DIN EN ISO/IEC 24760-1

ICS 35.030

IT-Sicherheit und Datenschutz – Rahmenwerk für Identitätsmanagement – Teil 1: Terminologie und Konzept (ISO/IEC 24760-1:2019); Deutsche Fassung EN 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 version EN 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 EN ISO/IEC 24760-1:2022

Gesamtumfang 38 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

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 EN ISO/IEC 24760-1:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-04-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

DIN EN ISO/IEC 29101, *Informationstechnik — Sicherheitstechniken — Architekturrahmenwerk für Datenschutz*

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 24760-1

Juni 2022

ICS 35.030

Deutsche Fassung

IT-Sicherheit und Datenschutz — 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)

Diese Europäische Norm wurde vom CEN am 6. Juni 2022 angenommen.

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





CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

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 Einschreibung . . . 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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

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 EN ISO/IEC 24760-1:2022 durch das Technische Komitee CEN-CENELEC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2023, und etwaige entgegenstehende nationale Normen müssen bis Januar 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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 und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, 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/IEC 24760-1:2019 wurde von CEN-CENELEC als EN ISO/IEC 24760-1:2022 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-1:2023-03

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, *IT 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

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
Gegenstand, 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 Verkörperung 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-T X1252 [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.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-1:2023-03

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 von anderen zu unterscheiden.

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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-1:2023-03

[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.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-1:2023-03