

**DIN EN ISO/IEC 24760-3**

ICS 35.030

Einsprüche bis 2022-06-29

**Entwurf**

**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

Technologies de l'information –  
Techniques de sécurité –  
Cadre pour la gestion de l'identité –  
Partie 3: Mise en oeuvre (ISO/IEC 24760-3:2016);  
Version allemande et anglaise prEN ISO/IEC 24760-3:2022

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-04-29 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter [www.din.de/go/entwuerfe](http://www.din.de/go/entwuerfe) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [nia@din.de](mailto:nia@din.de) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 79 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

## Nationales 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 prEN ISO/IEC 24760-3:2016 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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 24760-2:2015 | siehe | DIN EN ISO/IEC 24760-2* |
| ISO/IEC 27018        | siehe | DIN EN ISO/IEC 27018    |
| ISO/IEC 29100        | siehe | DIN EN ISO/IEC 29100    |
| ISO/IEC 29101        | siehe | DIN EN ISO/IEC 29101    |
| ISO/IEC 29134        | siehe | DIN EN ISO/IEC 29134    |
| ISO/IEC 29151        | siehe | DIN EN ISO/IEC 29151    |

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

---

\* Zur Zeit Entwurf.

## 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 24760-2\*, *Informationstechnik — Sicherheitsverfahren — Ein Rahmenwerk für das Identitätsmanagement — Teil 2: Referenzarchitektur und Anforderungen*

DIN EN ISO/IEC 27018, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung*

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

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

DIN EN ISO/IEC 29134, *Informationstechnik — Sicherheitsverfahren — Leitlinien für die Datenschutz-Folgenabschätzung*

DIN EN ISO/IEC 29151, *Informationstechnik — Sicherheitsverfahren — Leitfaden für den Schutz personenbezogener Daten*

– *Entwurf* –

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

– Leerseite –

**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)

## **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<br>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 von 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<br>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<br>Föderation von Identitätsmanagementsystemen . . . . . | 21    |
| A.1 Allgemeines . . . . .                                                                                                                   | 21    |
| A.2 Modelle von vertrauenswürdigen Identitätsföderationen . . . . .                                                                         | 22    |
| A.3 Management und organisatorische Überlegungen . . . . .                                                                                  | 24    |
| A.4 Feststellung . . . . .                                                                                                                  | 25    |
| A.4.1 IIP Allgemein . . . . .                                                                                                               | 25    |
| A.4.2 Feststellung des IIP . . . . .                                                                                                        | 26    |
| A.4.3 Feststellung 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        |
| <b>Anhang B (normativ) Umsetzung des Identitätsmanagements mit attributbasierten Zugangsdaten zur Verbesserung des Datenschutzes</b> |                                                              | <b>31</b> |
| 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                                                                                                                                | Darstellung                                                  | 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 — geprüfte Erzeugungs-/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 Feststellungsdialog 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 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 prEN ISO/IEC 24760-3:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

### **Anerkennungsnotiz**

Der Text von ISO/IEC 24760-3:2016 wurde von CEN als prEN 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-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](http://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](http://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 der 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 der 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.

Dieser Teil der 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*.

## 1 Anwendungsbereich

Dieser Teil von ISO/IEC 24760 stellt einen Leitfaden für das Management von Identitätsinformationen und für die Sicherstellung der Konformität eines Identitätsmanagementsystems mit ISO/IEC 24760-1 und ISO/IEC 24760-2 bereit.

Dieser Teil von ISO/IEC 24760 gilt für ein Identitätsmanagementsystem, in dem Identifikatoren oder pbD, die sich auf Entitäten beziehen, zum Zwecke der Identifizierung oder Authentifizierung von Entitäten und/oder zum Zwecke der Entscheidungsfindung unter Verwendung von Attributen von Entitäten erfasst, verarbeitet, gespeichert, übertragen oder verwendet werden. Umsetzungen für das Identitätsmanagement können auch in anderen Normen behandelt werden.

