

DIN EN ISO/IEC 24760-1



ICS 35.030

Einsprüche bis 2022-03-28

Entwurf

**Informationstechnik –
Sicherheitsverfahren –
Rahmenwerk für Identitätsmanagement –
Teil 1: Terminologie und Konzept (ISO/IEC 24760-1:2019);
Deutsche und Englische Fassung prEN ISO/IEC 24760-1:2022**

IT Security and Privacy –
A framework for identity management –
Part 1: Terminology and concepts (ISO/IEC 24760-1:2019);
German and English version prEN ISO/IEC 24760-1:2022

Sécurité IT et confidentialité –
Cadre pour la gestion de l'identité –
Partie 1: Terminologie et concepts (ISO/IEC 24760-1:2019);
Version allemande et anglaise prEN ISO/IEC 24760-1:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-01-28 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 66 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 24760-1:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 24760-1:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 9001	siehe	DIN EN ISO 9001
ISO/IEC 27007	siehe	DIN EN ISO/IEC 27007
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100
ISO/IEC 29101	siehe	DIN EN ISO/IEC 29101

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen (ISO 9001); Deutsche und Englische Fassung EN ISO 9001*

DIN EN ISO/IEC 27007, *Informationstechnik — Sicherheitsverfahren — Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007); Deutsche Fassung EN ISO/IEC 27007*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz (ISO/IEC 29100); Deutsche Fassung EN ISO/IEC 29100*

DIN EN ISO/IEC 29101, *Informationstechnik — Sicherheitstechniken — Architekturrahmenwerk für Datenschutz (ISO/IEC 29101); Deutsche Fassung EN ISO/IEC 29101*

– *Entwurf* –

E DIN EN ISO/IEC 24760-1:2022-03

– Leerseite –

**Informationstechnik – Sicherheitsverfahren – Rahmenwerk für
Identitätsmanagement – Teil 1: Terminologie und Konzept (ISO/IEC 24760-1:2019)**

IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts
(ISO/IEC 24760-1:2019)

Sécurité IT et confidentialité – Cadre pour la gestion de l'identité – Partie 1: Terminologie et concepts
(ISO/IEC 24760-1:2019)

Inhalt

	Seite
Europäisches Vorwort	3
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Symbole und Abkürzungen	14
5 Identität	14
5.1 Allgemeines	14
5.2 Identitätsinformationen	15
5.3 Identifikator	16
5.4 Digitaler Ausweis	16
5.4.1 Allgemeines	16
5.4.2 Management digitaler Ausweise	18
6 Attribute	18
6.1 Allgemeines	18
6.2 Attributarten	19
6.3 Ursprungsdomäne	20
7 Verwaltung von Identitätsinformationen	20
7.1 Allgemeines	20
7.2 Lebenszyklus von Identitäten	21
8 Identifizierung	23
8.1 Allgemeines	23
8.2 Verifizierung	24
8.3 Registrierung	24
8.4 Anmeldung	25
8.5 Legitimation	25
8.5.1 Allgemeines	25
8.5.2 Identitätsnachweis	26
9 Authentifizierung	26
10 Pflege	27
11 Aspekte der Implementierung	27
12 Datenschutz	28
Literaturhinweise	29
Stichwortverzeichnis	31

Bilder

Bild 1 — Lebenszyklus von Identitäten	22
---	----

Europäisches Vorwort

Der Text von ISO/IEC 24760-1:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 24760-1:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 24760-1:2019 wurde von CEN als prEN ISO/IEC 24760-1:2022 ohne irgendeine Abänderung genehmigt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

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 und IEC sind 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 erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder der IEC-Liste der erhaltenen Patenterklärungen (siehe <http://patents.iec.ch>).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Security techniques* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 24760-1:2011), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- neue Begriffe wurden dem Abschnitt 3 hinzugefügt;
- einige Definitionen wurden vereinfacht und berichtigt;
- einige Begriffe wurden gelöscht und einige ersetzt;
- die einleitenden Absätze von Unterabschnitt 5.1 wurden umformuliert;
- die neuen Unterabschnitte 5.4 und 8.5 wurden erstellt.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 24760 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

Datenverarbeitungssysteme erheben in der Regel eine Reihe von Informationen über ihre Benutzer, sei es eine Person, ein Gerät oder eine Software, die mit ihnen verbunden ist, und treffen auf der Grundlage der erhobenen Informationen Entscheidungen. Solche identitätsbasierten Entscheidungen können den Zugriff auf Anwendungen oder andere Ressourcen betreffen.

Um der Notwendigkeit Rechnung zu tragen, Systeme, die identitätsbasierte Entscheidungen treffen, effizient und effektiv zu implementieren, legt die Normenreihe ISO/IEC 24760 ein Rahmenwerk für die Ausgabe, Verwaltung und Verwendung von Daten fest, die dazu dienen, Personen, Organisationen oder informationstechnische Komponenten zu beschreiben, die im Namen von Personen oder Organisationen arbeiten.

Für viele Organisationen ist das ordnungsgemäße Management von Identitätsinformationen von entscheidender Bedeutung, um die Sicherheit der organisatorischen Prozesse aufrechtzuerhalten. Für Personen ist ein korrektes Identitätsmanagement zum Schutz personenbezogener Daten wichtig.

