DIN EN ISO/IEC 24760-2

DIN

ICS 35.030

Informationstechnik – Sicherheitsverfahren – Rahmenwerk für Identitätsmanagement – Teil 2: Referenzarchitektur und Anforderungen (ISO/IEC 24760-2:2015); Deutsche Fassung EN ISO/IEC 24760-2:2022

Information technology –
Security techniques –
A framework for identity management –
Part 2: Reference architecture and requirements (ISO/IEC 24760-2:2015);
German version EN ISO/IEC 24760-2:2022

Technologies de l'information –
Techniques de sécurité –
Cadre pour la gestion de l'identité –
Partie 2: Architecture de référence et exigences (ISO/IEC 24760-2:2015);
Version allemande EN ISO/IEC 24760-2:2022

Gesamtumfang 63 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

Nationales Vorwort

Der Text von ISO/IEC 24760-2:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 24760-2:2022 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 Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

ISO/IEC 24760-1	siehe	DIN EN ISO/IEC 24760-1
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 24760-1, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 1: Terminologie und Konzept*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 24760-2

September 2022

ICS 35.030

Deutsche Fassung

Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 2: Referenzarchitektur und Anforderungen (ISO/IEC 24760-2:2015)

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

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité — Partie 2: Architecture de référence et exigences (ISO/IEC 24760-2:2015)

Diese Europäische Norm wurde vom CEN am 5. September 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 24760-2:2023-03

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Symbole und Abkürzungen 8
5 Referenzarchitektur 8
5.1 Allgemeines 8
5.2 Architekturelemente 9
5.2.1 Überblick 9
5.2.2 Sichtweisen 9
5.3 Kontextsicht 10
5.3.1 Interessengruppen 10
5.3.2 Akteure 13
5.3.3 Kontextmodell 19
5.3.4 Anwendungsfallmodell 20
5.3.5 Einhaltungs- und Führungsmodell 22
5.4 Funktionale Sicht 23
5.4.1 Komponentenmodell 23
5.4.2 Prozesse und Dienste 24
5.4.3 Physisches Modell 31
5.5 Identitätsmanagementszenarien 31
5.5.1 Allgemeines 31
5.5.2 Unternehmensszenario 31
5.5.3 Föderiertes Szenario 31
5.5.4 Dienstszenario 32
5.5.5 Heterogenes Szenario 32
6 Anforderungen an das Management von Identitätsinformationen 32
6.1 Allgemeines 32
6.2 Zugangsrichtlinie für Identitätsinformationen 32
6.3 Funktionale Anforderungen für das Management von Identitätsinformationen 33
6.3.1 Richtlinie für den Lebenszyklus von Identitätsinformationen 33
6.3.2 Bedingungen und Verfahren zur Beendigung oder Löschung einer Identität 33
6.3.3 Schnittstelle für Identitätsinformationen 34
6.3.4 Referenzkennung 34
6.3.5 Qualität der Identitätsinformationen und Einhaltung 36
6.3.6 Archivierung von Informationen 36
6.3.7 Beendigung und Löschung von Identitätsinformationen 36
6.4 Nicht-funktionale Anforderungen 37
Anhang A (informativ) **Rechtliche und behördliche Aspekte** 38
Anhang B (informativ) **Anwendungsfallmodell** 39
Anhang C (informativ) **Komponentenmodell** 43
C.1 Modell 43
C.2 UML-Legende 44
Anhang D (informativ) **Anwendungsfallmodell** 46
D.1 Allgemeines 46
D.2 Einwilligungsmanagement 46
D.3 Management des Lebenszyklus von Zugangsdaten 48
D.4 Management von Konfigurationsdaten 50
D.5 Richtlinienmanagement 51

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

D.6 Management des Lebenszyklus von Betroffenen 54
Literaturhinweise 59

Bilder

Bild 1 — Kontextmodell für das Identitätsmanagement 20
Bild 2 — Basisanwendungsfall für Identitätsinformationen 21
Bild B.1 — Beispielhaftes Anwendungsfalldiagramm für ein Identitätsmanagementsystem 42
Bild B.2 — Beispiel einer formalisierten Anwendungsfallbeschreibung 42
Bild C.1 — Funktionskomponenten in einem Identitätsmanagementsystem 44
Bild C.2 — Graphische Elemente in einem UML-Komponentendiagramm 44
Bild D.1 — Prozessdiagramm für das Einwilligungsmanagement 46
Bild D.2 — Prozessdiagramm für das Management des Lebenszyklus von Zugangsdaten 48
Bild D.3 — Prozessdiagramm für das Management von Konfigurationsdaten 50
Bild D.4 — Prozessdiagramm für Richtlinien- und Konformitätsmanagement 52
Bild D.5 — Prozessdiagramm für das Management des Lebenszyklus von Betroffenen 54
Bild D.6 — Prozessdiagramm für den Abgleich von Identitätsinformationen 55
Bild D.7 — Lebenszyklusdiagramm für den Lebenszyklus des Identitätsinformationsmanagements 56