## 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 24760-1, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

## 3 Begriffe

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

### 3.1

#### **Identitätsmanagementsystem**

System, das Richtlinien, Verfahren, Technologie und andere Ressourcen für die Pflege von Identitätsinformationen einschließlich Metadaten umfasst

[QUELLE: ISO/IEC 24760-2:2015, 3.3]

### 3.2

#### **Identitätsprofil**

Identität, die durch ein Identitäts-Template festgelegte Attribute enthält

### 3.3

#### **Identitäts-Template**

Definition einer bestimmten Menge von Attributen

Anmerkung 1 zum Begriff: In der Regel dienen die Attribute in einem Profil dazu, einen bestimmten technischen oder geschäftlichen Zweck zu unterstützen, der von den vertrauenden Parteien benötigt wird.

### 3.4

#### **Identitätsdiebstahl**

Ergebnis einer erfolgreichen Identitätstäuschung

### 3.5

#### **Föderationsmanager**

Akteur in einer Föderation, der für das Management der sich aus dem Betrieb der Föderation ergebenden Aspekte zuständig ist

Anmerkung 1 zum Begriff: Ein bestehendes Föderationsmitglied oder ein unabhängiger Dritter kann die Rolle des Föderationsmanagers übernehmen.

### 3.6

#### **Betroffene(r)**

Entität, auf die sich die Identitätsinformationen in einem Identitätsmanagementsystem beziehen

[QUELLE: ISO/IEC 24760-2:2015, 3.4]

## **4 Symbole und Abkürzungen**

Für die Anwendung dieses Dokuments gelten die folgenden Symbole und Abkürzungen.

|     |                                                                    |
|-----|--------------------------------------------------------------------|
| IKT | Informations- und Kommunikationstechnologie                        |
| IIP | Identitätsinformationsanbieter (en: Identity Information Provider) |
| IIA | Identitätsinformationsstelle (en: Identity Information Authority)  |
| pbD | personenbezogene Daten                                             |
| RP  | vertrauende Partei (en: Relying Party)                             |

## **5 Minderung des identitätsbezogenen Risikos beim Management von Identitätsinformationen**

### **5.1 Überblick**

In Abschnitt 5 werden Umsetzungen zum Umgang mit identitätsbezogenen Risiken beim Betrieb eines Identitätsmanagementsystems nach ISO/IEC 24760-1, ISO/IEC 24760-2 und ISO/IEC 29115 dargelegt.

### **5.2 Risikobeurteilung**

Eine Funktion eines Identitätsmanagementsystems besteht darin, das Risiko von Identitätsfehlern sowie die Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten, verarbeiteten und übermittelten Identitätsinformationen zu verwalten. Es ist notwendig, sich über den Grad des Risikos klar zu werden, der von der jeweiligen Anwendung abhängt. Der Eigentümer der Anwendung sollte eine Risikobeurteilung durchführen, um den Grad des Risikos zu bestimmen. Das Ergebnis enthält Informationen, die zur Festlegung der erforderlichen Risikomanagementkriterien und -prozesse für das Identitätsmanagementsystem verwendet werden können. Zu den Informationen, die ein Identitätsmanagementsystem benötigt, gehören die erforderliche Vertrauenswürdigkeitsstufe in Bezug auf Identitätsinformationen sowie die Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit dieser Informationen.

ISO/IEC 24760-2 legt Instrumente zum Risikomanagement in Form von Richtlinien, Vorschriften, Gestaltung und Architektur fest. In einigen Fällen, bei denen es um Verbraucher geht, haben der Schutz personenbezogener Daten und die Kontrolle der Betroffenen über die Verwendung ihrer personenbezogenen Daten Priorität. ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29134 und ISO/IEC 29151 (wird noch veröffentlicht) enthalten Anforderungen und Leitlinien für den Datenschutz.

Identitätsinformationen, die von einem Identitätsmanagementsystem verwaltet werden, dürfen auch durch Verweisung auf Identitätsinformationsanbieter in einer anderen Domäne verwaltet werden. Beispielsweise darf die Legitimation von einem Diensteanbieter durchgeführt werden, der in einer anderen Domäne als dem Identitätsmanagementsystem tätig ist.