Die Normenreihe ISO/IEC 24760 legt die grundlegenden Konzepte und Betriebsstrukturen des Identitätsmanagements fest, um das Management von Informationssystemen so zu gestalten, dass diese den geschäftlichen, vertraglichen, regulatorischen und gesetzlichen Verpflichtungen nachkommen können.

Das Ziel dieses Dokuments ist es, die Terminologie und die Konzepte für das Identitätsmanagement festzulegen, um ein gemeinsames Verständnis auf dem Gebiet des Identitätsmanagements zu fördern.

1 Anwendungsbereich

In diesem Dokument werden Begriffe für das Identitätsmanagement definiert und die Kernkonzepte von Identität und Identitätsmanagement sowie deren Beziehungen zueinander festgelegt.

Es ist auf jedes Informationssystem anwendbar, das Identitätsinformationen verarbeitet.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 24760-2:2015, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

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:

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

3.1 Allgemeine Begriffe

3.1.1

Entität

Begriff, der für den Betrieb einer *Domäne* (3.2.3) relevant ist und erkennbar eine eigene Existenz hat

Anmerkung 1 zum Begriff: Eine Entität kann eine physische oder eine logische Ausführungsform haben.

BEISPIEL Eine Person, eine Organisation, ein Gerät, eine Gruppe solcher Begriffe, ein menschlicher Teilnehmer an einem Telekommunikationsdienst, eine SIM-Karte, ein Reisepass, eine Netzwerkkarte, eine Softwareanwendung, ein Dienst oder eine Website.

3.1.2

Identität

partielle Identität

Menge von *Attributen* (3.1.3), die sich auf eine *Entität* (3.1.1) beziehen

Anmerkung 1 zum Begriff: Eine Entität kann mehr als eine Identität aufweisen.

Anmerkung 2 zum Begriff: Mehrere Entitäten können die gleiche Identität haben.

Anmerkung 3 zum Begriff: ITU-TX1252 [13] legt die charakteristische Verwendung einer *Identität* fest. In diesem Dokument impliziert der Begriff *Identifikator* diesen Aspekt.

3.1.3

Attribut

Merkmal oder Eigenschaft einer *Entität* (3.1.1)

BEISPIEL Mögliche Attribute sind ein Entitätstyp, Adressinformationen, eine Telefonnummer, eine Berechtigung, eine MAC-Adresse, ein Domänenname.

3.1.4

Identifikator

Attribut oder eine Menge von *Attributen* (3.1.3), die eine *Identität* (3.1.2) in einer *Domäne* (3.2.3) eindeutig kennzeichnen

Anmerkung 1 zum Begriff: Ein Identifikator kann ein speziell erstelltes Attribut sein, dem ein Wert zugewiesen wird, der innerhalb der Domäne eindeutig ist.

BEISPIEL Als Identifikator können der Name eines Vereins mit einer Vereinsmitgliedsnummer, die Nummer einer Krankenversicherungskarte zusammen mit dem Namen der Versicherungsgesellschaft, eine E-Mail-Adresse oder ein globaler Identifikationsschlüssel, ein Universal Unique Identifier (UUID), verwendet werden. In einem Wählerverzeichnis reicht die Kombination der Attribute *Name*, *Anschrift* und *Geburtsdatum* aus, um einen Wähler eindeutig zu identifizieren.

3.1.5

Ursprungsdomäne

Domäne (3.2.3), in der ein Wert für ein *Attribut* (3.1.3) geschaffen oder dessen Wert (neu) zugewiesen wurde

Anmerkung 1 zum Begriff: Die Ursprungsdomäne kann als Metadaten für ein Attribut bereitgestellt werden.

Anmerkung 2 zum Begriff: Die Ursprungsdomäne legt in der Regel die Bedeutung und das Format des Attributwerts fest. Eine solche Spezifikation kann sich auf internationale Normen stützen.

Anmerkung 3 zum Begriff: Ein Attribut kann einen expliziten Wert enthalten, der auf die Ursprungsdomäne verweist, z. B. einen ISO-Ländercode für eine Reisepassnummer als Verweisung auf das ausstellende Land, das die Ursprungsdomäne der Identitätsinformationen im Reisepass ist.

Anmerkung 4 zum Begriff: Operativ kann eine Ursprungsdomäne als maßgebliche Quelle für ein Attribut zur Verfügung stehen (manchmal auch als Attribute Authority bezeichnet). Eine maßgebliche Quelle kann außerhalb der eigentlichen Ursprungsdomäne betrieben werden. Für ein und dieselbe Ursprungsdomäne können mehrere maßgebliche Quellen existieren.

BEISPIEL Die Ursprungsdomäne einer Clubmitgliedsnummer ist der spezifische Club, der die Nummer vergeben hat.

3.1.6

Referenzkennung

RI, en: reference identifier

Identifikator (3.1.4) in einer *Domäne* (3.2.3), der für die Dauer, in der eine *Entität* (3.1.1) in der Domäne bekannt ist, gleich bleiben soll und für einen in einer Richtlinie festgelegten Zeitraum, nachdem die Entität in dieser Domäne nicht mehr bekannt ist, nicht mit einer anderen Entität verbunden ist

Anmerkung 1 zum Begriff: Eine Referenzkennung bleibt mindestens für die Dauer der Existenz der Entität in einer Domäne bestehen und kann länger als die Entität bestehen, z. B. für Archivierungszwecke.

