorrangiges Ziel dieser AG war:

- den Nutzen von Zertifizierungen aufzuzeigen,
- den Aufwand dafür abzubilden und
- Erfahrungsberichte aus Österreich in dieser Hinsicht zu sammeln.

In die Recherche wurden DINI, nestor, ISO 16363 sowie Core Trust Seal (CTS) inklusive seiner Vorgänger einbezogen. Diese sollen hier kurz vorgestellt werden.

1.1. DINI-Zertifikat

Das DINI-Zertifikat wird vom Verein „Deutsche Initiative für Netzwerkinformation e.V." vergeben.[2] Ziele des DINI-Zertifikates sind die Verbesserung der Publikationsinfrastruktur für das elektronische Publizieren sowie die Stärkung Open Access-basierter Publikationsformate. Die Initiative möchte hierfür einen internationalen Standard schaffen. Um DINI-zertifiziert zu werden, muss das Repositorium Mindestanforderungen erfüllen. Zu den Hauptkriterien gehören: Sichtbarkeit des Gesamtangebotes, Leitlinien (Policy), Unterstützung für AutorInnen und HerausgeberInnen, rechtliche Aspekte, Informationssicherheit, Erschließung und Schnittstellen, offene Metriken und Langzeitarchivierung.[3]

1.2. nestor-Siegel

nestor ist das deutsche Kompetenznetzwerk für Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen. Das von nestor entwickelte und angebotene Verfahren der erweiterten Selbstevaluierung auf der Grundlage der DIN-Norm 31644 „Kriterien für vertrauenswürdige digitale Langzeitarchive" bietet digitalen Repositorien eine abgestimmte und praxisgerechte Möglichkeit, um zu prüfen, ob sie vertrauenswürdig sind.[4] Bei einem po-

sitiven Ergebnis des begutachteten Prüfverfahrens kann dies durch das nestor-Siegel dargestellt werden.

Dieses kann unabhängig von anderen Verfahren durchgeführt oder gemeinsam mit dem extended certificate im Rahmen eines europäischen Zertifizierungsverfahrens erworben werden. In diesem Fall sieht das „European framework for audit and certification of digital repositories" den Erwerb des CTS vor.[5]

1.3. ISO 16363

Diese von der Internationalen Organisation für Normierung (ISO) herausgegebene Zertifizierung gehört zu einer Gruppe von drei ISO Zertifikaten: ISO 14721 (OAIS-Referenzmodell[6]), ISO 16363 (Audit and certification of trustworthy digital repositories) sowie ISO 16919 (Requirements for bodies providing audit and certification of candidate trustworthy digital repositories). Hier ist zu berücksichtigen, dass ISO 14721 rein funktional gesehen wird, ohne Anwendungsbeispiele und Beurteilungskriterien. Erst bei ISO 16363 erfolgt die Bewertung des Repositoriums anhand des OAIS-Modells und der Erfüllung der ISO 14721. Die Vorgaben bestehen aus 50 Hauptkriterien, die folgendermaßen unterteilt sind: Organisatorische Infrastruktur, Umgang mit digitalen Objekten, Infrastruktur und Risikomanagement.[7] Im Falle einer positiven Beurteilung kann ein Repositorium als vertrauenswürdig bezeichnet werden. Die eigentliche Zertifizierung erfolgt aber erst in einem dritten Schritt über ISO 16919 – auf Basis von ISO 16363.[8]

Die bereits unter nestor erwähnte deutsche Norm DIN 31644 ist gleichzeitig mit der ISO 16363 erschienen und umfasst dieselben Grundprinzipien, ist jedoch auf rund 35 allgemeinere und knapper gehaltene Beurteilungskriterien verkürzt.