Wenn Identitätsinformationen erhoben und gespeichert werden, muss der Identitätsmanagementdienst Maßnahmen zum Risikomanagement ergreifen, um die Risiken abzuschwächen, die durch eine von der vertrauenden Partei in der Anwendungsdomäne durchgeführte Risikobeurteilung ermittelt wurden. Vertrauenswürdigkeitsstufen in Bezug auf Identitätsinformationen und Zugangsdienste müssen von der vertrauenden Partei entsprechend den beurteilten Risikograden bestimmt und festgelegt werden.

## 5.3 Vertrauenswürdigkeit der Identitätsinformationen

### 5.3.1 Allgemeines

Das Vertrauen in die von einem Identitätsmanagementsystem bereitgestellten Identitätsinformationen beruht auf Prozessen, die die Gültigkeit der Informationen von ihrer Erhebung bis zu ihrer anschließenden Speicherung und Pflege durch das System sicherstellen. Die Vertrauenswürdigkeit wird in der Regel in Form von Vertrauenswürdigkeitsstufen quantifiziert, wobei höhere Stufen einer größeren Vertrauenswürdigkeit entsprechen. Die Vertrauenswürdigkeitsstufe, die erreicht wird, hängt von der Qualität der Identitätsinformationen und der Präzision der Verfahren zur Identitätsvalidierung ab. Die Vertrauenswürdigkeitsstufen sind in ISO/IEC 29115 beschrieben.

### 5.3.2 Legitimation

Die Legitimation, d. h. die Validierung von Identitätsinformationen für die Registrierung einer Entität in einer Domäne, muss eine bestimmte Vertrauenswürdigkeitsstufe erfüllen. Die Vertrauenswürdigkeitsstufe für die Legitimation hängt von der Art und den Merkmalen der Informationen und in einigen Fällen vom Umfang dieser Informationen ab, z. B. von der Anzahl der unabhängigen Identitätsinformationsanbieter, die als Informationsquellen verwendet werden.

Eine höhere Vertrauenswürdigkeitsstufe bei der Identitätsverifizierung wird möglicherweise erreicht

- mit der Verifizierung zusätzlicher Zugangsdaten, die von verschiedenen Quellen ausgegeben wurden, und
- mit Hilfe einer vertrauenswürdigen externen Partei, die die Entität kennt, um die behaupteten Identitätsinformationen zu validieren.

ANMERKUNG 1 ISO/IEC 29003 enthält Anforderungen für die Legitimation.

ANMERKUNG 2 ISO/IEC 29115 legt fest, wie verschiedene Vertrauenswürdigkeitsstufen erreicht werden können.

### 5.3.3 Zugangsdaten

Ein Identitätsmanagementsystem darf mehrere Arten von Zugangsdaten ausgeben, die sich in der Vertrauenswürdigkeitsstufe der durch die Zugangsdaten dargestellten Identitätsinformationen unterscheiden.

Ein Identitätsmanagementsystem, das durch einen kryptographischen Mechanismus unterstützte Zugangsdaten mit einer hohen Vertrauenswürdigkeitsstufe ausgibt, sollte einen Dienst für vertrauende Parteien anbieten, um den kryptographischen Validierungsprozess aktiv zu unterstützen.

### 5.3.4 Identitätsprofil

Ein Identitätsmanagementsystem darf ein oder mehrere Identitätsprofile zum Erfassen, Strukturieren oder Darstellen von Identitätsinformationen verwenden.

ANMERKUNG Obwohl ein Profil Informationen zur Identität enthalten kann, dient es nicht der Identifizierung. Sein Zweck ist es, Systemprozessen, die diese Informationen für ihre Prozesse benötigen, Identitätsinformationen über eine Entität zur Verfügung zu stellen.

Eine Entität darf mehrere Identitätsprofile haben, von denen jedes einen anderen Satz von Attributen für die Entität enthält. So darf beispielsweise eine Sprachpräferenz in einem Profil für eine Zugangsschnittstelle vorhanden sein und nicht in einem Profil für Buchinteressen.