Anmerkung 2 zum Begriff: Eine Referenzkennung für eine Entität kann sich während der Lebensdauer einer Entität ändern, so dass die alte Referenzkennung für diese Entität nicht mehr gilt.

BEISPIEL Eine Führerscheinnummer, die während des gesamten Lebens eines Fahrers gleich bleibt, ist ein dauerhafter Identifikator, der auf zusätzliche Identitätsinformationen verweist und eine Referenzkennung ist. Eine IP-Adresse ist keine Referenzkennung, da sie auch anderen Entitäten zugewiesen werden kann.

3.1.7

Betroffene(r)

Subjekt

Entität (3.1.1), deren Identitätsinformationen von einem *Identitätsmanagementsystem* (3.4.8) gespeichert und verwaltet werden

Anmerkung 1 zum Begriff: Im Zusammenhang mit dem Datenschutz oder in Fällen, in denen ein(e) Betroffene(r) als ausführendes Organ angesehen wird, bezieht sich ein(e) Betroffene(r) in der Regel auf eine Person.

[QUELLE: ISO/IEC 24760-2:2015, 3.4 modifiziert — Das Wort „betrifft“ wurde klarer formuliert und Anmerkung 1 zum Begriff wurde umformuliert.]

3.2 Identifizierung

3.2.1

Identifizierung

Prozess der Erkennung einer *Entität* (3.1.1) in einer bestimmten *Domäne* (3.2.3) in Abgrenzung zu anderen Entitäten

Anmerkung 1 zum Begriff: Bei der Identifizierung werden behauptete oder beobachtete Attribute überprüft.

Anmerkung 2 zum Begriff: Die Identifizierung ist in der Regel Teil der Interaktionen zwischen einer Entität und den Diensten in einer Domäne sowie dem Zugriff auf Ressourcen. Die Identifizierung kann mehrfach erfolgen, während die Entität in der Domäne bekannt ist.

3.2.2

Verifizierung

Prozess der Feststellung, dass die *Identitätsinformationen* (3.2.4), die mit einer bestimmten *Entität* (3.1.1) verbunden sind, korrekt sind

Anmerkung 1 zum Begriff: Bei der Verifizierung wird in der Regel festgestellt, welche Attribute erforderlich sind, um eine Entität in einer Domäne zu erkennen, und es wird geprüft, ob diese erforderlichen Attribute vorhanden sind, ob sie die richtige Syntax haben, ob sie innerhalb eines bestimmten Gültigkeitszeitraums existieren und ob sie zu der Entität gehören.

3.2.3

Domäne

Anwendbarkeitsdomäne

Kontext

Umgebung, in der eine *Entität* (3.1.1) eine Menge von *Attributen* (3.1.3) zur *Identifizierung* (3.2.1) und für andere Zwecke verwenden kann

Anmerkung 1 zum Begriff: Im Allgemeinen ist die Domäne einer Identität in Bezug auf die jeweilige Menge von Attributen genau definiert.

Anmerkung 2 zum Begriff: ITU-T X1252 [13] verwendet den Begriff Kontext; dieses Dokument bevorzugt den Begriff Domäne.

BEISPIEL Ein von einer Organisation eingesetztes IT-System, das den Benutzern die Anmeldung ermöglicht, ist die Domäne für den Anmeldenamen des Benutzers.

3.2.4

Identitätsinformationen

Menge der Werte von *Attributen* (3.1.3), optional mit zugehörigen Metadaten in einer *Identität* (3.1.2)

Anmerkung 1 zum Begriff: In einem System der Informations- und Kommunikationstechnologie ist eine Identität als Identitätsinformationen vorhanden.

3.3 Authentifizierung von Identitätsinformationen

3.3.1

Authentifizierung

formalisierter Prozess der *Verifizierung* (3.2.2), der im Erfolgsfall zu einer *authentifizierten Identität* (3.3.2) für eine *Entität* (3.1.1) führt

Anmerkung 1 zum Begriff: Der Authentifizierungsprozess umfasst Prüfungen eines oder mehrerer von einer Entität bereitgestellten Identitätsattribute durch einen Verifizierer, um deren Korrektheit mit dem erforderlichen Grad an Sicherheit festzustellen.

Anmerkung 2 zum Begriff: Bei der Authentifizierung wird in der Regel eine Richtlinie verwendet, um einen erforderlichen Grad an Sicherheit für das Ergebnis eines erfolgreichen Abschlusses festzulegen.

3.3.2

authentifizierte Identität

Identitätsinformationen (3.2.4) für eine *Entität* (3.1.1), die zur Aufzeichnung des Ergebnisses der *Authentifizierung* (3.3.1) erstellt wurden

Anmerkung 1 zum Begriff: Eine authentifizierte Identität enthält in der Regel Informationen, die im Rahmen des Authentifizierungsprozesses gewonnen wurden, z. B. den erreichten Grad an Sicherheit.