1.4. Core Trust Seal (CTS)

CTS ist aus dem Data Seal of Approval (DSA) und dem World Data System (WDS) – unter Mitwirkung der ResearchData Alliance (RDA) – entstanden. Das DSA wurde seit 2010 als Zertifizierungsinstrument verwendet. Bei der Entwicklung des CTS wurde darauf geachtet, dass keine neuen Standards, Vorschriften oder hohe Investitionen erforderlich sind, sondern auf bereits Vorhandenem aufgesetzt werden kann.[9] Seit Juli 2017 sind Repositorien, die sich für das DSA bewerben, CoreTrustSeal zertifiziert. Datenrepositorien, die sich zuvor über die DSA-Website in der Übergangsphase

2017–2018 zur Zertifizierung angemeldet hatten, haben ihre Anträge mit dem DSA-Tool nach dem CTS-Verfahren vervollständigt und eine CTS-Zertifizierung erhalten.[10]

CTS basiert wie auch ISO 14721 auf dem OAIS-Referenzmodell sowie den FAIR-Prinzipien.[11] Die 16 Anforderungen im CTS lassen sich in fünf Kategorien gliedern:

- Informationen zur Institution
- organisatorische Infrastruktur
- digitale Objektverwaltung
- technische und sicherheitsrelevante Aspekte
- Feedback

Für jede Anforderung ist eine Selbstevaluierung zu erstellen. Der fertige Antrag wird eingereicht, von GutachterInnen überprüft und kritisch hinterfragt. Alle bewilligten CTS-Gutachten sind online verfügbar. Das schafft zusätzlich eine starke Community.[12]

1.5. Zusammenfassung

Auf den ersten Blick scheint die Auswahl an Zertifizierungen groß zu sein. Jedoch kann das DINI-Zertifikat derzeit nur in Deutschland beantragt werden – siehe dazu Kapitel 5. Das nestor-Siegel gilt eher als Erweiterung für bereits bestehende Zertifikate und ist für den Einstieg herausfordernd. Dies trifft ebenso für die ISO-Zertifikate zu, welche mit 50 Hauptkriterien einen beachtlichen Umfang haben.

Das CTS kann als Basis weiterer Zertifizierungen gesehen werden – sowohl nestor als auch DIN und ISO können darauf aufsetzen.[13]

Mit seinen 16 Anforderungen ist der Arbeitsaufwand für das CTS vergleichsweise überschaubar. Im Folgenden wird das CTS daher im Detail betrachtet.

2. Warum CTS ein Thema für Repository-BetreiberInnen ist

Das Veröffentlichen von Publikationen, Forschungsdaten und anderem im Rahmen von Lehre und Forschung entstandenem Output in Repositorien ist noch nicht als Selbstverständlichkeit bei Forschenden angekommen. Es fehlt teilweise das Wissen über Repositorien und zusätzlich besteht eine Unsicherheit, ob Repositorien vertraut werden kann. Daher bedarf es einer Vertrauensbasis auf Seiten der Repositorien-BetreiberInnen wie auch

der Lehrenden und Forschenden. Dies kann durch ein Zertifikat erreicht werden. Forschungsförderer empfehlen nachdrücklich eine Auseinandersetzung mit dieser Thematik.

2.1. Der Wissenschaftsfonds (FWF)

Bereits seit 01.01.2019 hat der FWF in seiner Open Access-Policy für Forschungsdaten eine Empfehlung hinsichtlich zertifizierter Repositorien inkludiert: *„Darüber hinaus werden ausdrücklich zertifizierte Repositorien (z.B. CoreTrustSeal) empfohlen und jene, welche die „Criteria for the Selection of Trustworthy Repositories" von Science Europe erfüllen."*[14]

Für die Speicherung der Forschungsdaten können laut FWF institutionelle, disziplinspezifische oder disziplinübergreifende Repositorien gewählt werden. Diese Repositorien müssen im Verzeichnis re3data.org gelistet sein.[15]

2.2. Europäische Union (EU)

Im Bericht der Europäischen Kommission (EK) vom November 2018 wird das CTS folgendermaßen beschrieben: *„[CTS and the predecessors WDS and DSA] are widely used and trusted by diverse communities at the international level as core basic certification frameworks"*.[16]

Durch das CTS zeigt man eine freiwillige Verpflichtung zur Daten- und Servicequalität sowie zur Langzeitarchivierung und bedient die verschiedenen Zielgruppen, DatenproduzentInnen, DatennachnutzerInnen und ForschungsgeldgeberInnen. Zusätzlich steigert man die nationale und internationale Sichtbarkeit des Repositoriums.

