

DIN EN ISO 21298



ICS 35.240.80

**Medizinische Informatik –
Funktionelle und strukturelle Rollen (ISO 21298:2017, korrigierte Fassung
2017-04);
Deutsche Fassung EN ISO 21298:2017**

Health informatics –
Functional and structural roles (ISO 21298:2017, Corrected version 2017-04);
German version EN ISO 21298:2017

Informatique de santé –
Rôles fonctionnels et structurels (ISO 21298:2017, Version corrigée 2017-04);
Version allemande EN ISO 21298:2017

Gesamtumfang 47Seiten

DIN-Normenausschuss Medizin (NAMed)

Nationales Vorwort

Dieses Dokument (EN ISO 21298:2017) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ (Sekretariat: ANSI, USA) in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ (Sekretariat: NEN, Niederlande) unter Beteiligung deutscher Experten erarbeitet.

Das zuständige nationale Normungsgremium ist der Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ des DIN-Normenausschusses Medizin (NAMed).

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 22600-1	siehe DIN EN ISO 22600-1
ISO 22600-2	siehe DIN EN ISO 22600-2

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 22600-1, *Medizinische Informatik — Privilegienmanagement und Zugriffssteuerung — Teil 1: Übersicht und Policy-Management*

DIN EN ISO 22600-2, *Medizinische Informatik — Privilegienmanagement und Zugriffssteuerung — Teil 2: Formale Modelle*

Deutsche Fassung

Medizinische Informatik —
Funktionelle und strukturelle Rollen
(ISO 21298:2017, korrigierte Fassung 2017-04)

Health informatics —
Functional and structural roles
(ISO 21298:2017, Corrected version 2017-04)

Informatique de santé —
Rôles fonctionnels et structurels
(ISO 21298:2017, Version corrigée 2017-04)

Diese Europäische Norm wurde vom CEN am 20. Januar 2017 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Europäisches Vorwort	3
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Abkürzungen	11
5 Rollen zur Modellierung in einem architektonischen Zusammenhang	11
5.1 Rollen innerhalb des generischen Komponentenmodells	11
5.2 Rollen und Policy-Aspekte	13
5.3 Rollen im Privilegienmanagement	15
5.4 Beziehungen dieser Norm zu verwandten Privilegienmanagement-Spezifikationen	15
5.5 Strukturelle Rollen	16
5.5.1 Allgemeines	16
5.5.2 Strukturelle Rollen von Heilberufen der Internationalen Arbeitsorganisation für eine zuständigkeitsübergreifende Darstellung	16
5.5.3 Fachrichtungen im Gesundheitswesen	18
5.6 Funktionelle Rollen	19
6 Formale Modellierung von Rollen	21
6.1 Rollen im generischen Komponentenmodell	21
6.2 Entwicklung des Rollenmodells	22
6.2.1 Beziehungen und Transformation	22
6.2.2 Zuweisung von strukturellen Rollen	22
6.2.3 Spezifikation der generischen Rollen	23
6.3 Beziehungen zwischen strukturellen und funktionellen Rollen	25
7 Anwendungsfälle für die Verwendung struktureller und funktioneller Rollen in einem interregionalen oder internationalen Kontext	25
Anhang A (informativ) Abbildung von Beispielen nach ISCO-08	27
Anhang B (informativ) Muster für ein Zertifikatsprofil für eine reglementierte Gesundheitsfachkraft	43
Literaturhinweise	45

Europäisches Vorwort

Dieses Dokument (EN ISO 21298:2017) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2017, und etwaige entgegenstehende nationale Normen müssen bis August 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 21298:2017, korrigierte Fassung 2017-04, wurde von CEN als EN ISO 21298:2017 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung von Nationalen Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird normalerweise von ISO Technischen Komitees durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO, nehmen ebenfalls an der Arbeit teil. ISO arbeitet eng mit der Internationalen Elektrotechnischen Kommission (IEC) bei allen elektrotechnischen Themen zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der Grundsätze der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: www.iso.org/iso/foreword.html.

Diese erste Ausgabe von ISO 21298 ersetzt ISO/TS 21298:2008, die technisch überarbeitet wurde.