Anmerkung 2 zum Begriff: Das Vorhandensein einer authentifizierten Identität in einer bestimmten Domäne bedeutet, dass eine Entität in dieser Domäne anerkannt wurde.

Anmerkung 3 zum Begriff: Eine authentifizierte Identität hat üblicherweise eine durch eine Authentifizierungsrichtlinie begrenzte Lebensdauer.

3.3.3

Identitätsinformationsstelle

IIA, en: identity information authority

Entität (3.1.1), die sich auf eine bestimmte *Domäne* (3.2.3) bezieht und beweisbare Aussagen über die Gültigkeit und/oder Richtigkeit eines oder mehrerer Attributwerte in einer *Identität* (3.1.2) machen kann

Anmerkung 1 zum Begriff: Eine Identitätsinformationsstelle ist üblicherweise mit der Domäne verbunden, z. B. der Ursprungsdomäne, in der die Attribute, zu denen die IIA Aussagen machen kann, eine besondere Bedeutung haben.

Anmerkung 2 zum Begriff: Die Tätigkeit einer Identitätsinformationsstelle kann Gegenstand einer Datenschutzrichtlinie sein.

Anmerkung 3 zum Begriff: Eine Entität kann die Funktionen des Identitätsinformationsanbieters und der Identitätsinformationsstelle kombinieren.

3.3.4

Identitätsinformationsanbieter

Identitätsanbieter

IIP, en: identity information provider

Entität (3.1.1), die *Identitätsinformationen* (3.2.4) zur Verfügung stellt

Anmerkung 1 zum Begriff: Typische Operationen, die von einem Identitätsinformationsanbieter durchgeführt werden, sind die Erstellung und Pflege von Identitätsinformationen für Entitäten, die in einer bestimmten Domäne bekannt sind. Ein Identitätsinformationsanbieter und eine Identitätsinformationsstelle können ein und dieselbe Entität sein.

3.3.5

digitaler Ausweis

Darstellung einer *Identität* (3.1.2) zur Verwendung bei der *Authentifizierung* (3.3.1)

Anmerkung 1 zum Begriff: Wie in 5.4 beschrieben, sind die üblichen Ausführungen eines digitalen Ausweises sehr unterschiedlich. Um diesem breiten Spektrum Rechnung zu tragen, ist die in diesem Dokument übernommene Definition sehr allgemein gehalten.

Anmerkung 2 zum Begriff: Ein digitaler Ausweis wird in der Regel zur *Datenauthentifizierung* der Identitätsinformationen der jeweiligen Identität vergeben. Die Datenauthentifizierung wird üblicherweise bei der Autorisierung verwendet.

Anmerkung 3 zum Begriff: Die Identitätsinformationen, die durch einen digitalen Ausweis dargestellt werden, können z. B. auf ein von Menschen lesbares Medium gedruckt oder in einem physischen Token gespeichert sein. In der Regel können solche Informationen so aufbereitet werden, dass ihre wahrgenommene Gültigkeit verstärkt wird.

Anmerkung 4 zum Begriff: Ein digitaler Ausweis kann ein Benutzername, eine PIN, eine Smartcard, ein Token, ein Fingerabdruck, ein Reisepass usw. sein.

3.3.6

Verifizierer

Entität (3.1.1), die die *Verifizierung* (3.2.2) durchführt

Anmerkung 1 zum Begriff: Ein Verifizierer kann mit der Entität, die die Identifizierung von Entitäten für eine bestimmte Domäne kontrolliert, identisch sein oder in deren Namen handeln.

3.3.7

vertrauende Partei

RP, en: relying party

Entität (3.1.1), die sich auf die *Verifizierung* (3.2.2) von *Identitätsinformationen* (3.2.4) für eine bestimmte Entität stützt

Anmerkung 1 zum Begriff: Eine vertrauende Partei ist einem Risiko ausgesetzt, das durch falsche Identitätsinformationen verursacht wird. In der Regel besteht eine Vertrauensbeziehung zu einer oder mehreren Identitätsinformationsstellen.

3.3.8

Identitätsbehauptung

Aussage einer *Identitätsinformationsstelle* (3.3.3), die von einer *vertrauenden Partei* (3.3.7) zur *Authentifizierung* (3.3.1) verwendet wird

Anmerkung 1 zum Begriff: Eine Identitätsbehauptung kann der kryptografische Nachweis einer erfolgreichen Authentifizierung sein, der mit zwischen den Parteien vereinbarten Algorithmen und Schlüsseln erstellt wird, z. B. in einer Föderation einer elektronischen Identität.

3.4 Verwaltung von Identitäten

3.4.1

Identitätsmanagement

IDM

Prozesse und Richtlinien zur Verwaltung des Lebenszyklus und des Wertes, des Typs und der optionalen Metadaten von *Attributen* (3.1.3) in *Identitäten* (3.1.2), die in einer bestimmten *Domäne* (3.2.3) bekannt sind

Anmerkung 1 zum Begriff: Im Allgemeinen ist das Identitätsmanagement an Interaktionen zwischen Parteien beteiligt, bei denen *Identitätsinformationen* (3.2.4) verarbeitet werden.