Tabellen

Tabelle 1 — Überblick über die im Rahmen von Identitätsinformationsmanagementprozessen ausgetauschten Informationen 25
Tabelle 2 — Überblick über die in bestimmten Identitätsmanagementprozessen ausgetauschten Informationen 26
Tabelle 3 — Überblick über die Informationen, die in zusätzlichen Funktionen des Identitätsmanagementsystems ausgetauscht werden 29
Tabelle B.1 — Im Anwendungsfalldiagramm dargestellte Akteure 39
Tabelle B.2 — Zusammenfassende Definition der Anwendungsfälle für ein Identitätsmanagementsystem 40
Tabelle C.1 — Funktionskomponenten eines Identitätsmanagementsystems 43
Tabelle C.2 — Terminologie des UML-Komponentendiagramms 45
Tabelle D.1 — Beschreibung des Geschäftsprozesselements für das Einwilligungsmanagement . 47
Tabelle D.2 — Beschreibung des Geschäftsprozesselements für das Management des Lebenszyklus von Zugangsdaten 49
Tabelle D.3 — Beschreibung des Geschäftsprozesselements für das Konfigurationsmanagement 51
Tabelle D.4 — Beschreibung des Geschäftsprozesselements für das Richtlinien- und Konformitätsmanagement 53
Tabelle D.5 — Beschreibung der Geschäftsprozesselemente im Lebenszyklus des Betroffenen . . 56

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

Europäisches Vorwort

Der Text von ISO/IEC 24760-2:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als EN ISO/IEC 24760-2:2022 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 März 2023, und etwaige entgegenstehende nationale Normen müssen bis März 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 24760-2:2015 wurde von CEN als EN ISO/IEC 24760-2:2022 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

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. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

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).

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

Bezüglich einer Erklärung der Bedeutung ISO-spezifischer Ausdrücke im Zusammenhang mit Konformitätsbewertung sowie Informationen über die Einhaltung der Prinzipien der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT) seitens ISO siehe folgende URL: www.iso.org/iso/foreword.html.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Security techniques*.

ISO/IEC 24760 mit dem Haupttitel *Information technology — Security techniques — A framework for identity management* besteht aus den folgenden Teilen:

— *Part 1: Terminology and concepts*

— *Part 2: Reference architecture and requirements*

Der folgende Teil ist in Vorbereitung:

— *Part 3: Practice*

Weitere Teile werden möglicherweise folgen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

Einleitung

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

Um der Notwendigkeit Rechnung zu tragen, Systeme, die identitätsbasierte Entscheidungen treffen, effizient und effektiv zu implementieren, legt dieser Teil von ISO/IEC 24760 ein Rahmenwerk für die Ausgabe, Verwaltung und Verwendung von Daten fest, das dazu dient, 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.

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.

Dieser Teil von ISO/IEC 24760 definiert eine Referenzarchitektur für ein Identitätsmanagementsystem, die die wichtigsten Architekturelemente und deren Zusammenhänge enthält. Diese Architekturelemente werden in Bezug auf die Modelle für das Identitätsmanagement beschrieben. Dieser Teil von ISO/IEC 24760 legt die Anforderungen an das Design und die Implementierung eines Identitätsmanagementsystems fest, so dass es die Ziele der an der Einführung und dem Betrieb des Systems beteiligten Interessengruppen erfüllen kann.

Dieser Teil von ISO/IEC 24760 soll eine Grundlage für die Implementierung anderer internationaler Normen im Zusammenhang mit der Verarbeitung von Identitätsinformationen bilden, wie z. B.