Das für dieses Dokument verantwortliche Komitee ist ISO/TC 215, *Health informatics*.

Diese korrigierte Version beinhaltet die folgende Korrektur:

— Austausch des Bildes 2.

Einleitung

Dieses Dokument enthält eine Spezifikation für die Kodierung von Informationen, die sich auf Rollen für Fachleute und Verbraucher im Gesundheitswesen beziehen. Es wurden mindestens fünf Bereiche ermittelt, für die ein Modell zur Kodierung von Rolleninformationen erforderlich sind.

- a) **Privilegienmanagement und Zugriffssteuerung:** die rollenbasierte Zugriffssteuerung ist nicht ohne wirksame Mittel zur Aufzeichnung von Rolleninformationen für Akteure im Gesundheitswesen möglich;
- b) **Verzeichnisdienste:** strukturelle Rollen werden gewöhnlich in Verzeichnissen von Gesundheitsdienstleistern aufgezeichnet (siehe z. B. ISO 21091);
- c) **Zugriffsprotokollierung:** funktionelle Rollen werden gewöhnlich in Zugriffsprotokollen für Gesundheitsinformationsanwendungen aufgezeichnet;
- d) **Public-Key-Infrastruktur (PKI):** Die Normenreihe ISO 17090 ermöglicht die Kodierung von Rollen im Gesundheitswesen in Zertifikaterweiterungen, wobei jedoch für diese Rollen kein strukturiertes Vokabular festgelegt ist. Dieses Dokument legt ein derartiges kodiertes Vokabular fest;
- e) **Verwendungszweck:** Eine Rollenspezifikation legt fest, für welche Zwecke Informationen im Gesundheitswesen angewendet werden können. Oftmals sind Verwendungszwecke mit speziellen Rollen verknüpft (siehe z. B. ISO 21091).

Zusätzlich zu diesen sicherheitsbezogenen Anwendungen gibt es mehrere weitere mögliche Anwendungen für diese Norm wie folgt:

- **Erbringung von klinischer Versorgung:** Finden und Erkennen der richtigen Fachleute für einen Gesundheitsdienst;
- **Unterstützung bei der Pflege:** Rechnungslegung von Gesundheitsdiensten;
- **Kommunikationsmanagement:** Lenkung von auf Gesundheitswesen bezogenen Nachrichten mithilfe einer speziellen Rolle;
- **Verwaltung des Gesundheitswesens und Qualitätssicherung:** Festlegung des Verwendungszweckes für spezielle Daten.

Das vorliegende Dokument ergänzt weitere maßgebende Normen, die ebenfalls Rollen für den Zweck der Zugriffssteuerung beschreiben und festlegen. Es erweitert das Modell durch die Trennung von Rolle und Policy. Diese Trennung ermöglicht eine größere und flexiblere Fähigkeit zur Instanziierung von Verfahrensvorschriften über mehrere Domänen und Zuständigkeitsbereiche. Die Rückwärtskompatibilität mit ANSI International Committee for Information Technology Standards (INCITS) und HL7 RBAC (Role-Based Access Control) ist durch eine Vereinfachung gegeben, indem Policy und Rolle miteinander zu einem einzigen Konstrukt kombiniert werden.

Auf die in diesem Dokument festgelegten Rollenkonzepte wird in vielen Internationalen Normen, wie z. B. Normen der ISO, des CEN und HL7 International, verwiesen und sie werden darin wiederverwendet. Beispiele hierfür sind ISO 22600, Literaturhinweis [9], Literaturhinweis [10] und Literaturhinweis [11].

Die Europäische Kommission und das EU-Parlament haben eine Richtlinie über die Anerkennung von Berufsqualifikationen festgelegt (Richtlinie 2005/36/EG), in der medizinische Fachrichtungen festgelegt werden (siehe <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02005L0036-20140117&from=EN>).

Anhang A enthält die Abbildung von Beispielen nach ISCO-08, während Anhang B Muster für ein Zertifikatsprofil für eine reglementierte Gesundheitsfachkraft enthält.