Ein Identitäts-Template darf als internationale oder branchenspezifische Norm festgelegt werden. Die Verwendung eines genormten Identitäts-Templates zur Aufzeichnung von Identitätsattributen würde die Verwendung von Identitätsprofilen über verschiedene Domänen hinweg erleichtern.

Ein Identitätsprofil darf in der Zugangsverwaltung verwendet werden, um die erforderlichen Identitätsattribute zu bestimmen, die für die Autorisierung einer Rolle oder eines Privilegs beim Zugang zu Informationen erforderlich sind. Ein Identitätsprofil darf als vorkonfigurierte Teilmenge von Identitätsinformationen verwendet werden, die bei der Interaktion mit einem Dienst angezeigt werden.

Ein Attribut in einem Identitätsprofil darf mit einer Vertrauenswürdigkeitsstufe verbunden sein. Mithilfe eines Identitätsprofils mit zugehörigen Vertrauenswürdigkeitsstufen zur Darstellung von Identitätsinformationen wird impliziert, dass jede Information mindestens mit der zugehörigen Vertrauenswürdigkeitsstufe validiert wurde. Ein Identitätsprofil, das die Anforderungen für den Zugang zu Diensten oder Ressourcen festlegt, darf mit einem spezifischen zusätzlichen Entitätsidentifikator verbunden sein, der die mit den spezifischen Privilegien verbundenen Aktivitäten angeben darf.

## 6 Identitätsinformationen und Identifikatoren

### 6.1 Überblick

Organisationen sollten die Belange der Informationssicherheit für ihr Unternehmen und die Einhaltung der einschlägigen Rechtsvorschriften verstehen und die Geschäftsleitung dabei unterstützen, die geschäftlichen Anforderungen zu erfüllen. Im Hinblick auf das Identitätsmanagement sollten sich Organisationen über ihre Haftung im Klaren sein und sicherstellen, dass angemessene Maßnahmen ergriffen werden, um die Risiken und Folgen von Informationslecks, Korruption und Verfügbarkeitsverlust bei der Erfassung, Speicherung, Verwendung, Übermittlung und Entsorgung von Identitätsdaten abzuschwächen. Organisationen sollten Maßnahmenziele und Maßnahmen festlegen, um sicherzustellen, dass die Anforderungen an die Informationssicherheit erfüllt werden.

### 6.2 Richtlinie für den Zugang von Identitätsinformationen

Die Identitätsinformationen zu einer Entität sollten so verwaltet werden, dass Folgendes sichergestellt ist:

- die Identitätsinformationen bleiben im Laufe der Zeit korrekt und aktuell;
- nur befugte Entitäten haben zu den Identitätsinformationen Zugang und sind für alle Verwendungen und Änderungen von Identitätsinformationen rechenschaftspflichtig, wodurch die Rückverfolgbarkeit jeder Verarbeitung von Identitätsinformationen durch eine beliebige Entität, sei es eine Person, ein Prozess oder ein System, sichergestellt wird;
- die Organisation erfüllt ihre Verpflichtungen in Bezug auf Vorschriften und vertragliche Vereinbarungen;
- die Betroffenen sind gegen das Risiko von Identitätsdiebstahl und anderen identitätsbezogenen Straftaten geschützt.

**ANMERKUNG** In der Regel wird in einer Informationssicherheitspolitik die Notwendigkeit eines sicheren Managements von Identitätsinformationen hervorgehoben. Die Aufbewahrung und der Schutz von Informationen zur Identität von Entitäten ist auch beim Umgang mit Dritten erforderlich und wird in der Regel in den Betriebsverfahren dokumentiert.

### 6.3 Identifikatoren

#### 6.3.1 Allgemeines

Ein Identifikator ermöglicht die eindeutige Unterscheidung einer Entität von einer anderen Entität in einer Anwendbarkeitsdomäne. Eine Entität darf mehrere unterschiedliche Identifikatoren in derselben Domäne haben. Dies erleichtert unter Umständen die Darstellung der Entität in bestimmten Situationen, z. B. beim Verbergen der Identität der Entität, wenn die Identitätsinformationen der Entität zur Verwendung in bestimmten Prozessen oder Systemen bereitgestellt werden. Ein in einer Domäne erstellter Identifikator darf absichtlich in einer anderen Domäne wiederverwendet werden, sofern der wiederverwendete Identifikator auch in der anderen Domäne die Eindeutigkeit der Identität sicherstellt.