Anmerkung 2 zum Begriff: Prozesse und Richtlinien im Identitätsmanagement unterstützen gegebenenfalls die Funktionen einer *Identitätsinformationsstelle* (3.3.3), insbesondere um die Interaktion zwischen einer Entität, für die eine Identität verwaltet wird, und der Identitätsinformationsstelle zu handhaben.

3.4.2

Legitimation

Erstauthentifizierung

Verifizierung (3.2.2) auf der Grundlage von *Identitätsnachweisen* (3.4.4), um einen bestimmten Grad an Sicherheit zu erreichen

Anmerkung 1 zum Begriff: In der Regel wird die Legitimation im Rahmen der Registrierung vorgenommen. Ein Identitätsnachweis kann auch bei der Pflege der registrierten Identitätsinformationen erforderlich sein, z. B. bei der Wiederherstellung eines Benutzerkontos.

Anmerkung 2 zum Begriff: Die Legitimation umfasst in der Regel eine Verifizierung der zur Verfügung gestellten Identitätsinformationen und kann Eindeutigkeitsprüfungen, möglicherweise auf der Grundlage biometrischer Verfahren, beinhalten.

Anmerkung 3 zum Begriff: Die Verifizierung für die Legitimation basiert in der Regel auf einer Registrierungsrichtlinie, die die Verifizierungskriterien für den von der Entität zu erbringenden Identitätsnachweis festlegt.

Anmerkung 4 zum Begriff: Die verifizierten *Identitätsinformationen* (3.2.4), die bei der Durchführung der Legitimation gewonnen werden, können in die Registrierung aufgenommen werden und zur Erleichterung der künftigen Identifizierung der Entität dienen.

3.4.3

Registrierung

Verfahren zur Bekanntmachung einer *Entität* (3.1.1) innerhalb einer bestimmten *Domäne* (3.2.3)

Anmerkung 1 zum Begriff: Die Registrierung umfasst in der Regel die Erhebung und Validierung von Identitätsinformationen zur Identifizierung einer Entität und die Erhebung der für die *Identitätsregistrierung* (3.4.6) erforderlichen Identitätsinformationen, auf die die eigentliche Identitätsregistrierung folgt.

3.4.4

Identitätsnachweis

Nachweis der Identität

Informationen, die die Validierung von *Identitätsinformationen* (3.2.4) unterstützen können

Anmerkung 1 zum Begriff: Identitätsnachweise sind die vorgelegten und erhobenen Informationen über eine Entität, die die erforderlichen Attribute für eine erfolgreiche Identifizierung oder Authentifizierung auf einem bestimmten (hohen) Grad an Sicherheit liefern.

3.4.5

Identitätsregister

IMS-Register

Verzeichnis der *Identitäten* (3.1.2)

Anmerkung 1 zum Begriff: Ein typisches Identitätsregister wird durch eine Referenzkennung indiziert.

Anmerkung 2 zum Begriff: Die Identitätsinformationsstelle in einer bestimmten Domäne verwendet in der Regel ihr eigenes Identitätsregister. Ein Identitätsregister kann jedoch von verwandten Domänen gemeinsam genutzt werden, z. B. innerhalb desselben Wirtschaftsunternehmens.

Anmerkung 3 zum Begriff: Die Zuverlässigkeit der Identitätsinformationen in einem Identitätsregister wird durch die bei der Registrierung angewandten Legitimationsrichtlinien bestimmt.

3.4.6

Identitätsanmeldung

Anmeldung

Prozess der Aufzeichnung der *Identitätsinformationen* (3.2.4) einer *Entität* (3.1.1) in einem *Identitätsregister* (3.4.5)

3.4.7

Generator zur Erzeugung der Referenzkennung

Instrument, das bei der *Registrierung* (3.4.3) verwendet wird, um einen neuen eindeutigen Wert für eine *Referenzkennung* (3.1.6) bereitzustellen

BEISPIEL Ein Datenbankmanagementsystem kann als Generator für Referenzkennungen fungieren, wenn es einem neuen Datensatz, der einer Tabelle hinzugefügt wird, eine eindeutige Datensatznummer zuweist, die als Referenzkennung verwendet wird.

3.4.8

Identitätsmanagementsystem

Mechanismus, der Richtlinien, Verfahren, Technologie und andere Ressourcen für die Pflege von *Identitätsinformationen* (3.2.4) einschließlich zugehöriger Metadaten umfasst

Anmerkung 1 zum Begriff: Ein Identitätsmanagementsystem wird in der Regel zur *Identifizierung* (3.2.1) oder *Authentifizierung* (3.3.1) von Entitäten eingesetzt. Es kann zur Unterstützung anderer automatisierter Entscheidungen auf der Grundlage von Identitätsinformationen für eine in der Domäne des Identitätsmanagementsystems erkannte Entität eingesetzt werden.

[QUELLE: ISO/IEC 24760-2:2015, 3.3, modifiziert — in der Anmerkung 1 zum Begriff wurde „Anwendungs“ vor „domäne“ gestrichen.]