— ISO/IEC 29100, *Information technology — Security techniques — Privacy framework,*

— ISO/IEC 29101, *Information technology — Security techniques — Privacy reference architecture,*

— ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework* und

— ISO/IEC 29146, *Information technology — Security techniques — A framework for access management.*

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

1 Anwendungsbereich

Dieser Teil von ISO/IEC 24760

— enthält Leitlinien für die Implementierung von Systemen zum Management von Identitätsinformationen und

— legt Anforderungen für die Implementierung und den Betrieb eines Rahmenwerks für das Identitätsmanagement fest.

Dieser Teil von ISO/IEC 24760 ist anwendbar für jedes Informationssystem, in dem identitätsrelevante Informationen verarbeitet oder gespeichert werden.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument als Ganzes oder teilweise zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. 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 24760-1, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 24760-1 und die folgenden Begriffe.

3.1
dokumentiertes Design
maßgebliche Beschreibung struktureller, funktionaler und betrieblicher Systemaspekte

Anmerkung 1 zum Begriff: Ein dokumentiertes Design ist die Dokumentation, die als Anleitung für die Implementierung eines IKT-Systems dient.

Anmerkung 2 zum Begriff: Ein dokumentiertes Design umfasst in der Regel die Beschreibung einer konkreten Architektur des IKT-Systems.

3.2
Identitätsmanagementstelle
Stelle, die für die Festlegung und Durchsetzung von Betriebsrichtlinien für ein *Identitätsmanagementsystem* (3.3) zuständig ist

Anmerkung 1 zum Begriff: Eine Identitätsmanagementstelle gibt in der Regel das Design, die Implementierung und den Einsatz eines Identitätsmanagementsystems in Auftrag.

BEISPIEL Die Führungsebene eines Unternehmens, das ein Identitätsmanagementsystem zur Unterstützung seiner Dienste einsetzt.

3.3
Identitätsmanagementsystem
Mechanismus, der Richtlinien, Verfahren, Technologie und andere Ressourcen für die Pflege von Identitätsinformationen einschließlich zugehöriger Metadaten umfasst

Anmerkung 1 zum Begriff: Ein Identitätsmanagementsystem wird in der Regel zur Identifizierung oder Authentifizierung von Entitäten eingesetzt. Es kann zur Unterstützung anderer automatisierter Entscheidungen auf der Grundlage von

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

Identitätsinformationen für eine in der Anwendungsdomäne des Identitätsmanagementsystems erkannte Entität eingesetzt werden.

3.4
Betroffener
Subjekt
Entität, auf die sich die Identitätsinformationen in einem *Identitätsmanagementsystem* (3.3) beziehen

Anmerkung 1 zum Begriff: Im Zusammenhang mit den Anforderungen an den Datenschutz bezieht sich ein Betroffener auf eine Person.

3.5
Außerkraftsetzung
Prozess, der in einem *Identitätsmanagementsystem* (3.3) durchgeführt wird, wenn ein bestimmtes Attribut für eine bestimmte Entität nicht mehr gültig ist, um das Attribut für die künftige Verwendung als ungültig zu kennzeichnen

Anmerkung 1 zum Begriff: Die Außerkraftsetzung von Attributen darf Teil der Aktualisierung des Attributwerts sein, z. B. bei einer Adressänderung.

Anmerkung 2 zum Begriff: Die Außerkraftsetzung erfolgt in der Regel für ein Attribut, das vor Ablauf des ihm zugeordneten Gültigkeitszeitraums als nicht mehr gültig eingestuft wird.

Anmerkung 3 zum Begriff: Der Begriff „Widerruf“ wird üblicherweise für die Außerkraftsetzung von Attributen verwendet, bei denen es sich um Zugangsdaten handelt.

Anmerkung 4 zum Begriff: Die Außerkraftsetzung erfolgt in der Regel unmittelbar nach der Festlegung, dass ein Attribut für eine bestimmte Entität nicht mehr gültig ist.

3.6
Regulierungsstelle
Stelle, die durch Gesetz, Verordnung oder Vereinbarung beauftragt und ermächtigt ist, den Betrieb von *Identitätsmanagementsystemen* (3.3) zu überwachen

3.7
Interessengruppe
Einzelperson, Team, Organisation oder Klassen davon, die ein Interesse an einem System haben

[QUELLE: ISO/IEC 42010]

4 Symbole und Abkürzungen

IKT	Informations- und Kommunikationstechnologie
IMS	Identitätsmanagementsystem
pbD	personenbezogene Daten

5 Referenzarchitektur

5.1 Allgemeines

Dieser Abschnitt beschreibt die Architekturelemente eines Identitätsmanagementsystems und deren Zusammenhänge.