### 6.3.2 Kategorisierung des Identifikators nach der Art der Entität, mit der der Identifikator verknüpft ist

#### 6.3.2.1 Personenkennzeichen

Ein Personenkennzeichen darf z. B. ein vollständiger Name, ein Geburtsdatum, ein Geburtsort oder verschiedene Pseudonyme sein, wie z. B. eine von einer Behörde als Referenz zugewiesene Nummer, z. B. eine Passnummer, eine nationale Identitätsnummer oder eine Personalausweisnummer.

Die Verwendung von Pseudonymen als Identifikatoren ist bei Personenkennzeichen üblich; siehe 6.3.3.2.

**ANMERKUNG** Ein Pseudonym kann die Privatsphäre von Personen in einem Identitätsauthentifizierungsaustausch mit einer vertrauenden Partei verbessern, da ein Pseudonym möglicherweise weniger personenbezogene Daten preisgibt, als wenn ein echter Name als Identifikator verwendet wird.

#### 6.3.2.2 Identifikator, der einer nicht personenbezogenen Entität zugewiesen wurde

Bei nicht personenbezogenen Einheiten, z. B. Geräten oder anderen Informationsobjekten, dürfen die Aktivitäten wie bei Personen identifiziert und aufgezeichnet werden.

Gerätekennungen ermöglichen die Unterscheidung zwischen Geräten in dem Bereich, in dem sie arbeiten.

**ANMERKUNG 1** Beispiel: Die International Mobile Equipment Identity (IMEI) ist ein Identifikator des Mobiltelefons im Bereich der GSM-Mobilfunkdienste.

**ANMERKUNG 2** Beispiel 2: Die GSM-SIM-Chipkartennummer (ICCID, en: Integrated Circuit Card Identifier) ist eine eindeutige Gerätekennung im Bereich eines Mobiltelefondienstes. Eine SIM-Karte enthält auch andere Kennungen, darunter die des Benutzers, der die SIM-Karte registriert hat.

Die Identifikatoren von Informationsobjekten müssen möglicherweise auch in ihren Domänen unterschieden werden. Eines ihrer Attribute oder eine Kombination ihrer Attribute wird in der Regel als Identifikator verwendet.

**ANMERKUNG 3** Beispiel: Prozessname, Sitzungsname, Pfadname, Uniform Resource Names (URN), Uniform Resource Identifier (URI) sind Beispiele für Identifikatoren von Informationsobjekten.

**ANMERKUNG 4** Beispiel: URI ist ein Beispiel eines Identifikators für einen Ort, aber das Objekt an diesem Ort kann sich jederzeit ändern.

### 6.3.3 Kategorisierung des Identifikators nach der Art der Verknüpfung

#### 6.3.3.1 Verinymischer Identifikator

Ein verinymischer Identifikator ist ein Identifikator, der in seiner Anwendbarkeitsdomäne beständig ist, innerhalb von Domänen und domänenübergreifend verwendet werden darf und es einer vertrauenden Partei ermöglicht, weitere Identitätsinformationen über die mit dem Identifikator verbundene Entität zu erhalten. Zu den häufig beobachteten eindeutigen Identifikatoren gehören die E-Mail-Adresse, die Mobiltelefonnummer, die Reisepassnummer, die Führerscheinnummer, die Sozialversicherungsnummer und das Paar aus Name und Geburtsdatum.