3.4.9

Registrierungsstelle

RA, en: registration authority

Entität (3.1.1), die sich auf eine bestimmte *Domäne* (3.2.3) bezieht und für die *Registrierung* (3.4.3), die *Legitimation* (3.4.2) und die *Identitätsregistrierung* (3.4.6) zuständig ist

3.4.10

Aussteller des digitalen Ausweises

Entität (3.1.1), die für die Bereitstellung eines *digitalen Ausweises* (3.3.5) für eine(n) Betroffene(n) (3.1.7) in einer bestimmten *Domäne* (3.2.3) zuständig ist

Anmerkung 1 zum Begriff: Ein *digitaler Ausweis* (3.3.5), der von einem Aussteller des digitalen Ausweises bereitgestellt wird, kann eine physische Form haben, z. B. eine Mitgliedskarte (Chipkarte).

Anmerkung 2 zum Begriff: Die Ausstellung eines *digitalen Ausweises* (3.3.5) für eine(n) *Betroffene(n)* (3.1.7) kann als *Attribut* (3.1.3) für den/die Betroffene(n) erfasst werden, z. B. durch Aufzeichnung der eindeutigen Nummer des ausgestellten Tokens.

Anmerkung 3 zum Begriff: Ein von einem Aussteller bereitgestellter *digitaler Ausweis* (3.3.5) kann aus einem Benutzernamen und einem Passwort bestehen. Ein digitaler Ausweis in Form einer Chipkarte oder eines ähnlichen Sicherheitsinstruments kann so konfiguriert werden, dass er ein Passwort offline validiert.

3.4.11

Zertifizierungsdienstanbieter

CSP, en: credential service provider

vertrauenswürdige *Entität* (3.1.1), die mit einer bestimmten *Domäne* (3.2.3) verbunden ist und für die Verwaltung der in dieser Domäne ausgestellten *digitalen Ausweise* (3.3.5) zuständig ist

Anmerkung 1 zum Begriff: Es ist möglich, dass ein CSP als Aussteller von *digitalen Ausweisen* (3.4.10) fungiert.

3.5 Föderation

3.5.1

föderierte Identität

Identität (3.1.2) zur Nutzung in mehreren *Domänen* (3.2.3)

Anmerkung 1 zum Begriff: Einige oder alle Domänen, in denen eine föderierte Identität verwendet werden kann, können formell zu einer Identitätsföderation zusammengeschlossen werden. Identitätsinformationsanbieter von Domänen in der Föderation können gemeinsam eine föderierte Identität verwalten.

Anmerkung 2 zum Begriff: Die föderierte Identität kann dauerhaft oder temporär sein.

3.5.2

Identitätsföderation

Vereinbarung zwischen zwei oder mehr *Domänen* (3.2.3), in der festgelegt wird, wie *Identitätsinformationen* (3.2.4) zum Zwecke der domänenübergreifenden *Identifizierung* (3.2.1) ausgetauscht und verwaltet werden sollen

Anmerkung 1 zum Begriff: Die Einrichtung einer Identitätsföderation umfasst in der Regel eine Vereinbarung über die Verwendung gemeinsamer Protokolle und Verfahren zu Steuerungsmaßnahmen für den Datenschutz, die Datensicherheit und das Auditing. In der Föderationsvereinbarung kann die Verwendung von genormten Datenformaten und kryptografischen Techniken festgelegt werden.

Anmerkung 2 zum Begriff: Die Föderationsvereinbarung kann die Grundlage für Identitätsstellen in jedem der Anwendbarkeitsdomänen sein, um gegenseitig digitale Ausweise für die Autorisierung anzuerkennen.

3.6 Datenschutz

In Rechtsordnungen, in denen bestimmten Arten von Rechtsträgern das Recht auf Datenschutz gewährt wird, ist der Begriff ‚Person‘ in den folgenden Definitionen so auszulegen, dass er auch solche Entitäten einschließt; andernfalls wird der Begriff ‚Person‘ in Bezug auf eine einzelne menschliche Person verwendet.

3.6.1

selektive Offenlegung

Prinzip des *Identitätsmanagements* (3.4.1), das einer Person ein gewisses Maß an Steuerungsmaßnahmen über die *Identitätsinformationen* (3.2.4) gibt, die an einen Dritten übertragen werden können, z. B. bei der *Authentifizierung* (3.3.1)

3.6.2

minimale Offenlegung

Grundsatz des *Identitätsmanagements* (3.4.1), wonach die Anforderung oder Übermittlung von *Identitätsinformationen* (3.2.4) an Dritte auf die für einen bestimmten Zweck unbedingt erforderlichen Informationen beschränkt wird

Anmerkung 1 zum Begriff: Der Grundsatz der Verhältnismäßigkeit bezieht sich auf die minimale Offenlegung, sofern der Aufwand der Steuerungsmaßnahmen im Verhältnis zur Tätigkeit angemessen ist.

3.6.3

Pseudonym

Identifikator (3.1.4), der die minimalen *Identitätsinformationen* (3.2.4) enthält, die ausreichen, damit ein *Verifizierer* (3.3.6) ihn als Verbindung zu einer bekannten *Identität* (3.1.2) herstellen kann

Anmerkung 1 zum Begriff: Ein Pseudonym kann verwendet werden, um die Risiken für die Privatsphäre zu verringern, die mit der Verwendung von Identifikatoren mit festen oder bekannten Werten verbunden sind.

Anmerkung 2 zum Begriff: Ein Pseudonym kann ein Identifikator mit einem von der Person gewählten oder zufällig zugewiesenen Wert sein.