Das dokumentierte Design der Architektur eines Identitätsmanagementsystems sollte auf ISO/IEC 42010 beruhen.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

ANMERKUNG Die in dieser Norm definierte Referenzarchitektur und Architekturbeschreibung beruhen auf ISO/IEC 42010.

Das dokumentierte Design der Architektur eines Identitätsmanagementsystems sollte das System in seinem Einsatzkontext auf der Grundlage der in diesem Teil von ISO/IEC 24760 definierten *Interessengruppen* und *Akteuren* festlegen. Bei den Akteuren auf Geschäftsebene handelt es sich um Interessengruppen. Einige Interessengruppen interagieren nicht mit dem System. Das dokumentierte Design muss die Anforderungen sowohl der Akteure als auch der Nicht-Akteure berücksichtigen. Das dokumentierte Design muss eine vollständige Beschreibung der Akteure enthalten.

Ein dokumentiertes Design eines Identitätsmanagementsystems, das diesem Teil von ISO/IEC 24760 entspricht, sollte eine geeignete Architekturbeschreibungssprache und Referenzarchitekturkomponenten und -funktionen nach den in dieser Internationalen Norm definierten Begriffen verwenden.

5.2 Architekturelemente

5.2.1 Überblick

Elemente in dieser Referenzarchitektur sind:

— Interessengruppen (5.3.1),

— Akteure (5.3.2),

— Sichten (5.3, 5.4),

— Modelle (5.3.3, 5.3.4, 5.3.5, 5.4.1, 5.4.3),

— Komponenten (5.4.1),

— Prozesse (5.4.2) und

— Informationsflüsse und Aktionen (5.4.2).

5.2.2 Sichtweisen

5.2.2.1 Allgemeines

Das dokumentierte Design eines Identitätsmanagementsystems muss eine kontextbezogene und eine funktionale Sicht umfassen. Es darf eine physische Sicht einschließen. Das dokumentierte Design darf weitere Sichten enthalten, z. B. eine Informationssicht.

ANMERKUNG Das erforderliche Mindestmaß an Sichtweisen beschreibt die Interaktionen des Systems mit seiner Umgebung sowie die internen Komponenten und Interaktionen des Systems.

Die Beschreibung einer Sicht sollte zielgerichtet sein. Die Diagramme in den Beschreibungen der Sichten sollten mit einem Text versehen werden, der die dargestellten Elemente definiert.

ANMERKUNG Die Beschreibung der Sichtweisen in diesem Abschnitt beruht auf Literaturhinweis [2].

5.2.2.2 Kontextsicht

Definition — Im dokumentierten Design beschreibt die Kontextsicht die Beziehungen, Abhängigkeiten und Interaktionen zwischen dem System und seiner Umgebung (die Menschen, Systeme und externen Entitäten, mit denen es interagiert).

Belange — Anwendungsbereich und Zuständigkeiten des Systems, Identität der externen Entitäten und der verwendeten Dienste und Daten, Art und Merkmale der externen Stellen, Identität und Zuständigkeiten der

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 24760-2:2023-03

externen Schnittstellen, Art und Merkmale der externen Schnittstellen, sonstige externe Abhängigkeiten, Auswirkungen des Systems auf seine Umgebung sowie Gesamtvollständigkeit, Konsistenz und Kohärenz.

Modelle — Eine Kontextsicht darf ein Kontextmodell, Anwendungsfälle und Interaktionsszenarien enthalten. Das Kontextmodell ist ein informelles Boxen- und Liniendiagramm, das das betrachtete System als Black-Box mit Schnittstellen, Interaktionen auf oberster Ebene und Abhängigkeiten von externen Entitäten darstellt. Siehe 5.3.3.

Zu beachtende Punkte — Fehlende oder falsche externe Entitäten, fehlende implizite Abhängigkeiten, lockere oder ungenaue Schnittstellenbeschreibungen, unangemessene Detailgenauigkeit, schleichende Ausweitung des Anwendungsbereichs, impliziter oder angenommener Kontext oder Anwendungsbereich, zu komplizierte Interaktionen, übermäßige Verwendung von Fachjargon.

5.2.2.3 Funktionale Sicht

Definition — Im dokumentierten Design beschreibt die funktionale Sicht die wichtigsten funktionalen Elemente mit operativen Verantwortlichkeiten, Schnittstellen und primären Interaktionen.

