

E DIN EN ISO/IEC 24760-3:2022-06 (D/E)

Erscheinungsdatum: 2022-04-29

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement -
Teil 3: Umsetzung (ISO/IEC 24760-3:2016); Deutsche und Englische Fassung prEN
ISO/IEC 24760-3:2022

Information technology - Security techniques - A framework for identity management
- Part 3: Practice (ISO/IEC 24760-3:2016); German and English version prEN ISO/IEC
24760-3:2022

Inhalt	Seite
Europäisches Vorwort.....	7
Vorwort.....	8
Einleitung.....	9
1 Anwendungsbereich.....	10
2 Normative Verweisungen.....	10
3 Begriffe.....	10
4 Symbole und Abkürzungen.....	11
5 Minderung des identitätsbezogenen Risikos beim Management von Identitätsinformationen.....	11
5.1 Überblick.....	11
5.2 Risikobeurteilung.....	11
5.3 Vertrauenswürdigkeit der Identitätsinformationen.....	12
5.3.1 Allgemeines.....	12
5.3.2 Legitimation.....	12
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 von Identitätsinformationen.....	13
6.3 Identifikatoren.....	14
6.3.1 Allgemeines.....	14
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.....	15
6.3.4 Kategorisierung des Identifikators durch die Gruppierung von Entitäten.....	15
6.3.5 Management von Identifikatoren.....	16
7 Überprüfen der Nutzung von Identitätsinformationen.....	16
8 Maßnahmenziele und Maßnahmen.....	16
8.1 Allgemeines.....	16
8.2 Kontextbezogene Komponenten für die Maßnahme.....	16
8.2.1 Einrichtung eines Identitätsmanagementsystems.....	16
8.2.2 Feststellung der Identitätsinformationen.....	19
8.2.3 Management von Identitätsinformationen.....	20
8.3 Architekturkomponenten für die Maßnahme.....	22
8.3.1 Einrichtung eines Identitätsmanagementsystems.....	22
8.3.2 Steuerung eines Identitätsmanagementsystems.....	23

Anhang A (normativ) Umsetzung des Managements von Identitätsinformationen in einer Föderation von Identitätsmanagementsystemen.....	25
A.1 Allgemeines.....	25
A.2 Modelle von vertrauenswürdigen Identitätsföderationen.....	26
A.3 Management und organisatorische Überlegungen	28
A.4 Feststellung.....	29
A.4.1 IIP Allgemein	29
A.4.2 Feststellung des IIP.....	30
A.4.3 Feststellung der IIA.....	30
A.5 Überlegungen zu föderationsübergreifenden Szenarien.....	31
A.6 Bedrohungen und Maßnahmen.....	32
A.6.1 Allgemeines.....	32
A.6.2 Anforderung der authentifizierten Identität	32
A.6.3 Autorisierung der Freigabe von Attributen.....	33
A.6.4 Erlangung von Hilfsattributen	34
A.7 Zusammenlegung von Identitätsinformationsstellen.....	34
Anhang B (normativ) Umsetzung des Identitätsmanagements mit attributbasierten Zugangsdaten zur Verbesserung des Datenschutzes.....	36
B.1 Allgemeines.....	36
B.2 Akteure	36
B.2.1 Überblick.....	36
B.2.2 Betroffene(r).....	37
B.2.3 Vertrauende Partei.....	38
B.2.4 Identitätsinformationsanbieter	38
B.2.5 Identitätsinformationsstelle	38
B.3 Kontrollschritte	39
B.3.1 Allgemeines.....	39
B.3.2 Ausgabe von Zugangsdaten.....	39
B.3.3 Darstellung.....	39
B.3.4 Außerkraftsetzung.....	40
B.4 Architekturschichten und Komponenten.....	40
B.4.1 Allgemeines.....	40
B.4.2 Anwendungsbereitstellungsschicht.....	41
B.4.3 Kernkomponenten — geprüfte Erzeugungs-/Verifizierungsschicht	41
Literaturhinweise	44
Bilder	
Bild A.1 — Paarweises Föderationsmodell	26
Bild A.2 — Komplexes Föderationsmodell	27
Bild A.3 — Gateway-Föderationsmodell.....	27
Bild A.4 — Beispiel für einen grundlegenden Feststellungsdialog der Föderation	31
Bild B.1 — Akteure einer attributbasierten Zugangsdatenarchitektur und ihre Interaktionen.....	37
Bild B.2 — Hauptbestandteile des Tokens des Betroffenen und der Ausrüstung der vertrauenden Partei	40
Bild B.3 — Architektur des Tokens des Betroffenen.....	42