1 Anwendungsbereich

Dieses Dokument legt ein Modell für die Beschreibung von funktionellen und strukturellen Rollen fest und füllt dieses mit einem Basissatz von Rollen für den internationalen Einsatz in Anwendungen des Gesundheitswesens. Rollen werden in der Regel Entitäten, die Akteure sind, zugeordnet. Dies wird auf Rollen von Personen (z. B. die Rollen der Heilberufe) und ihre Rollen im Rahmen der Erbringung von Pflege (z. B. Behandelte) fokussiert.

Rollen können struktureller (z. B. approbierter Allgemeinmediziner, nicht-lizenzierte Schreibkraft usw.) oder funktioneller (z. B. Anbieter, der Mitglied eines therapeutischen Teams ist, behandelnder Arzt, verschreibender Arzt usw.) Art sein. Strukturelle Rollen sind relativ statisch, oft über viele Jahre hinweg. Sie beschäftigen sich mit Beziehungen zwischen Entitäten, die auf einem Niveau von komplexen Konzepten angegeben werden. Funktionelle Rollen sind an der Realisierung von Maßnahmen ausgerichtet und daher sehr dynamisch. Sie werden gewöhnlich in einem aufteilbaren Niveau durch feingliedrige Konzepte angegeben.

Rollen, die in diesem Dokument behandelt werden, sind nicht auf Zwecke des Privilegienmanagements beschränkt, obwohl das Privilegienmanagement und die Zugriffssteuerung eine der Anwendungen dieses Dokuments sind. Dieses Dokument behandelt keine Spezifikationen, die sich auf Berechtigungen beziehen. Dieses Dokument behandelt die Rolle und die Berechtigung als separate Konstrukte. Weitere Einzelheiten hinsichtlich der Beziehung zwischen Berechtigungen, Policies und Zugriffssteuerungen sind in ISO 22600 beschrieben.

2 Normative Verweisungen

In diesem Dokument sind keine normativen Verweisungen angegeben.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>;
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>.

3.1 Zugriffssteuerung
(en: access control)
Mittel zur Sicherstellung, dass nur autorisierte Entitäten in entsprechend autorisierter Weise Zugriff auf die Ressourcen eines Datenverarbeitungssystems nehmen können

[QUELLE: ISO/IEC 2382-8:2015, 2126294]

3.2 Autorisierer für Attributzertifikate
AA

(en: attribute certificate authority, AA)
Autorisierer, der durch Ausgabe von *Attributzertifikaten* (3.3) Privilegien zuweist

[QUELLE: ISO/IEC 9594-8:2014, 3.5.2, modifiziert]

3.3

Attributzertifikat

(en: attribute certificate)

digital von einem Attributautorisierer unterzeichnete Datenstruktur, die einige Attributwerte mit einer *Identifizierung* (3.12) über ihren Halter bindet

[QUELLE: ISO/IEC 9594-8:2014, 3.5.1]

3.4

Autorisierung

(en: authorization)

Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen

Anmerkung 1 zum Begriff: Abgeleitet von ISO 7498-2: Erteilung von Rechten einschließlich Gewährung des Zugriffs auf der Grundlage von Zugriffsrechten.

[QUELLE: ISO 22600-1:2014, 3.6]

3.5

Zertifizierungsstelle

CA

Zertifikatsaussteller

(en: certification authority, CA)

Behörde, die von einer oder mehreren vertrauenden Parteien als vertrauenswürdig erachtet wird, um Zertifikate erstellen, zuweisen und verwalten zu können

Anmerkung 1 zum Begriff: Wahlweise kann die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen [ISO 9594-8]. Die Zertifizierungsstelle gibt Zertifikate durch Unterzeichnung von Zertifikatsdaten mit ihrem privaten Signaturschlüssel aus.

Anmerkung 2 zum Begriff: Die Bezeichnung als Behörde meint in diesem Zusammenhang keine Regierungsbehörde, sondern nur, dass die betreffende Einrichtung als vertrauenswürdig erachtet wird. Zertifikatsaussteller (en: certificate issuer) kann die bessere Benennung sein, Zertifizierungsstelle (en: certification authority, CA) ist aber sehr weit verbreitet.