Die EK befindet sich gerade in der Entwicklungsphase des neuen Forschungsförderungsrahmenprogrammes Horizon Europe (2021–2027), dem Nachfolger von Horizon 2020. In den derzeit verfügbaren Unterlagen sind sowohl *„mandatory OA to publications"* als auch *„OA to research data ensured in line with the principle 'as open as possible, as closed as necessary'"*[17] verankert. In diesem Zusammenhang bleibt auch eine konkrete, technische Realisierung der European Open Science Cloud (EOSC) abzuwarten. Es findet sich bereits folgende Empfehlung an digitale Infrastrukturen im Bericht der EK: *„[…] CoreTrustSeal (CTS) for trusted digital repositories, should be used as a starting point to develop assessment frameworks for FAIR services. Repositories that steward data for a substantial period of time should be encouraged and supported to achieve CTS certification."*[18]

3. CTS in D-A-CH

Im D-A-CH-Raum ist die Verbreitung des CTS noch überschaubar. In der Schweiz gibt es zwei Institutionen, die das CTS erlangt haben (FORS in Lausanne, WGMS in Zürich), in Österreich drei (GAMS in Graz sowie ARCHE und AUSSDA in Wien; Phaidra in Wien hat beantragt) und in Deutschland circa zwanzig.[19]

Die in Österreich bislang zertifizierten Institutionen haben durch ihre Mitgliedschaft in internationalen Forschungsinfrastrukturen die Vorgabe gehabt, das CTS zu erlangen: AUSSDA durch CESSDA ERIC, ARCHE durch CLARIN ERIC und GAMS durch DARIAH ERIC.

4. Der Fragebogen: Überblick und Vergleich der Antworten

An jene österreichischen Institutionen, die das CTS bereits erlangt bzw. beantragt haben, wurde ein Fragebogen bestehend aus neun Fragen ausgeschickt. Ziel war, die wichtigsten Erfahrungen während der gesamten Projektphase bis zur Einreichung des CTS zu sammeln und die Ergebnisse als Hilfestellung für interessierte Repositorien-BetreiberInnen zur Verfügung zu stellen. Alle vier Institutionen haben den Fragebogen retourniert. Die Antworten sind vollständig oder bei inhaltlichen Überschneidungen in zusammengefasster Form abgebildet. Auf Wunsch wurden die Antworten anonym und nicht zuordenbar ausgeführt.

4.1. Warum haben Sie sich für die Einreichung zum CTS entschieden und gab es auch noch andere Zertifikate, deren Erlangung Sie in Erwägung gezogen haben?

Andere Zertifikate wurden von den befragten Institutionen aufgrund des Aufwandes nicht in Erwägung gezogen. Die Hauptgründe für die CTS-Zertifizierung waren:

- Das Repositorium bzw. dessen Vorgänger waren bereits mit dem DSA zertifiziert.
- Eine erfolgreiche Zertifizierung bietet einen Vorteil beim kompetitiven Einwerben von Drittmitteln.
- Das CTS wird vermutlich eine Anforderung von Fördergebern sein.
- Das CTS fördert die Vernetzung mit Repositorien-BetreiberInnen im internationalen Wissenschafts- und Forschungsraum.

- Die Zertifizierung bietet eine gute Möglichkeit, sich selbst nach vordefinierten Kriterien zu evaluieren und eventuelle Verbesserungen durchzuführen.
- Die Zertifizierung bringt Impulse für das Management und hilft, neue Perspektiven zu entwickeln.
- Eine Zertifizierung fördert die Etablierung einheitlicher Standards.

4.2. Wie haben Sie sich auf die Einreichung vorbereitet (z.B. welche Abteilungen und wie viele Personen waren wie beteiligt, mussten Vorgesetzte überzeugt werden)?

Für die Koordinierung, Betreuung und Zusammenstellung des Berichts waren in den meisten Fällen ein bis zwei Personen beauftragt. Zum Teil konnte auf bestehende Strukturen aufgebaut werden. Insgesamt waren allerdings in unterschiedlicher Intensität und Funktion bedeutend mehr Personen beteiligt. Zudem benötigte es auch Informationen von anderen Abteilungen (IT, Rechtsabteilung). Bei allen einreichenden Institutionen diente ein kollaboratives Dokument als Arbeitsgrundlage, sowie regelmäßige Teamsitzungen oder Treffen nach Bedarf. Die Vorgesetzten unterstützten das Vorhaben.