Ein eindeutiger Identifikator kann es unter Umständen ermöglichen, Identitätsinformationen für Entitäten, die in verschiedenen Domänen bekannt sind, zu korrelieren. Es ist zwar in Ordnung, die Identitäten zu korrelieren, wenn dies von der Person gewünscht wird, aber eine unerwartete Korrelation, z. B. ein Profiling, hat negative Auswirkungen auf die Privatsphäre. Aufgrund der Art des anonymisierten Identifikators können Angreifer im Falle eines Informationslecks eine solche Korrelation durchführen und Bedrohungen schaffen, z. B. indem sie datenschutzrelevante Informationen generieren, die der/die Betroffene nicht offenlegen wollte.

### 6.3.3.2 Pseudonymer Identifikator

Ein pseudonymer Identifikator ist ein Identifikator, der in seiner Domäne beständig ist und keine zusätzlichen Identitätsinformationen offenlegt. Solange keine anderen identifizierenden Informationen in der Domäne verfügbar sind, können Identitäten aus verschiedenen Domänen nicht mit einem pseudonymen Identifikator korreliert werden. Ein pseudonymer Identifikator darf verwendet werden, um eine unerwünschte Korrelation von Identitätsinformationen für Entitäten über Domänen hinweg zu verhindern.

**ANMERKUNG** Die bloße Verwendung pseudonymer Identifikatoren bedeutet nicht, dass die Identitätsdaten pseudonym sind. Andere Attribute, die zu einem bestimmten Zeitpunkt oder über mehrere Zeitpunkte hinweg kombiniert werden, reichen möglicherweise aus, um eindeutige Identifikatoren abzuleiten.

### 6.3.3.3 Kurzlebiger Identifikator

Ein kurzlebiger Identifikator ist ein Identifikator, der nur für einen kurzen Zeitraum und nur innerhalb einer einzigen Domäne verwendet wird. Er darf sich bei mehrfacher Nutzung desselben Dienstes oder derselben Ressource ändern.

**ANMERKUNG 1** Bei korrekter Verwendung macht es ein kurzlebiger Identifikator sehr schwierig, zwei Besuche einer Entität miteinander in Verbindung zu bringen.

**ANMERKUNG 2** Ein kurzlebiger Identifikator wird häufig im Rahmen einer attributbasierten Zugangskontrolle verwendet, bei der der Zugang zu einer Ressource gewährt wird, wenn die Entität ein bestimmtes Attribut besitzt. Wenn beispielsweise einer Person der Zugang zu einer Ressource gewährt wird, weil sie Mitglied einer bestimmten Gruppe ist, würde sich die Identität aus einem kurzlebigen Identifikator und einem Gruppenidentifikator zusammensetzen. Diese würden den Zweck der Zugangskontrolle erfüllen und gleichzeitig die offengelegten Daten oder die Möglichkeit der Verknüpfung von Mehrfachzugriffen minimieren, während die einzelnen Entitäten weiterhin unterschieden werden.

## 6.3.4 Kategorisierung des Identifikators durch die Gruppierung von Entitäten

### 6.3.4.1 Individueller Identifikator

Ein individueller Identifikator ist ein Identifikator, der mit nur einer Entität innerhalb einer Anwendbarkeitsdomäne verbunden ist.

### 6.3.4.2 Gruppenidentifikatoren

Entitäten werden manchmal zu einer Gruppenentität zusammengefasst, wenn die Notwendigkeit besteht, Aktivitäten in einer Gruppe auszuführen. Eine eindeutige Gruppenentität wird die Gruppenentität repräsentieren, und Gruppenidentifikatoren werden dazu beitragen, die Entität der Gruppe eindeutig zu identifizieren und die Aktivitäten der Gruppenentität in ihren Domänen aufzuzeichnen. Gruppenidentifikatoren dienen dem Bedürfnis einer Person, die Aktivitäten in einer Gruppe oder im Namen einer Gruppe durchführt; sie verbergen möglicherweise den Verursacher einer Aktivität in einer Gruppe. Daher können unter Umständen zusätzliche Techniken erforderlich sein, um eine einzelne Entität eindeutig als Mitglied einer Gruppenentität zu identifizieren.

## 6.3.5 Management von Identifikatoren

Bei der Aktualisierung von Identitätsinformationen für eine bekannte Entität darf ein Identitätsmanagementsystem der geänderten Identität einen neuen Identifikator zuweisen; es darf auch die Verbindung des alten Identifikators mit der Identität aufheben. Geänderte Identitätsinformationen dürfen proaktiv an Teilsysteme weitergegeben werden, die auf sie angewiesen sind.

