



Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 24760-3:2022

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 3: Umsetzung (ISO/IEC 24760-3:2016)

Information technology - Security
techniques - A framework for identity
management - Part 3: Practice (ISO/IEC
24760-3:2016)

Technologies de l'information -
Techniques de sécurité - Cadre pour la
gestion de l'identité - Partie 3: Mise en
oeuvre (ISO/IEC 24760-3:2016)

09/2022



Nationales Vorwort

Diese Europäische Norm EN ISO/IEC 24760-3:2022 wurde als luxemburgische Norm ILNAS-EN ISO/IEC 24760-3:2022 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

DIESES WERK IST URHEBERRECHTLICH GESCHÜTZT

Kein Teil dieser Veröffentlichung darf ohne schriftliche Einwilligung weder vervielfältigt noch in sonstiger Weise genutzt werden - sei es elektronisch, mechanisch, durch Fotokopien oder auf andere Art!

ILNAS-EN ISO/IEC 24760-3:2022

EUROPÄISCHE NORM **EN ISO/IEC 24760-3**

EUROPEAN STANDARD

NORME EUROPÉENNE

September 2022

ICS 35.030

Deutsche Fassung

**Informationstechnik - Sicherheitsverfahren - Rahmenwerk
für Identitätsmanagement - Teil 3: Umsetzung (ISO/IEC
24760-3:2016)**

Information technology - Security techniques - A
framework for identity management - Part 3: Practice
(ISO/IEC 24760-3:2016)

Technologies de l'information - Techniques de sécurité
- Cadre pour la gestion de l'identité - Partie 3: Mise en
oeuvre (ISO/IEC 24760-3:2016)

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 und CENELEC-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 und elektrotechnischen Komitees 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 Centre:
Rue de la Science 23, B-1040 Brussels**

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 Minderung des identitätsbezogenen Risikos beim Management von Identitätsinformationen	8
5.1 Überblick	8
5.2 Risikobeurteilung	8
5.3 Vertrauenswürdigkeit der Identitätsinformationen	9
5.3.1 Allgemeines	9
5.3.2 Legitimation	9
5.3.3 Zugangsdaten	9
5.3.4 Identitätsprofil	9
6 Identitätsinformationen und Identifikatoren	10
6.1 Überblick	10
6.2 Richtlinie für den Zugang zu Identitätsinformationen	10
6.3 Identifikatoren	10
6.3.1 Allgemeines	10
6.3.2 Kategorisierung des Identifikators nach der Art der Entität, mit der der Identifikator verknüpft ist	11
6.3.3 Kategorisierung des Identifikators nach der Art der Verknüpfung	11
6.3.4 Kategorisierung des Identifikators durch die Gruppierung von Entitäten	12
6.3.5 Management von Identifikatoren	12
7 Überprüfen der Nutzung von Identitätsinformationen	13
8 Maßnahmenziele und Maßnahmen	13
8.1 Allgemeines	13
8.2 Kontextbezogene Komponenten für die Maßnahme	13
8.2.1 Einrichtung eines Identitätsmanagementsystems	13
8.2.2 Feststellung der Identitätsinformationen	15
8.2.3 Management von Identitätsinformationen	17
8.3 Architekturkomponenten für die Maßnahme	18
8.3.1 Einrichtung eines Identitätsmanagementsystems	18
8.3.2 Steuerung eines Identitätsmanagementsystems	19
Anhang A (normativ) Umsetzung des Managements von Identitätsinformationen in einer Föderation von Identitätsmanagementsystemen	21
A.1 Allgemeines	21
A.2 Modelle von vertrauenswürdigen Identitätsföderationen	22
A.3 Management und organisatorische Überlegungen	24
A.4 Auffindung	25
A.4.1 IIP Allgemein	25
A.4.2 IIP-Auffindung	26
A.4.3 Auffindung der IIA	26
A.5 Überlegungen zu föderationsübergreifenden Szenarien	27
A.6 Bedrohungen und Maßnahmen	28
A.6.1 Allgemeines	28
A.6.2 Anforderung der authentifizierten Identität	28
A.6.3 Autorisierung der Freigabe von Attributen	29
A.6.4 Erlangung von Hilfsattributen	30

A.7	Zusammenlegung von Identitätsinformationsstellen	30
Anhang B	(normativ) Umsetzung des Identitätsmanagements mit attributbasierten	
	Zugangsdaten zur Verbesserung des Datenschutzes	31
B.1	Allgemeines	31
B.2	Akteure	31
B.2.1	Überblick	31
B.2.2	Betroffene(r)	32
B.2.3	Vertrauende Partei	32
B.2.4	Identitätsinformationsanbieter	33
B.2.5	Identitätsinformationsstelle	33
B.3	Kontrollschritte	34
B.3.1	Allgemeines	34
B.3.2	Ausgabe von Zugangsdaten	34
B.3.3	Vorlage	34
B.3.4	Außerkraftsetzung	35
B.4	Architekturschichten und Komponenten	35
B.4.1	Allgemeines	35
B.4.2	Anwendungsbereitstellungsschicht	36
B.4.3	Kernkomponenten — Nachweiserzeugungs-/verifizierungsschicht	36
	Literaturhinweise	39

Bilder

Bild A.1	— Paarweises Föderationsmodell	22
Bild A.2	— Komplexes Föderationsmodell	23
Bild A.3	— Gateway-Föderationsmodell	23
Bild A.4	— Beispiel für einen grundlegenden Auffindungsdialo der Föderation	27
Bild B.1	— Akteure einer attributbasierten Zugangsdatenarchitektur und ihre Interaktionen	32
Bild B.2	— Hauptbestandteile des Tokens des Betroffenen und der Ausrüstung der vertrauenden Partei	35
Bild B.3	— Architektur des Tokens des/der Betroffenen	37

Europäisches Vorwort

Der Text von ISO/IEC 24760-3:2016 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 24760-3:2022 durch das Technische Komitee CEN/CLC/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 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 24760-3:2016 wurde von CEN als EN ISO/IEC 24760-3:2022 ohne irgendeine Abänderung genehmigt.

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-Directives, 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-Directives, 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 Patentерklärungen (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: <https://www.iso.org/foreword-supplementary-information.html>.

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

ISO/IEC 24760 besteht unter dem allgemeinen Titel *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement* aus den folgenden Teilen:

- *Part 1: Terminology and concepts*
- *Part 2: Reference architecture and requirements*
- *Part 3: Practice*

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 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.

Dieser Teil von 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 legt Umsetzungen für das Identitätsmanagement vor. Diese Umsetzungen umfassen die Vertrauenswürdigkeit bei der Steuerung der Nutzung von Identitätsinformationen, die Kontrolle des Zugangs zu Identitätsinformationen und anderen Ressourcen, die auf Identitätsinformationen basieren, sowie die Maßnahmenziele, die bei der Einrichtung und Pflege eines Identitätsmanagementsystems implementiert werden sollten.

ISO/IEC 24760 besteht aus den folgenden Teilen:

- ISO/IEC 24760-1: *Terminology and concepts*;
- ISO/IEC 24760-2: *Reference architecture and requirements*;
- ISO/IEC 24760-3: *Practice*.

ISO/IEC 24760 soll als Grundlage für andere Internationale Normen im Bereich des Identitätsmanagements dienen, darunter die folgenden:

- ISO/IEC 29100, *Privacy framework*;
- ISO/IEC 29101, *Privacy reference architecture*;
- ISO/IEC 29115, *Entity authentication assurance framework*;
- ISO/IEC 29146, *A framework for access management*.