4.3. Wie wurde das Zeitmanagement organisiert?

Die Einreichung für das CTS wurde als Projekt mit einer projektverantwortlichen Hauptperson angesetzt. Diese erstellte einen Projektzeitplan für die Übermittlung der Daten aus den jeweiligen Abteilungen, den Korrekturdurchgang, organisierte regelmäßige Treffen und erinnerte die KollegInnen an die Einhaltung des Projektplans. In einer Institution wurde der Zeitaufwand optimistischer eingeschätzt, als es dann tatsächlich der Fall war.

4.4. Wurden Aufwand und Zeitrahmen von Beginn an realistisch eingeschätzt?

Eine Institution konnte bei der Einschätzung des Zeitaufwands auf Erfahrungen aus der ersten DAS-Zertifizierungsphase zurückgreifen. Die Anforderungen für das CTS sind allerdings umfänglicher als jene für das DSA. Genügend Zeit sollte für den internen Abstimmungsprozess eingeplant werden, vor allem für abteilungsübergreifende Themen. Eine andere Institution hat bereits während der Konzeptions- und Implementierungsphase des Repositoriums den Zertifizierungsprozess nach CTS angestoßen. Hier

wurde angemerkt, dass dieser deutlich effizienter geplant werden kann, wenn das Repositorium schon im Echtbetrieb läuft und die Abläufe formalisiert sind.

4.5. Welches Requirement des CTS hat sich als schwierigstes/aufwändigstes herausgestellt, bei welchen Requirements war deutlich mehr Arbeit nötig als vorgesehen?

Da der Aufwand für die einzelnen Requirements von den Standards des Archivs und der Repositorium-Software abhängt, wurde diese Frage zum Teil unterschiedlich beantwortet. So wurde je nach Institution entweder die Erfüllung der organisatorischen oder der technischen Requirements als aufwändiger wahrgenommen.

Konkret genannt wurden Requirements, die zusätzliche Belege in Form von Policies oder Dokumentation verlangen, wie beispielsweise R7 (data integrity and authenticity), R8 (appraisal) oder R12 (workflows).

Als im Arbeitsaufwand umfassender wurden auch die Requirements R3 (continuity of access), R9 (documented storage procedures) und R15-16 (technical infrastructure und security) beschrieben. In diesen sind beispielsweise die Bereiche Datenübernahme nach Ablauf eines Förderzeitraumes sowie Erstellung von Backup-Plänen und Service-Level-Agreements abgedeckt.

Für eine Institution stellte die Klarstellung, wie viele Stellen mit Management und Wartung nachhaltig betraut sind, die größte Herausforderung dar.

4.6. War für den Einreichungsprozess ein gemeinsames Glossar für ein einheitliches Verständnis der Begriffe notwendig bzw. wäre ein solches hilfreich gewesen?

Das von CTS zur Verfügung gestellte Glossar[20] war für alle befragten Institutionen hilfreich. Zusätzlich ist ein gemeinsames Glossar für ein einheitliches Verständnis der Kernbegriffe (strategy, policy) sowie eine einheitliche Schreibweise (amerikanisches / britisches Englisch) empfehlenswert.

4.7. Wie hat die Organisation auf das Thema Policy und die dadurch notwendigen organisationsinternen Abstimmungen reagiert? Wurde es durch die Einreichung zum CTS notwendig, bestehende Policies Ihrer Institution (z.B. eine Open Access-Policy oder Policy zum Umgang mit Forschungsdaten) anzupassen oder neu zu erstellen?

Die Antworten zu dieser Frage waren unterschiedlich. Die beschriebenen Prozesse umfassten einen mehrstufigen Abstimmungsprozess über viele Jahre (begleitet von einem externen Berater), problemlose Konsultationsprozesse auch im Rahmen der Erstellung neuer Policies (collection policy, privacy policy und deposition agreement) sowie den Fall, dass Abstimmungen mit anderen Abteilungen gar nicht notwendig waren.

4.8. Was hat es intern, aber auch extern gebracht, das CTS zu bekommen?

Durch das CTS wurde sowohl die interne als auch die nationale und internationale Sichtbarkeit gesteigert, sowie die Chancen bei der Drittmitteleinwerbung verbessert. Intern hat das CTS dazu beigetragen, dass Abläufe und Prozesse transparenter und viel bewusster wahrgenommen werden. Viel implizites Wissen wurde expliziert, wobei die genaue Dokumentation und Erarbeitung von Policies einen großen Mehrwert für die gesamte Organisation darstellt. Ein zusätzlicher Nutzen ist, dass die CTS-Zertifizierung Grundlage für weitere Zertifizierungen darstellt. Eine Institution gab an, die Auswirkungen noch nicht abschätzen zu können.