[QUELLE: ISO 22600-1:2014, 3.8]

3.6

Delegierung

(en: delegation)

Übertragung eines Privilegs von einer *Entität* (3.8), die dieses Privileg besitzt, auf eine andere Entität

[QUELLE: ISO 22600-1:2014, 3.10]

3.7

Delegierungspfad

(en: delegation path)

geordnete Abfolge von Zertifikaten, die zusammen mit der Authentifizierung der Identität eines *Privilegienverfechters* (3.19) verarbeitet werden können, um die Authentizität des Privilegs eines solchen Privilegienverfechters zu überprüfen

[QUELLE: ISO 22600-2:2014, 3.15]

3.8

Entität

(en: entity)

jede konkrete oder abstrakte interessierende Sache

Anmerkung 1 zum Begriff: Während das Wort Entität im Allgemeinen als Verweisung auf jede Sache verwendet werden kann, ist es im Zusammenhang mit der Modellierung für die Verweisung auf Dinge des modellierten Gegenstandsbereiches vorbehalten.

3.9

funktionelle Rolle

(en: functional role)

Rolle (3.21), die an eine Aktivität gebunden ist

Anmerkung 1 zum Begriff: Funktionelle Rollen können so zugewiesen sein, dass sie während einer Handlung auszuführen sind.

Anmerkung 2 zum Begriff: Funktionelle Rollen sind in diesem Dokument spezifiziert.

Anmerkung 3 zum Begriff: Funktionelle Rollen entsprechen der Partizipation im Referenzinformationsmodell der ISO/HL7 21731.

Anmerkung 4 zum Begriff: Siehe auch *strukturelle Rolle* (3.26).

3.10

Organisation des Gesundheitswesens

(en: healthcare organization)

amtlich eingetragene Organisation, deren Haupttätigkeit auf die Erbringung von Gesundheitsdienstleistungen oder die Gesundheitsförderung gerichtet ist

BEISPIEL Krankenhäuser, Anbieter von Gesundheits-Webseiten im Internet sowie Forschungseinrichtungen des Gesundheitswesens.

Anmerkung 1 zum Begriff: Es wird anerkannt, dass die Organisation für ihre Aktivitäten gesetzlich haftbar ist, sie braucht jedoch nicht für ihre spezielle *Rolle* (3.21) im Gesundheitswesen registriert zu sein.

[QUELLE: ISO 17090-1:2013, 3.1.4]

3.11

Gesundheitsfachkraft

(en: healthcare professional)

im Gesundheitswesen tätige Person, die über eine Berechtigung als Fachkraft im Gesundheitswesen verfügt, die in einem bestimmten Zuständigkeitsbereich anerkannt ist

Anmerkung 1 zum Begriff: Die Berechtigung als Fachkraft im Gesundheitswesen berechtigt einen im Gesundheitswesen Tätigen dazu, unabhängig von einer *Rolle* (3.21) in einer *Organisation des Gesundheitswesens* (3.10) Gesundheitsdienstleistungen zu erbringen.

BEISPIELE Allgemeinmediziner, Vertrauensarzt, Therapeut, Zahnarzt usw.

3.12

Identifizierung

(en: identification)

Durchführungen von Prüfungen mit dem Ziel, ein Datenverarbeitungssystem in die Lage zu versetzen, Entitäten zu erkennen

3.13

nicht reglementierte Gesundheitsfachkraft

(en: non-regulated healthcare personnel)

Person, die bei einer *Organisation des Gesundheitswesens* (3.10) angestellt ist, aber keine reglementierte Gesundheitsfachkraft ist

BEISPIELE Massagetherapeut, Musiktherapeut usw.

[QUELLE: ISO 17090-1:2013, 3.1.5, modifiziert]

3.14**Angestellter einer Organisation**

(en: organisation employee)

Person, die bei einer *Organisation des Gesundheitswesens* (3.10) oder einer *unterstützenden Organisation* (3.27) angestellt ist

BEISPIEL Schreibkräfte für medizinische Unterlagen, Mitarbeiter der Krankenversicherung, die über Ansprüche entscheiden, sowie Datentypisten für Arzneimittelbestellungen.