## 7 Überprüfen der Nutzung von Identitätsinformationen

Das Management und die Verarbeitung von Identitätsinformationen durch autorisierte Stellen in einer Domäne kann unter Umständen verschiedenen rechtlichen, regulatorischen und branchenspezifischen Anforderungen unterliegen, die ein gewisses Maß an Überwachung und Rückverfolgbarkeit erfordern.

**ANMERKUNG** Diese Anforderungen können sehr vielfältig sein und reichen von Protokolldateien und anderen Maßnahmen zum Schutz personenbezogener Daten bis hin zur Einhaltung der erforderlichen Zeitstempelgenauigkeit und Rückverfolgbarkeit; siehe ISO/IEC 18014.

Eine Entität, die Dienste im Zusammenhang mit dem Identitätsmanagement anbietet, sollte Mechanismen bereitstellen, die die Überprüfbarkeit sicherstellen.

## 8 Maßnahmenziele und Maßnahmen

### 8.1 Allgemeines

Abschnitt 8 fasst die Sicherheitsziele und die zugehörigen Maßnahmen zusammen, die bei der Einrichtung oder Überprüfung eines Identitätsmanagementsystems zu verifizieren sind.

Die Struktur der Maßnahmen folgt der in ISO/IEC 27002 dargestellten Struktur.

### 8.2 Kontextbezogene Komponenten für die Maßnahme

#### 8.2.1 Einrichtung eines Identitätsmanagementsystems

##### 8.2.1.1 Zielsetzung

Einrichtung eines Managementsystems zur Initiierung und Kontrolle der Umsetzung des Managements von Identitätsinformationen für Entitäten.

##### 8.2.1.2 Festlegung und Dokumentierung der Anwendbarkeitsdomäne

#### Maßnahme

Die vertrauenden Parteien, für die eine Entität oder eine Gruppe von Entitäten ihre Identität anwenden kann und die die Identität zur Identifizierung und für andere Zwecke verwenden dürfen, müssen so dokumentiert werden, dass sie sowohl für die Betreiber als auch für die beteiligten Entitäten klar verständlich sind.

#### Leitlinien für die Implementierung

Eine Dokumentation, die die Grenzen der Domäne eines Systems für das Identitätsmanagement beschreibt, sollte allen interessierten Parteien zur Verfügung gestellt werden. In dieser Dokumentation sollten die Grenzen festgelegt werden, innerhalb derer die Identitätsinformationen verifiziert werden können. Mögliche Erweiterungen auf andere Domänen oder Gruppen von Entitäten sollten ebenfalls dokumentiert werden.

Die Dokumentation sollte die rechtlichen oder sonstigen Beschränkungen und die damit verbundenen Verpflichtungen in Bezug auf die Kontrolle von Identitätsinformationen in einer Domäne klarstellen.

#### Weitere Informationen

Eine Domäne einer Identität ist in Bezug auf eine bestimmte Gruppe von Attributen, die Gruppen von Entitäten festlegen, genau definiert.

Ein IT-System innerhalb einer Organisation, das einer Gruppe von Entitäten erlaubt, sich anzumelden, ist eine Sub-Domäne in dieser Organisation.

### **8.2.1.3 Identifizierung von Identitätsinformationsanbietern (IIP), Identitätsinformationsstellen (IIA), Identitätsmanagementstellen und Regulierungsstellen**

#### **Maßnahme**

Identitätsinformationsstellen für Identitätsinformationen, die von einem Identitätsmanagementsystem verwaltet werden, müssen für die Domäne eines Identitätsmanagementsystems festgelegt werden.

Die Entitäten, die die Verantwortung für den Schutz von Identitätsinformationen auf Seiten der Verwaltung und der Aufsichtsbehörden übernehmen, müssen ebenfalls identifiziert werden.