3.6.4

kurzlebiger Identifikator

Identifikator (3.1.4) mit begrenzter Gültigkeitsdauer

Anmerkung 1 zum Begriff: In der Regel wird einem Subjekt ein kurzlebiger Identifikator als kryptografischer digitaler Ausweis zur Verfügung gestellt, um eine *authentifizierte Identität* (3.3.2) darzustellen.

Anmerkung 2 zum Begriff: Üblicherweise kann ein kurzlebiger Identifikator nur in der *Domäne* (3.2.3) verifiziert werden, die ihn erstellt hat, möglicherweise auch in mit dieser Domäne föderierten Domänen.

3.6.5

Blindbestätigung

Grundsatz des *Identitätsmanagements* (3.4.1), keine *Identitätsinformationen* (3.2.4) für eine *Entität* (3.1.1) an Dritte weiterzugeben, außer einer Erklärung, dass die Entität in einer *Domäne* (3.2.3) bekannt ist

Anmerkung 1 zum Begriff: Die Blindbestätigung bietet ein hohes Maß an Schutz für die Privatsphäre eines/einer *Betroffenen* (3.1.7).

Anmerkung 2 zum Begriff: Die Blindbestätigung kann mit einem *kurzlebigen Identifikator* (3.6.4) oder einem Pseudonym realisiert werden.

4 Symbole und Abkürzungen

IKT	Informations- und Kommunikationstechnologie
IDM	Identitätsmanagement
IIP	Identitätsinformationsanbieter (en: Identity Information Provider)
IIA	Identitätsinformationsstelle (en: Identity Information Authority)
RI	Referenzkennung (en: Reference Identifier)
RP	vertrauende Partei (en: Relying Party)
SSO	einmalige Anmeldung (en: Single Sign On)
URI	einheitlicher Identifikator für Ressourcen (en: Uniform Resource Locator)
UUID	Identifikationsschlüssel (en: Universal Unique Identifier)

5 Identität

5.1 Allgemeines

Eine Identität repräsentiert eine Entität in einem IKT-System als zu speichernde oder zu verarbeitende Daten. Die (geschäftlichen) Zwecke einer bestimmten Anwendungsdomäne, die von einem IKT-System bedient wird, bestimmen, welche der zu einer Entität gehörenden Attribute in ihrer Identität verwendet werden sollen. Eine dauerhaft gespeicherte Identität ist die Grundlage für die Identifizierung eines/einer Betroffenen. Wenn eine dauerhafte Identität kein Identifikator ist, kann die Identifizierung zusätzliche Informationen vom/von der Betroffenen erfordern.

Eine Identität kann ganz oder teilweise durch einen dem/der Betroffenen ausgestellten digitalen Ausweis dargestellt werden. Wenn eine Identität durch einen solchen digitalen Ausweis repräsentiert wird, kann ein Identifikator für den digitalen Ausweis in die registrierte Identität aufgenommen werden.

Dieses Dokument betrachtet jede Menge von Attributen, die eine bestimmte Entität beschreiben, als Identität für die Entität. In einigen Domänen können die dauerhaft gespeicherten Identitätsinformationen für verschiedene Entitäten identisch sein. In diesem Fall werden bei der Identifizierung zusätzliche Informationen verwendet, um eine Entität bei Bedarf als eigenständig zu erkennen. In anderen Normen, z. B. ITU-T X1252 [13], ist der ausdrückliche Zweck einer Identität die Fähigkeit der Identitätsinformationen, Entitäten voneinander zu unterscheiden, soweit dies für Anwendungen in einer Domäne relevant ist („im Kontext“).

Eine Entität kann mehrere Identitäten haben, wobei sich jede Identität auf mindestens eine Domäne bezieht. Eine Entität kann mehrere Identitäten haben, die sich auf dieselbe Domäne beziehen. Einige Identitäten einer Entität können in keiner Domäne eindeutig sein.

ANMERKUNG 1 Der Begriff Entität wird in einem weiteren Sinn verstanden. Sie repräsentiert eine natürliche Person, eine moralische oder juristische Person (Institution, Unternehmen), ein Objekt (Informationen, ein System, ein Gerät) oder eine Gruppe dieser individuellen Entitäten.

ANMERKUNG 2 Ein Mensch ist eine Entität in diesem Dokument und hat eine einzige, vollständige Existenz. Sie kann durch viele verschiedene Attribute beschrieben werden. Unterschiedliche Mengen dieser Attribute bilden unterschiedliche Identitäten für ein und dieselbe menschliche Entität.

Wenn eine Identität in einer bestimmten Domäne nicht eindeutig ist, kann sie dazu dienen, eine Gruppe von Entitäten in dieser Domäne, die ein oder mehrere Merkmale gemeinsam haben, von anderen Entitäten zu unterscheiden, die ein solches Merkmal nicht haben.

Die Identität einer Entität dient dazu, relevante Informationen über die Entität bei ihren Interaktionen mit den von einer Domäne bereitgestellten Diensten und dem Zugriff auf Ressourcen bekannt zu machen. Eine Domäne legt die Art und den Bereich der zulässigen Werte von Attributen fest, die zur Identifizierung oder für andere Zwecke verwendet werden sollen.

