

E DIN EN ISO/IEC 24760-3:2026-12 (D/E)

Erscheinungsdatum: 2026-11-06

Informationssicherheit, Cybersicherheit und Datenschutz - Ein Rahmenwerk für das Identitätsmanagement - Teil 3: Praxis (ISO/IEC 24760-3:2025); Deutsche und Englische Fassung EN ISO/IEC 24760-3:2026

Information security, cybersecurity and privacy protection - A framework for identity management - Part 3: Practice (ISO/IEC 24760-3:2025); German and English version EN ISO/IEC 24760-3:2026

Inhalt	Seite
Europäisches Vorwort.....	6
Vorwort.....	7
Einleitung.....	8
1 Anwendungsbereich.....	9
2 Normative Verweisungen.....	9
3 Begriffe.....	9
4 Abkürzungen.....	10
5 Minderung des identitätsbezogenen Risikos beim Management von Identitätsinformationen.....	10
5.1 Allgemeines.....	10
5.2 Risikobeurteilung.....	11
5.3 Vertrauenswürdigkeit der Identitätsinformationen.....	11
5.3.1 Allgemeines.....	11
5.3.2 Legitimation.....	11
5.3.3 Zugangsdaten.....	12
5.3.4 Identitätsprofil.....	12
6 Identitätsinformationen und Identifikatoren.....	13
6.1 Überblick.....	13
6.2 Richtlinie für den Zugang zu Identitätsinformationen.....	13
6.3 Identifikatoren.....	13
6.3.1 Allgemeines.....	13
6.3.2 Kategorisierung des Identifikators nach der Art der Entität, mit der der Identifikator verknüpft ist.....	14
6.3.3 Kategorisierung des Identifikators nach der Art der Verknüpfung.....	14
6.3.4 Kategorisierung des Identifikators durch die Gruppierung von Entitäten.....	15
6.3.5 Management von Identifikatoren.....	15
6.3.6 Kategorisierung des Identifikators nach Art der Wertschöpfung.....	16
7 Überprüfen der Nutzung von Identitätsinformationen.....	17
8 Maßnahmenziele und Maßnahmen.....	17
8.1 Allgemeines.....	17
8.2 Kontextbezogene Komponenten für die Maßnahme.....	17
8.2.1 Einrichtung eines Identitätsmanagementsystems.....	17
8.2.2 Feststellung der Identitätsinformationen.....	20
8.2.3 Management von Identitätsinformationen.....	21
8.3 Architekturkomponenten für die Maßnahme.....	23
8.3.1 Einrichtung eines Identitätsmanagementsystems.....	23
8.3.2 Steuerung eines Identitätsmanagementsystems.....	24

Anhang A (informativ) Umsetzung des Managements von Identitätsinformationen in einer Föderation von Identitätsmanagementsystemen.....	26
A.1 Allgemeines.....	26
A.2 Modelle von vertrauenswürdigen Identitätsföderationen.....	27
A.3 Management und organisatorische Überlegungen	29
A.4 Auffindung.....	30
A.4.1 IIP Allgemein	30
A.4.2 IIP-Auffindung.....	31
A.4.3 Auffindung der IIA.....	31
A.5 Überlegungen zu föderationsübergreifenden Szenarien.....	32
A.6 Bedrohungen und Maßnahmen.....	33
A.6.1 Allgemeines.....	33
A.6.2 Anforderung der authentifizierten Identität	33
A.6.3 Autorisierung der Freigabe von Attributen.....	34
A.6.4 Erlangung von Hilfsattributen	35
A.7 Zusammenlegung von Identitätsinformationsstellen.....	35
Anhang B (informativ) Umsetzung des Identitätsmanagements mit attributbasierten Zugangsdaten zur Verbesserung des Datenschutzes.....	37
B.1 Allgemeines.....	37
B.2 Akteure	37
B.2.1 Überblick.....	37
B.2.2 Betroffene(r).....	38
B.2.3 Vertrauende Partei	39
B.2.4 Identitätsinformationsanbieter	39
B.2.5 Identitätsinformationsstelle	39
B.3 Kontrollschritte	40
B.3.1 Allgemeines.....	40
B.3.2 Ausgabe von Zugangsdaten.....	40
B.3.3 Vorlage.....	40
B.3.4 Außerkraftsetzung.....	41
B.4 Architekturschichten und Komponenten.....	42
B.4.1 Allgemeines.....	42
B.4.2 Anwendungsbereitstellungsschicht.....	42
B.4.3 Kernkomponenten — Nachweiserzeugungs-/verifizierungsschicht.....	42
Literaturhinweise	45

Bilder

Bild 1 — Betrieblicher Anwendungsbereich eines Identitätsmanagementsystems.....	11
Bild A.1 — Paarweises Föderationsmodell	27
Bild A.2 — Komplexes Föderationsmodell	28
Bild A.3 — Gateway-Föderationsmodell.....	28
Bild A.4 — Beispiel für einen grundlegenden Auffindungsdialo g der Föderation	32
Bild B.1 — Akteure einer attributbasierten Zugangsdatenarchitektur und ihre Interaktionen.....	38
Bild B.2 — Hauptbestandteile des Tokens des Betroffenen und der Ausrüstung der vertrauenden Partei	41
Bild B.3 — Architektur des Tokens des/der Betroffenen.....	43