4.9. Welchen Rat würden Sie einer Organisation geben, die sich gerade in der Planung/am Beginn des CTS-Zertifizierungsprozesses befindet?

- Eine Einreichung erst zu beginnen, wenn bestimmte Abläufe und Services etabliert sind.
- Einkalkulieren, dass vor allem an der Dokumentation und anderen öffentlich verfügbaren Dokumenten nachgebessert werden muss.
- Ausreichend Zeit einplanen, vor allem wenn es sich um die erstmalige Einreichung handelt.
- Informationen über die verschiedenen Anforderungen vorab einholen und eine Aufstellung der notwendigen Nachweise und Dokumente anfertigen.
- Das Datenarchiv sollte bereits auf OAIS-Prinzipien aufbauend geplant werden, so sind viele der Anforderungen des CTS von Beginn an berücksichtigt.
- Insgesamt ist der Aufwand nicht zu unterschätzen. Es lohnt sich, einen Blick in die vorhandenen CTS-Zertifizierungen zu werfen, um einen Eindruck über die Anforderungen zu bekommen, sowie als Vorbereitung ein Benchmarking ausgewählter Zertifizierungen durchzuführen und dieses als Orientierung zu nutzen (pro Requirement alle Antworten sammeln).

- Jedes Requirement sollte ausführlich (idealerweise alle Fragen der extended guidance) behandelt werden und für sich alleine stehend Sinn ergeben. Manche Requirements überschneiden sich inhaltlich, hier ist erwünscht, dass die Information auch doppelt angeführt ist. Für diese Fälle wird ein identes Wording empfohlen. Dieses kann durch ein kollaboratives Dokument und ein gemeinsames Glossar erstellt werden.
- Mit jenen Requirements beginnen, die viel Abstimmungsarbeit zwischen verschiedenen Abteilungen benötigen.

5. Fazit

Obwohl in den Antworten unseres Fragebogens betont wurde, dass die Erlangung des CTS ein zeitlich und personell einschätzbares Unterfangen ist, sollten dennoch genügend Zeit und (vor allem personelle) Ressourcen eingeplant werden.

Wichtig ist, eine hauptverantwortliche Person zu definieren und diese für den gesamten Prozess von anderen Aufgaben weitestgehend freizustellen, da die Organisation der Zertifizierung idealerweise als Projekt abgewickelt wird.

Der Arbeitsaufwand ist in Relation zum entstehenden Nutzen vertretbar und die Vorteile einer Zertifizierung überwiegen. Von großem Wert für die Institutionen sind auch die im Rahmen des Zertifizierungsprozesses entstehenden Verschriftlichungen und Überarbeitungen von internen Arbeitsabläufen und Policies.[21]

Der zeitliche Aufwand für die jeweilige Institution ist von den internen Gegebenheiten abhängig. Aus den Antworten ergibt sich eine Prozessdauer von mehreren Monaten (mit hauptverantwortlicher Person als KoordinatorIn) bis zu über einem Jahr (ohne Koordinationsperson).

Die Kosten für das CTS entstehen vorrangig durch die zu investierende Arbeitszeit der jeweils beteiligten Personen und für das Zertifikat selbst. Aktuell ist eine Administrationspauschale von EUR 1.000,– (Stand Februar 2020) zu bezahlen.[22]

Das CTS eignet sich laut unseren Recherchen und der Nachfrage bei Fachleuten[23] sowohl für Publikations- als auch für Forschungsdatenrepositorien, die Verantwortung für den Erhalt und die Nutzbarkeit der archivierten digitalen Objekte übernehmen. Da das CTS ein internationaler Standard ist, stellen auch nationale Besonderheiten im Hinblick auf die rechtlichen Voraussetzungen (z.B. beim Urheberrecht) kein Hindernis für eine Zertifizierung dar.[24]

Anders stellt sich die Situation beim DINI-Zertifikat dar. Dieses kann aktuell nicht an Repositorien in Österreich vergeben werden – es fehlt eine Abstimmung der rechtlichen Anforderungen an das österreichische Recht sowie an einem GutachterInnenteam. Daher wird die Gründung einer eigenen Arbeitsgruppe „DINI in Österreich" empfohlen, welche mit der Unterstützung der deutschen „DINI-AG Elektronisches Publizieren" das Ziel verfolgt, eine DINI-Zertifizierung österreichischer Repositorien zu ermöglichen.[25]

Repositorien stellen einen Grundpfeiler für den freien Zugang zu wissenschaftlichem Output dar. Nach der umfassenden Beschäftigung mit der Thematik sprechen wir uns deutlich für eine Zertifizierung aus, da aus mehreren Blickwinkeln betrachtet die Vorteile klar überwiegen.