3.15**Policy**

(en: policy)

Reihe von gesetzlichen, politischen, organisatorischen, funktionellen und technischen Verpflichtungen, die sich auf Kommunikation und Zusammenarbeit beziehen

[QUELLE: ISO 22600-1:2014, 3.13]

3.16**Policy-Vereinbarung**

(en: policy agreement)

schriftliche Vereinbarung, nach der sich alle Beteiligten zur Einhaltung einer festgelegten Reihe von Policies verpflichten

[QUELLE: ISO 22600-1:2014, 3.14]

3.17**Principal**

(en: principal)

menschliche Benutzer und Objekte, die unter ihren eigenen Rechten arbeiten müssen

[QUELLE: OMG Security Services Specification: 2001]

3.18**Privileg**

(en: privilege)

Kapazität, die einer *Entität* (3.8) von einer Behörde entsprechend dem Attribut dieser Entität zugewiesen wird

Anmerkung 1 zum Begriff: Nach der OASIS-Norm Extensible Access Control Markup Language (XACML), Version 2.0 werden Privileg, Genehmigungen, Autorisierung, Berechtigung und Rechte durch den Begriff „Regel“ ersetzt.

[QUELLE: ISO 22600-1:2014, 3.17]

3.19**Privilegienverfechter**

(en: privilege assserter)

Privilegienhalter, der sein *Attributzertifikat* (3.3) oder ein Public-Key-Zertifikat verwendet, um sein *Privileg* (3.18) geltend zu machen

[QUELLE: ISO 22600-2:2014, 3.27]

3.20**Privilegienprüfer**

(en: privilege verifier)

Entität (3.8), die Zertifikate im Vergleich mit einer Privilegien-Policy überprüft

[QUELLE: ISO 22600-2:2014, 3.30]

3.21

Rolle

(en: role)

Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen

[QUELLE: ISO 22600-2:2014, 3.33]

3.22

Rollenzuweisungszertifikat

(en: role assignment certificate)

Zertifikat, das das Rollenattribut enthält und dem Zertifikathalter eine oder mehrere *Rollen* (3.21) zuweist

[QUELLE: ISO 22600-2:2014, 3.34]

3.23

Rollenzertifikat

(en: role certificate)

Zertifikat, das *Privilegien* (3.18) zuweist und zwar eher einer *Rolle* (3.21) als den betreffenden Personen direkt

Anmerkung 1 zum Begriff: Personen, denen eine Rolle durch ein *Attributzertifikat* (3.3) oder ein Public-Key-Zertifikat mit einer Subject-Verzeichnis-Attributerweiterung, die diese Zuweisung enthält, zugewiesen wird, werden die in dem Rollenzertifikat enthaltenen Privilegien indirekt zugewiesen.

3.24

Rollenspezifikationszertifikat

(en: role specification certificate)

Zertifikat, das die Zuweisung von *Privilegien* (3.18) zu einer *Rolle* (3.21) enthält

[QUELLE: ISO 22600-2:2014, 3.35]

3.25

unterstützter Gesundheitsdienstleister

(en: sponsored healthcare provider)

Gesundheitsdienstleister, der keine reglementierte Fachkraft im Zuständigkeitsbereich seiner Berufsausübung ist, der jedoch in seiner Gesellschaft des Gesundheitswesens aktiv ist und von einer reglementierten *Organisation des Gesundheitswesens* (3.10) unterstützt wird

BEISPIEL Ein Mitarbeiter zur Erziehung gegen Drogen- und Alkoholmissbrauch, der mit einer bestimmten ethnischen Gruppe arbeitet, oder Krankenpflegepersonal in einem Entwicklungsland.

[QUELLE: ISO 17090-1:2013, 3.1.10]

3.26

strukturelle Rolle

(en: structural role)

Rolle (3.21), die Beziehungen zwischen Entitäten im Sinne von Kompetenz festlegt und oftmals organisatorische oder strukturelle Beziehungen (Hierarchien) widerspiegelt

Anmerkung 1 zum Begriff: Strukturelle Rollen sind in diesem Dokument festgelegt.