ANMERKUNG 3 In einigen Fällen kann der Begriff „partielle Identität“ verwendet werden, um sich auf eine bestimmte Menge von Attributen zu beziehen, die aus einer größeren Menge von Attributen entnommen wurden, die im Gegensatz dazu als die vollständige Identität — alle verfügbaren Attribute — einer Entität in einer Domäne bezeichnet werden kann. Die Vorzugsbenennung in diesem Dokument ist Identität.

Eine Domäne sollte ein Identitätsmanagementsystem einsetzen, das der Normenreihe ISO/IEC 24760 entspricht, um die Identitätsinformationen der Entitäten zu verwalten, die sie erkennen will.

5.2 Identitätsinformationen

Informationen, die zu einer bestimmten Entität in einer Domäne gehören, werden als Identitätsinformationen bezeichnet.

Wenn eine gegebene Identitätsinformation eine Entität im Kontext eines bestimmten Anwendungsfalls ausreichend von anderen unterscheidet, dann ist diese Identitätsinformation eine *unterscheidende Identität*.

Wenn die Kombination der in der Identitätsinformation enthaltenen Werte in der Domäne eindeutig ist, dann ist diese Identitätsinformation ein *Identifikator* der Entität.

Wenn eine neue Identität für eine Entität in einer Domäne erstellt wird, kann ein Identitätsinformationsanbieter für die Domäne Werte für erforderliche Attribute der neuen Identität erstellen. Die neuen Attribute können bestehen aus:

- allen Informationen, die erforderlich sind, um die Interaktion zwischen der Domäne und der Entität, für die die Identität erstellt wird, zu erleichtern;
- allen für die künftige Identifizierung der Entität erforderlichen Informationen, einschließlich der Beschreibung von Aspekten der physischen Existenz der Entität;
- allen Informationen, die für die künftige Authentifizierung der Identität der Entität erforderlich sind; oder
- einer oder mehreren Referenzkennung(en).

Die neuen Identitätsinformationen können aus den Identitätsinformationen für die in der aktuellen oder einer anderen Domäne erstellten Entität abgeleitet werden. Die Ableitung von Informationen kann das Kopieren, das Abgleichen oder das Erstellen eines Pseudonyms beinhalten.

Die Domäne muss nachprüfen, dass die erstellten Identitätsinformationen genau zu der Entität gehören.

Identitätsinformationen können mit Metadaten verknüpft werden, die z. B. ihren Ursprung, ihren Verwendungszweck und ihre Gültigkeitsdauer angeben. Metadaten zu Identitätsinformationen können selbst Identitätsinformationen sein und können in die Identität, auf die sie sich beziehen, aufgenommen werden.

Identitätsinformationen und die damit verbundenen Metadaten können geändert werden. Die Verfahren und Bedingungen für das Ändern, Aktualisieren und Erstellen von Identitätsinformationen müssen in geeigneten Richtlinien festgelegt werden. Zu diesen Maßnahmen kann auch das Führen von Aufzeichnungen für Auditzwecke gehören. Diese Richtlinien können zwischen einer Reihe von Aufgaben und Aktivitäten im Zusammenhang mit dem Identitätslebenszyklus (siehe 7.2) unterscheiden, darunter:

- Anforderung und Erhalt von Informationen aus externen Quellen;
- Verifizierung und Validierung;
- Qualifizierung und Einstufung;
- Aufzeichnung;
- Bereitstellung;
- Archivierung; und
- Löschung.

5.3 Identifikator

Das eindeutige Attribut oder die eindeutigen Attribute in einer Identität, die als Identifikator verwendet werden, können

- der Entität zur ausschließlichen Nutzung in der Ursprungsdomäne zur Verfügung stehen, oder
- für die Verwendung in anderen Domänen als der Ursprungsdomäne geeignet sein.

Ein Identifikator kann in einer Ursprungsdomäne von Grund auf neu konstruiert werden, er kann das Ergebnis einer Beobachtung sein oder auf vorgelegten Identifikatoren basieren.

ANMERKUNG 1 In einigen Fällen, z. B. bei der einmaligen Anmeldung, kann ein Identifikator mit dem Ziel erstellt werden, auch außerhalb der Ursprungsdomäne verwendet zu werden.

ANMERKUNG 2 In einigen Fällen reicht der Identifikator allein nicht aus, um die Entität von einer anderen Entität in einer anderen Domäne als der Ursprungsdomäne zu unterscheiden. In diesem Fall kann die andere Domäne, abhängig von der Verwendung des Identifikators, zusätzliche Identitätsinformationen benötigen. Ein Beispiel hierfür ist ein Bibliotheksausweis, der die Mitgliedsnummer als Identifikator enthält und auch den regulären Zugang zu einem Museum ermöglicht, wo diese zusätzliche Information abgefragt wird, wenn das Museum eine Ausstellung hat, die ab einem bestimmten Alter zugänglich ist.

5.4 Digitaler Ausweis

5.4.1 Allgemeines

Ein digitaler Ausweis kann in verschiedenen Formaten vorliegen:

- als Informationen, die nur dem/der Betroffenen und dem Identitätsmanagementsystem bekannt sind, z. B. ein Passwort, eine PIN, eine Passphrase;