Welches Zertifikat für das eigene Repositorium am Besten geeignet ist, bleibt dabei natürlich den einzelnen Institutionen überlassen.

Mag.ª (FH) Doris Ernst, BA
ORCID: https://orcid.org/0000-0002-2354-0195
IST Austria, Library
E-Mail: doris.ernst@ist.ac.at

Mag.ª Gertraud Novotny, MSc
ORCID: https://orcid.org/0000-0002-8816-4936
Wirtschaftsuniversität Wien, Universitätsbibliothek
E-Mail: gertraud.novotny@wu.ac.at

MMag.ª Eva Maria Schönher
Wirtschaftsuniversität Wien, Universitätsbibliothek
E-Mail: eva.maria.schoenher@wu.ac.at

Literatur

CoreTrustSeal: https://www.coretrustseal.org (abgerufen am 27.01.2020, 12:52).

CoreTrustSeal Standards and Certification Board (2019). CoreTrustSeal Trustworthy Data Repositories Requirements: Glossary 2020–2022 (Version v02_00-2020-2022). Zenodo. http://doi.org/10.5281/zenodo.3632563

Deutsche Initiative für Netzwerkinformation e. V. (DINI): https://dini.de/ag/ (abgerufen am 13.02.2020, 16:30).

Deutsche Nationalbibliothek (DNB), Zertifizierung: https://www.dnb.de/DE/Professionell/Erhalten/Zertifizierung/zertifizierung.html (abgerufen am 25.02.2020, 16:20).

European Commission (2019). Horizon Europe, Investing to shape our future (August 2019). https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme_en (abgerufen am 27.01.2020, 12:52).

European Commission (2018). Turning FAIR into reality – Final report and action plan from the European Commission Expert Group on FAIR Data. https://doi.org/10.2777/1524

Forschungsdaten.org, FAIR data principles: https://www.forschungsdaten.org/index.php/FAIR_data_principles (abgerufen am 13.02.2010, 15:29).

FWF, Open Access für Forschungsdaten: https://fwf.ac.at/de/forschungsfoerderung/open-access-policy/open-access-fuer-forschungsdaten/ (abgerufen am 12.02.2020, 14:29).

iKeep, Digitale Archivierung nach ISO: http://ikeep.com/ISO_16363_ISO_16919_DIN_31644 (abgerufen am 25.02.2020, 16:20).

Mokrane, M., Recker, J. (2019). CoreTrustSealCertified Repositories. Enabling Findable, Accessible, Interoperable and Reusable (FAIR) Data. Proceedings of the 16th International Conference on Digital Preservation iPres (Amsterdam, The Netherlands, 16–20 September 2019), 92–100. https://ipres2019.org/static/proceedings/iPRES2019.pdf (abgerufen am 28.03.2020, 17:47).

nestor, nestor-Siegel für vertrauenswürdige digitale Langzeitarchive: https://www.langzeitarchivierung.de/Webs/nestor/DE/Zertifizierung/nestor_Siegel/siegel.html (abgerufen am 25.02.2020, 16:20).

Netzwerk für Repositorienmanager*innen (RepManNet): https://datamanagement.univie.ac.at/forschungsdatenmanagement/netzwerk-fuer-repositorienmanagerinnen-repmannet/ (abgerufen am 14.02.2020, 13:36).