Belange — Bezieht sich auf funktionale Fähigkeiten, externe Schnittstellen, interne Struktur und funktionale Designphilosophie.

Modelle — Eine funktionale Sicht darf ein Komponentenmodell, ein physisches Modell oder ein Infrastrukturmodell enthalten.

Im dokumentierten Design muss die funktionale Sicht die Normen und Leitlinien aufzeigen, die für jede der beschriebenen Funktionen gelten.

Siehe 5.4 für eine Anleitung zur Angabe einer Funktionssicht.

5.3 Kontextsicht

5.3.1 Interessengruppen

5.3.1.1 Allgemeines

Dieser Teil von ISO/IEC 24760 erkennt die folgenden direkten und indirekten Interessengruppen als besonders wichtig an

— Betroffener,

— Identitätsmanagementstelle,

— Identitätsinformationsstelle,

— vertrauende Partei,

— Regulierungsstelle,

— Auditor und

— Vertreter oder Schützer der Verbraucher/Bürger.

Jede Interessengruppe hat eine eigene Funktion im Identitätsmanagementsystem. Diese Funktionen bringen bestimmte Verantwortlichkeiten und Verpflichtungen mit sich. Mit Ausnahme von Regulierungsstellen und Verbrauchervertretern interagieren die Interessengruppen mit einem Identitätsmanagementsystem und sind daher in der Referenzarchitektur als Akteure vertreten (siehe 5.3.2).

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

Die Belange der Interessengruppen in einem Identitätsmanagementsystem werden in den folgenden Unterabschnitten beschrieben und sollten bei Design, Implementierung und Betrieb des Systems berücksichtigt werden.

5.3.1.2 Betroffener

Zu den Belangen eines Betroffenen in einem Identitätsmanagementsystem gehören:

— die Richtigkeit der erhobenen, verarbeiteten und gespeicherten Identitätsinformationen,

— der Datenschutz,

— Minimierung der vom Identitätsmanagementsystem erhobenen, verarbeiteten und gespeicherten Identitätsinformationen,

— Minimierung der Nutzung von Identitätsinformationen durch das Identitätsmanagementsystem in seiner Anwendbarkeitsdomäne,

— Fehler bei der Identifizierung, einschließlich falsch negativer und falsch positiver Identifizierung, sowie die Erkennung und Behandlung von Fehlern,

— Wissen und Einwilligung zur Weitergabe von Identitätsinformationen an Dritte,

— korrekte Darstellung durch erhobene, verarbeitete oder gespeicherte Identitätsinformationen,

— die Richtigkeit der Vorgänge bei der Erbringung von Diensten und der Zugang zu Ressourcen, die auf der Grundlage der in einer bestimmten Situation vorliegenden Attribute zur Verfügung gestellt werden,

— die Erhebung, Verarbeitung und Speicherung von Identitätsinformationen nur mit seiner Einverständniserklärung erfolgt,

— eine gerechte Behandlung bei seinen Interaktionen mit dem System und

— eine leicht verständliche, effektive und angemessene Benutzungsschnittstelle.

ANMERKUNG Belange eines Betroffenen, die sich auf einen Dienst eines Dritten beziehen, der Identitätsinformationen aus dem Identitätsmanagementsystem verwendet, sind keine Belange des Identitätsmanagementsystems und fallen daher nicht in den Anwendungsbereich dieser Norm.

5.3.1.3 Identitätsmanagementstelle

Zu den Belangen der Identitätsmanagementstelle in einem Identitätsmanagementsystem gehören:

— die Definition der Ziele des Identitätsmanagements für die vom Identitätsmanagementsystem bediente(n) Domäne(n),

— die Spezifikation von Richtlinien zur Aufrechterhaltung der Identitätsmanagementziele für die vom Identitätsmanagementsystem bediente(n) Domäne(n),

— die Erfüllung der Geschäftsziele des Identitätsmanagementsystems in Bezug auf Betroffene und Benutzer von Identitätsinformationen,

— dass die von den einzelnen Betroffenen bereitgestellten Identitätsinformationen zutreffend sind und sich mit einer bestimmten Vertrauenswürdigkeitsstufe auf die jeweiligen Betroffenen beziehen und

— die Einhaltung der Vorschriften.