Anmerkung 2 zum Begriff: Strukturelle Rollen entsprechen der Rolle des Referenzinformationsmodells der ISO/HL7 21731.

Anmerkung 3 zum Begriff: Siehe auch *funktionelle Rolle* (3.9).

3.27**unterstützende Organisation**

(en: supporting organization)

amtlich eingetragene Organisation, die Dienstleistungen für eine *Organisation des Gesundheitswesens* (3.10) erbringt, bei denen es sich jedoch nicht um Gesundheitsdienstleistungen handelt

BEISPIEL Stellen zur Finanzierung des Gesundheitswesens, wie z. B. Versicherungsträger, Lieferanten von Arzneimitteln und sonstigen Gütern.

[QUELLE: ISO 17090-1:2013, 3.1.11]

3.28**Angestellter einer unterstützenden Organisation**

(en: supporting organization employee)

Person, die bei einer *unterstützenden Organisation* (3.27) angestellt ist

4 Abkürzungen

AA	Attributautorisierer	(en: Attribute Authority)
CA	Zertifizierungsstelle	(en: Certification Authority)
GCM	Generisches Komponentenmodell	(en: Generic Component Model)
HL7	Health Level 7	(en: Health Level 7)
ILO	Internationale Arbeitsorganisation	(en: International Labour Organization)
NIST	National Institute of Standards and Technology	
PKI	Public-Key-Infrastruktur	(en: Public Key Infrastructure)
PMI	Privilege-Management-Infrastruktur	(en: Privilege Management Infrastructure)
RBAC	rollenbasierte Zugriffssteuerung	(en: Role-Based Access Control)
UML	vereinheitlichte Modellierungssprache	(en: Unified Modeling Language)
XACML	erweiterbare Zugriffskontroll-Auszeichnungssprache	(en: eXtensible Access Control Markup Language)
XML	erweiterbare Auszeichnungssprache	(en: eXtensible Markup Language)

5 Rollen zur Modellierung in einem architektonischen Zusammenhang**5.1 Rollen innerhalb des generischen Komponentenmodells**

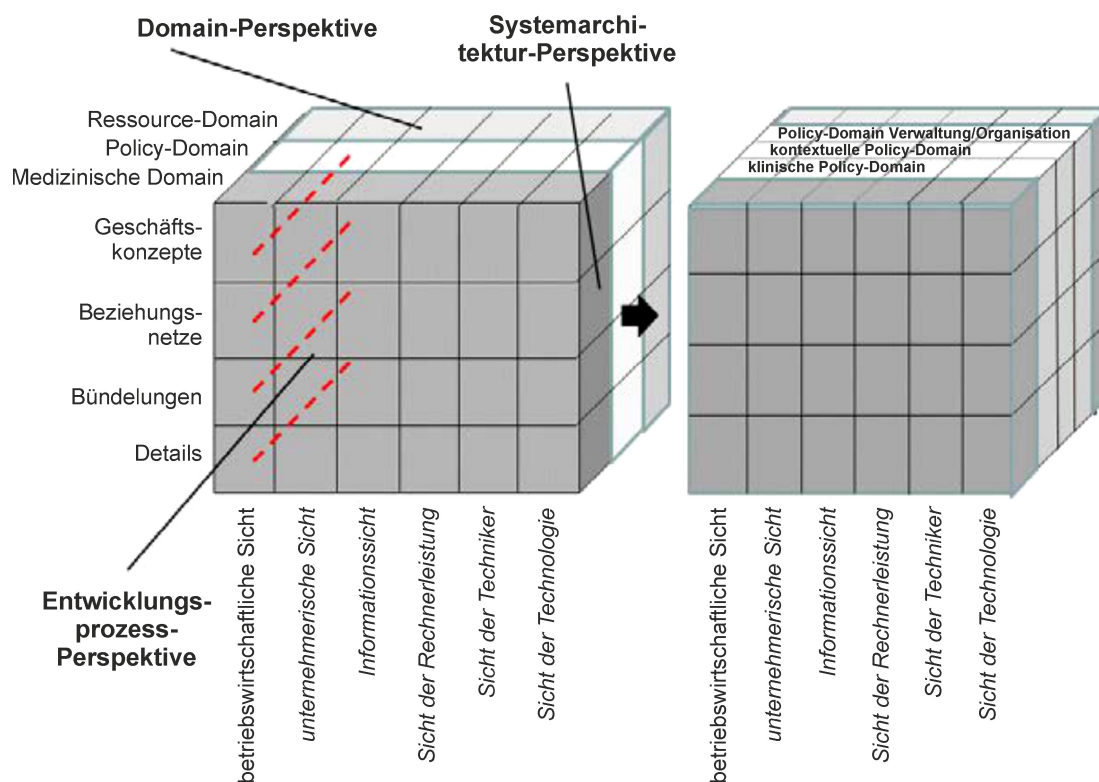
Für die Einbettung von Komponenten, welche funktionellen Anforderungen und Diensten, die in einem System benötigt werden, entsprechen, müssen die Komponenten dieses Systems in ihrem architektonischen Zusammenhang verwaltet werden. Daher müssen die Analyse der Anforderungen, die Konstruktion und der Einsatz dieser Komponenten auf der Grundlage einer Bezugs-Architektur nach einem einheitlichen Prozess entwickelt und verwaltet werden.