PTAB – Primary Trustworthy Digital Repository Authorisation Body Ltd, ISO 16363: http://www.iso16363.org/ (abgerufen am 25.02.2020, 16:20).
re3data: https://www.re3data.org/ (abgerufen am 13.02.2010, 15:40).
Wikipedia, Deutsche Initiative für Netzwerkinformation: https://de.wikipedia.org/wiki/Deutsche_Initiative_f%C3%BCr_Netzwerkinformation (abgerufen am 25.02.2020, 16:20).
Wikipedia, OAIS (Open Archival Information System): https://de.wikipedia.org/wiki/OAIS (abgerufen am 12.02.2020, 14:21).
Zarnitz, M. (2018). CoreTrustSeal und nestor-Siegel – Zertifizierungen für die digitale Langzeitarchivierung aus Sicht eines Langzeitarchivars (108. Deutscher Bibliothekartag / 7. Bibliothekskongress, Leipzig, 19.03.2018). urn:nbn:de:0290-opus4-161881

1 https://datamanagement.univie.ac.at/forschungsdatenmanagement/netzwerk-fuer-repositorienmanagerinnen-repmannet/
2 https://dini.de/dienste-projekte/dini-zertifikat/
3 https://de.wikipedia.org/wiki/Deutsche_Initiative_f%C3%BCr_Netzwerkinformation
4 https://www.langzeitarchivierung.de/Webs/nestor/DE/Zertifizierung/nestor_Siegel/siegel.html
5 https://www.dnb.de/DE/Professionell/Erhalten/Zertifizierung/zertifizierung.html
6 OAIS ist ein Referenzmodell für ein dynamisches, erweiterungsfähiges Archivinformationssystem, das im August 2012 als ISO-Standard 14721:2012 veröffentlicht wurde. Es gilt als wichtigster Standard für die elektronische Archivierung, siehe: https://de.wikipedia.org/wiki/OAIS
7 http://www.iso16363.org/
8 vgl. http://ikeep.com/ISO_16363_ISO_16919_DIN_31644
9 Survey on DAS-certified digital repositories, S. 5.
10 https://www.coretrustseal.org/about/history/data-seal-of-approval/
11 Die „FAIR Data Principles“ formulieren Grundsätze, die nachhaltig nachnutzbare Forschungsdaten erfüllen müssen und die Forschungsdateninfrastrukturen dementsprechend im Rahmen der von ihnen angebotenen Services implementieren sollten. Gemäß der FAIR-Prinzipien sollen Daten „Findable, Accessible, Interoperable, and Re-usable“ sein; siehe: https://www.forschungsdaten.org/index.php/FAIR_data_principles
12 CoreTrustSeal Certified Repositories. Enabling Findable, Accessible, Interoperable and Reusable (FAIT) Data. 16th International Conference on Digital Preservation iPres, Amsterdam, The Nederlands, S. 8.

13 Zarnitz, M. (2018): CoreTrustSeal und nestor-Siegel – Zertifizierungen für die digitale Langzeitarchivierung aus Sicht eines Langzeitarchivars, Bibliothekskongress 19.03.2018 Leipzig, urn:nbn:de:0290-opus4-161881, S. 3.
14 https://fwf.ac.at/de/forschungsfoerderung/open-access-policy/open-access-fuer-forschungsdaten/
15 In re3data.org, dem „Registry of Research Data Repositories" werden diese Repositorien in einem web-basierten Verzeichnis erschlossen und auffindbar gemacht. Aktuell (Jänner 2020) finden sich über 2.400 verzeichnete Repositorien im Verzeichnis.
16 „Turning FAIR into reality" 2018, S. 44.
17 https://ec.europa.eu/info/files/horizon-europe-investing-shape-our-future_en Horizon Europe – Investing to shape our future, Folie 20.
18 „Turning FAIR into reality" 2018, S. 44.
19 Siehe Deutschlandkarte unter https://www.coretrustseal.org/why-certification/certified-repositories/
20 http://doi.org/10.5281/zenodo.3632563
21 Auswertung der Fragebögen und Zarnitz, M. (2018): CoreTrustSeal und nestor-Siegel – Zertifizierungen für die digitale Langzeitarchivierung aus Sicht eines Langzeitarchivars, Bibliothekskongress 19.03.2018 Leipzig, urn:nbn:de:0290-opus4-161881, S. 4.
22 https://www.coretrustseal.org/apply/administrative-fee/
23 Laut Auskunft von Jonas Recker (Chair of the Core Trust Seal Board).
24 Laut Auskunft von Jonas Recker (Chair of the Core Trust Seal Board).
25 Vorgespräche geführt mit Isabella Meinecke (Staats- und Universitätsbibliothek Hamburg, DINI Arbeitsgruppe elektronisches Publizieren).