AVA Documents Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

5.3.1.4 Identitätsinformationsstelle

Zu den Belangen einer Identitätsinformationsstelle in einem Identitätsmanagementsystem gehören:

— die Richtigkeit der Identitätsinformationen,

— die Erfüllung der Anforderungen seitens der vertrauenden Parteien,

— die Einhaltung der Vorschriften und

— die Erfüllung der geschäftlichen Verpflichtungen gegenüber den Betroffenen.

5.3.1.5 Vertrauende Partei

Zu den Belangen einer vertrauenden Partei in einem Identitätsmanagementsystem gehören:

— Vertraulichkeit, Verfügbarkeit und Integrität sowie Anwendbarkeit bei einem Betroffenen von Identitätsinformationen,

— Bereitstellung genauer Identitätsinformationen zu den relevanten Betroffenen mit der erforderlichen Vertrauenswürdigkeitsstufe,

— effektive, dokumentierte und sichere Schnittstellen,

— die Konformität mit den für ihre Tätigkeit geltenden Vorschriften und

— ein wirksamer Mechanismus und Verfahren zur Auditierung.

5.3.1.6 Regulierungsstelle

Als externe, unabhängige Organisation sind folgende Belange einer Regulierungsstelle in einem Identitätsmanagementsystem von Bedeutung

— die ordnungsgemäße Dokumentation der Betriebsrichtlinien,

— der korrekte Betrieb, insbesondere bei der Anwendung der Betriebsrichtlinien,

— ordnungsgemäße Rechenschaftspflicht und Prüfung der Systemvorgänge,

— Einhaltung der Betriebspolitik und der betrieblichen Umsetzung mit den rechtlichen und regulatorischen Anforderungen,

— eine wirksame Berichterstattung über Systemvorgänge, einschließlich der Wirksamkeit der Kontrollen, der Vorfälle und der zur Behebung von Vorfällen getroffenen Maßnahmen, und

— wirksame Reaktion auf Vorfälle, die den Datenschutz verletzen oder zu verletzen drohen.

ANMERKUNG Als Akteure in einem Identitätsmanagementsystem (siehe 5.3.2.9) können Auditoren bei der Inspektion der Vorgänge in einem Identitätsmanagementsystem (siehe 5.4) die Interessen der Regulierungsstellen vertreten.

5.3.1.7 Vertreter oder Schützer der Verbraucher/Bürger

Verbraucher-/Bürgerschützer sind Einzelpersonen oder Gruppen, die aus der Zivilgesellschaft hervorgehen und versuchen, Verbraucher und Bürger vor Überwachung zu schützen und sich für bessere Datenschutzbestimmungen einzusetzen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

Verbraucher-/Bürgervertreter sind Personen, die von einem Betroffenen ernannt oder von Verbraucherorganisationen ausgewählt werden, um einen Verbraucher oder Bürger in seinen Rechten in Bezug auf den Datenschutz zu vertreten.

Die Hauptbelange der Vertreter und Schützer der Verbraucher/Bürger sind:

— Transparenz, Mitteilung, Einhaltung von Vorschriften und Schutz vor komplexer Rechtssprache, sowie

— Zugang zu Diensten für benachteiligte Bevölkerungsgruppen.

ANMERKUNG 1 Vertreter von Verbrauchern und Bürgern beteiligen sich an anerkannten gesellschaftlichen Prozessen, an denen mehrere Interessengruppen beteiligt sind, z. B. an der Führung, und legen bewährte Verfahren und Anforderungen fest, die von den Anbietern von Waren und Dienstleistungen für Verbraucher und Bürger zu erfüllen sind.

ANMERKUNG 2 Verbraucher- und Bürgervertreter werden ausgewählt, eingewiesen und gegebenenfalls geschult, um sicherzustellen, dass sie sich an vernünftigen und begründeten Diskussionen beteiligen, die sich nach Möglichkeit auf qualitativ hochwertige Nachweise stützen.

5.3.2 Akteure

5.3.2.1 Allgemeines

Ein Akteur interagiert mit einem Identitätsmanagementsystem, um an den Vorgängen des Identitätsmanagements teilzunehmen. Eine Entität darf mit demselben Identitätsmanagementsystem als eine Vielzahl unterschiedlicher Akteure interagieren. Das Design des Dokuments muss sämtliche Interaktionen aller vom System unterstützten Akteure definieren.