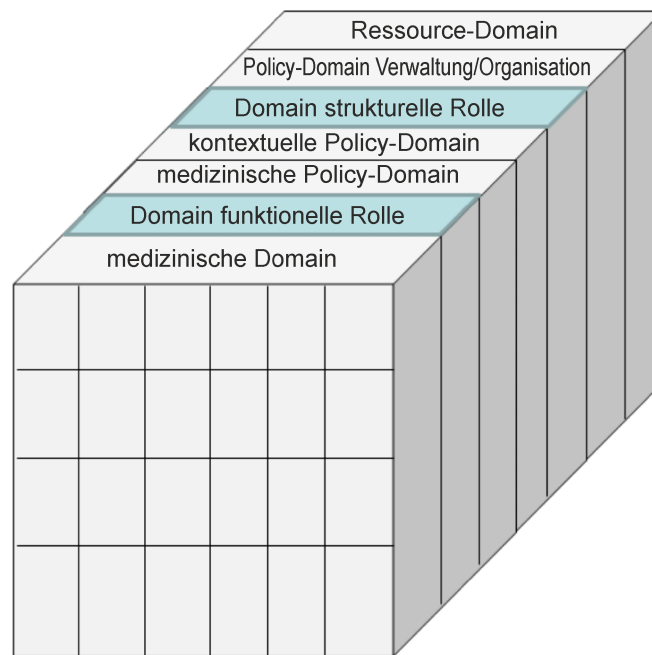
Mit dem generischen Komponentenmodell (GCM) wurde eine solche Bezugs-Architektur Mitte der 1990er Jahre in Übereinstimmung mit wesentlichen Normen für verteilte, komponentenbasierte, serviceorientierte und semantisch interoperable Informationssysteme entwickelt (z. B. ISO/IEC 9594-8, ISO/IEC 10746-2 und ISO/IEC 2382-8) und im Zusammenhang mit mehreren Spezifikationen des ISO/TC 215, des CEN/TC 251 und mit HL7-Spezifikationen angewendet. Das Modell legt eine komponentenbasierte und serviceorientierte Architektur für jede Domain fest. Obwohl dieses Dokument über Fragen der Sicherheit und des Datenschutzes hinausgeht, werden funktionelle und strukturelle Rollen auch dazu verwendet, Privilegien und die Zugriffssteuerung zu verwalten. In diesem eingeschränkten Zusammenhang wurden funktionelle und strukturelle Rollen in ISO 22600 festgelegt und modelliert. Dieses Dokument erweitert den Anwendungsbereich, die Dienstleistungen und den Einsatz von funktionellen und strukturellen Rollen, die jedoch trotzdem auf dem Architektur-Ansatz für semantisch interoperable eHealth-/pHealth- (persönliche Gesundheit) Informationssysteme [7, 8] beruhen.