Das dokumentierte Design sollte die Interaktionen der Akteure im Hinblick auf die Funktionen beschreiben, auf die sich die Interaktionen beziehen. Wenn ein Akteur, der mit dem Identitätsmanagementsystem interagiert, authentifiziert werden muss, bevor die Interaktion fortgesetzt werden kann, muss das dokumentierte Design die Grundlage für die Authentifizierung (z. B. entitätsbasierte, rollenbasierte usw. Authentifizierung), das Authentifizierungsverfahren und die für jede Interaktion erforderliche Vertrauenswürdigkeitsstufe wie in ISO/IEC 29115 festgelegt angeben.

ANMERKUNG Ein Zweck der Spezifizierung von Akteuren beim Design eines Identitätsmanagementsystems besteht darin, alle beabsichtigten Interaktionen mit dem System beschreiben zu können.

Ein dokumentiertes Design darf die folgenden Akteure erkennen:

— Betroffener;

— Identitätsmanagementstelle;

— Identitätsregistrierungsstelle;

— vertrauende Partei;

— Identitätsinformationsanbieter;

— Identitätsinformationsstelle;

— Verifizierer;

— Auditor.

Das dokumentierte Design muss die Vertrauenswürdigkeitsstufe festlegen, die erforderlich ist, um Entitäten zu identifizieren und zu authentifizieren, die Zugang zu Identitätsinformationen beantragen, die in ihrem Identitätsmanagementsystem enthalten sind, wie in ISO/IEC 29115 beschrieben. Die Vertrauenswürdigkeitsstufe

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

darf für verschiedene Arten von Informationen und die Art des gewährten Zugriffs, d. h. Lesen, Schreiben usw., unterschiedlich sein. Die Autorisierung darf wie in ISO/IEC 29146 beschrieben implementiert werden.

5.3.2.2 Betroffener

Ein Betroffener ist ein Akteur, der Identifizierungsinformationen bereitstellt, um seine Identität im Rahmen von Identifizierungsmanagementprozessen festzustellen und zu validieren. Der Betroffene hat folgende Verantwortlichkeiten

— als Entität bei der Beantragung der Anmeldung in einer Anwendbarkeitsdomäne genaue Identitätsinformationen für die Registrierung als neuer Betroffener anzugeben,

— als Systembenutzer nach der Registrierung zu beantragen, vom Identitätsmanagementsystem erkannt zu werden und für den Zugang zu Diensten oder die Nutzung von Ressourcen, die in der mit dem Identitätsmanagementsystem verbundenen Anwendbarkeitsdomäne verfügbar sind, zugelassen zu werden, und

— als Gegenstand der Beobachtung, um Informationen zur Identität für eine erleichterte Beobachtung zu erhalten.

ANMERKUNG Als Gegenstand der Beobachtung sind die erhaltenen Identitätsinformationen anonym, bis ihr Bezug zum Betroffenen hergestellt ist.

Ein Betroffener kann ein Identitätsmanagementsystem nutzen, um

— zu beantragen, von Informationen im Identitätsmanagementsystem erkannt zu werden und für den Zugang zu Diensten oder die Nutzung von Ressourcen, die in der mit dem Identitätsmanagementsystem verbundenen Anwendbarkeitsdomäne verfügbar sind, zugelassen zu werden, und

— als Mensch über die ihn betreffenden Identitätsinformationen im Identitätsmanagementsystem informiert zu werden und zu verlangen, dass etwaige Fehler in den Identitätsinformationen korrigiert werden.

ANMERKUNG Unter entsprechend definierten Umständen darf ein gesetzlich bevollmächtigter Vertreter im Namen eines Betroffenen handeln.

5.3.2.3 Identitätsmanagementstelle

Eine Identitätsmanagementstelle ist mit einer Anwendbarkeitsdomäne verbunden und ist verpflichtet und in der Lage, Geschäftsziele für das Identitätsmanagement in dieser Domäne zu definieren und anzupassen sowie Managementrichtlinien zur Erfüllung dieser Ziele festzulegen.

Eine Identitätsmanagementstelle verwendet Richtlinien, um die Verwendung der registrierten Identitätsinformationen zu regeln. In den Richtlinien dürfen die zu erbringenden Dienste festgelegt werden, einschließlich der Vertrauenswürdigkeitsstufe der Identitätsinformationen, die vom Identitätsmanagementsystem bereitgestellt werden dürfen. In den Richtlinien darf auch festgelegt werden, wie in unvorhergesehenen Fällen die Genehmigung für den Zugriff auf und die Änderung von Identitätsinformationen eingeholt werden kann.