Eine Systemarchitektur legt die Systemkomponenten, ihre Funktionen und Wechselbeziehungen fest. Eine Systemarchitektur wird in drei Dimensionen modelliert:

- Komponenten zur Erfüllung spezieller Anforderungen der Domain;
- die Dekomposition und, nach einer ausführlichen Beschreibung der zugrundeliegenden Konzepte, die Komposition dieser Komponenten nach entsprechenden Bündelungskonzepten/-regeln (z. B. Zusammenarbeit der Komponenten, Arbeitsabläufe, Algorithmus). Die Granularitätsstufen sind mindestens Geschäftskonzepte, Beziehungsnetze, Basisdienste/-funktionen und Basiskonzepte;
- die verschiedenen Sichtweisen auf diese Komponente nach ISO 10746 von der unternehmerischen Sicht (Geschäftsszenario, Anwendungsfall, Anforderungen) über die Informationssicht und die Sicht der Rechenleistung, die die plattformunabhängige Logik des Systems/der Komponente repräsentieren, bis hin zur Sicht der Techniker und Sicht der Technologie, die beide plattformspezifische Implementierungsaspekte behandeln.

Bild 1 stellt das generische Komponentenmodell vor, gibt die oben beschriebene Bezugs-Architektur an und ergänzt Sichtweisen nach ISO 10746 um eine praktische betriebswirtschaftliche Sicht.





ANMERKUNG Modelliert nach Literaturhinweis [8] (modifiziert).

Bild 1 — Darstellung der in dieser Norm festgelegten Rollenkonzepte mithilfe des generischen Komponentenmodells

Die in diesem Dokument festgelegten Grundsätze sind auch für andere Domains als das Gesundheitswesen anwendbar. In diesem Fall müssen die jeweilige Domain und ihre zugehörige Policy-Domain in Bild 1c eingegeben werden.

Die Entwicklung von Komponenten, die Darstellung ihrer Konzepte und ihre Bündelung beruhen auf einer Randbedingungs-Modellierung. Konzepte und Regeln können mithilfe von Metasprachen wie UML und UML-Ableitungen oder dem XML-Sprachensatz dargestellt werden.

5.2 Rollen und Policy-Aspekte

Rollen gruppieren Entitäten entsprechend ihrer Funktionen und Beziehungen im geschäftlichen Umfeld. Rollen sollten unter Berücksichtigung aller Dimensionen eines Systems verwaltet werden, dargestellt z. B. durch das GCM. Sie können durch ein Entitätenattribut ausgedrückt werden.

Zur Verwaltung der Beziehungen zwischen den Entitäten können strukturelle (organisatorische) und funktionelle Rollen festgelegt werden. Rollen könnten einer beliebigen Entität als ein Akteur in einer gegenseitigen Kommunikations- oder Kooperationsbeziehung zugewiesen werden (z. B. Person, Organisation, System, Gerät, Anwendung, Komponente usw.). Da Entitäten Akteure in Anwendungsfällen sind, haben Rollen eine Beziehung zu Akteuren und daher zu Aktionen. Funktionelle und strukturelle Rollen sind mit Policies verbunden und werden durch diese festgelegt.

Policies werden festgelegt und angewendet, um das Verhalten eines Systems zu regeln. Ohne gesonderte Belange, das heißt ohne Darstellung spezifischer Perspektiven in diesem System in spezifischen GCM-Dimensionen, werden Policies implizit in der Systemkomponenten-Spezifikation eingebettet. Sie steuern ein System durch Einschränkung der Systemkomponenten (Attribute und Operationen) und deren strukturelle und funktionelle Beziehungen. Das erfolgt z. B. in einigen vereinfachten Spezifikationen der rollenbasierte Zugriffssteuerung (RBAC) durch Zusammenfassung der Einschränkungen in einer Berechtigung, die an eine Rolle gebunden ist und als Berechtigungsattribut angegeben wird, ohne die treibende Policy explizit zu definieren und an die entsprechenden Komponente zu binden. Im Falle widersprüchlicher Einschränkungen sind zugehörige Zugriffssteuerungsentscheidungs-Policies einzusetzen.