Die Identitätsmanagementstelle muss die Ziele des Identitätsmanagements für eine Anwendbarkeitsdomäne festlegen, die von dem unter ihrer Befugnis betriebenen Identitätsmanagementsystem bedient wird. Die Identitätsmanagementstelle muss Richtlinien festlegen, um die Ziele des Identitätsmanagements für eine zugehörige Domäne zu erreichen.

Zu den Verantwortlichkeiten einer Identitätsmanagementstelle gehören:

— Erstellung, Änderung, oder Aufhebung von Betriebsrichtlinien,

— Sicherstellung der Einhaltung von Gesetzen und Vorschriften in Bezug auf die Richtlinien und den Betrieb des Identitätsmanagementsystems,

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03

— Forderung und Genehmigung der Änderung von Mechanismen zur Schaffung einer notwendigen Vertrauenswürdigkeitsstufe bei der Authentifizierung von Entitäten für den Zugriff auf Identitätsinformationen und Systemkontrollfunktionen,

— Reaktion auf Zwischenfälle,

— Genehmigung von Änderungen an der Art der im Identitätsregister gespeicherten Informationen,

— Initiierung regelmäßiger Audits und

— Evaluierung der Auditberichte, insbesondere über die Wirksamkeit der Richtlinien.

Eine Identitätsmanagementstelle darf sich mit einer oder mehreren anderen Identitätsmanagementstellen förmlich zusammenschließen, um eine „*Föderation*“ zu bilden.

ANMERKUNG Der Zweck besteht darin, die Anwendbarkeitsdomäne für Betroffene um die anderen Anwendbarkeitsdomänen in einer Föderation zu erweitern. Diese Erweiterung wird durch eine streng kontrollierte Weitergabe von Identitätsinformationen erreicht.

In einer Föderation gehören zu den Verantwortlichkeiten der einzelnen Identitätsmanagementstellen:

— eine Vertrauenswürdigkeitsstufe für Identitätsinformationen zu bieten, die den festgelegten Anforderungen jedes anderen Mitglieds der Föderation entspricht,

— die Kontrolle über den Zugriff auf die in seinem Identitätsmanagementsystem enthaltenen Identitätsinformationen zu behalten,

— sich zu vergewissern, dass die Vertrauenswürdigkeitsstufe, die ein anderes Mitglied der Föderation bei der Autorisierung des Zugriffs auf Identitätsinformationen in den Identitätsmanagementsystemen der Föderation erreicht hat, seinen Anforderungen für den Zugriff auf seine eigenen Identitätsinformationen entspricht,

— mit gemeinsamen Richtlinien für den Informationsaustausch zu arbeiten, und

— Richtlinien festzulegen, um das Vertrauen in die Vertrauenswürdigkeitsstufe der Identitätsauthentifizierung zu erhalten.

ANMERKUNG 1 Üblicherweise werden in einer Föderation einige der Richtlinien für das Identitätsmanagement, insbesondere für die Zugangsberechtigung, Teil einer Vereinbarung zwischen den an den Domänen beteiligten Identitätsmanagementstellen sein.

ANMERKUNG 2 Identitätsmanagementrichtlinien für den Einsatz in mehreren Anwendbarkeitsdomänen können durch internationale Normen festgelegt werden.

ANMERKUNG 3 Änderungen der Struktur, der Organisation und des Umfangs einer Datenföderation unterliegen unter Umständen externen Zwängen wie z. B. rechtlichen oder regulatorischen Anforderungen oder der Erteilung von Genehmigungen durch Regulierungsstellen.

ANMERKUNG 4 Die Mitglieder einer Föderation dürfen vereinbaren, die operativen Verantwortlichkeiten der Identitätsmanagementstelle an einen gemeinsamen Betreiber zu delegieren, der als „Föderationsstelle“ bezeichnet wird.

5.3.2.4 Identitätsregistrierungsstelle

Eine Identitätsregistrierungsstelle ist ein Akteur in einem System für das Identitätsmanagement, der verpflichtet und in der Lage ist, betriebliche Richtlinien für die Erhebung, Aufzeichnung und Aktualisierung von Identitätsinformationen im Identitätsregister festzulegen und durchzusetzen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 24760-2:2023-03