#### **Leitlinien für die Implementierung**

Die mit einem Identitätsmanagementsystem verbundenen Entitäten wie die Quelle der Identitätsinformationen (IIP), die maßgebliche Aussage über verfügbare Informationen (IIA), die Identitätsmanagementstelle und alle einschlägigen staatlichen oder sonstigen Regulierungsstellen sollten eindeutig identifiziert werden.

Die Aufgaben eines Identitätsinformationsanbieters bestehen darin, Identitätsinformationen für Entitäten, die in einer bestimmten Domäne bekannt sind, zu erstellen, zu pflegen und zugänglich zu machen. Es sollte auch angegeben werden, mit welchen Verfahren der Zugang zu den Informationen oder die Inanspruchnahme der von diesen operativen Entitäten angebotenen Dienste möglich ist.

Alle Änderungen in Bezug auf die Verfügbarkeit und die Verfahren für den Zugang und die Inanspruchnahme von Diensten sollten den interessierten Parteien aktiv mitgeteilt werden.

#### **Weitere Informationen**

Eine Entität darf die Funktionen des Identitätsinformationsanbieters und der Identitätsinformationsstelle kombinieren.

### **8.2.1.4 Identifizierung der vertrauenden Partei (RP)**

#### **Maßnahme**

Für die Domäne des Identitätsmanagementsystems müssen die vertrauenden Parteien bekannt gemacht werden.

#### **Leitlinien für die Implementierung**

Vertrauende Parteien haben vertrauensvolle Beziehungen zu einer oder mehreren Identitätsinformationsstellen. Die mit einer Identitätsinformationsstelle verbundenen vertrauenden Parteien dürfen in der Gestaltungsphase bekannt sein. RPs dürfen sich im Laufe der Zeit ändern, indem sie einer Beziehung zu einer oder mehreren Identitätsinformationsstellen in der Domäne beitreten oder sie verlassen.

#### **Weitere Informationen**

Eine vertrauende Partei ist einem Risiko ausgesetzt, das durch falsche oder ungültige Identitätsinformationen verursacht wird.

### **8.2.1.5 Pflege eines Identitätsmanagementsystems**

#### **Maßnahme**

Es muss ein Prozess beschrieben werden, der die Pflege der wichtigen operativen Entitäten in einem Identitätsmanagementsystem sicherstellt.

#### **Leitlinien für die Implementierung**

Im Laufe der Zeit dürfen die Domänen eines Identitätsmanagementsystems verschiedene Identitätsinformationsstellen, Identitätsinformationsanbieter und vertrauende Parteien verwenden, um ihre Interaktionen mit Entitäten zu unterstützen. Domänen dürfen auch geschaffen und beendet werden bzw. die Bedingungen für ihre Anwendbarkeit dürfen sich ändern.

Wichtige Entitäten für die Verwendung eines Identitätsmanagementsystems, z. B. IIA, IIP und RP, können unter Umständen ebenfalls nicht mehr existieren, nachdem sie ersetzt, archiviert oder gelöscht wurden. Ein Identitätsmanagementsystem sollte Richtlinien und Prozesse dokumentieren, die die Kontrolle dieser wichtigen Entitäten sicherstellen und dafür sorgen, dass wertvolle Informationen des Identitätsmanagementsystems nicht verloren gehen.

#### **8.2.1.6 Sicherstellung der Privatsphäre**

##### **Maßnahme**

Wenn menschliche Entitäten innerhalb eines Identitätsmanagementsystems, das ihre Identitätsinformationen verwaltet, interagieren, muss es über dokumentierte Richtlinien und bewährte Kontrollmaßnahmen verfügen, die den Datenschutz dieser Entitäten sicherstellen.

##### **Leitlinien für die Implementierung**

Ein grundlegendes Ziel bei der Einrichtung eines Identitätsmanagementsystems ist es, sicherzustellen, dass die Privatsphäre von Entitäten zu jeder Zeit gewahrt bleibt.

Ein Identitätsmanagementsystem muss alle sensiblen Informationen, die es über menschliche Entitäten verarbeitet, in Übereinstimmung mit ISO/IEC 24760-1 dokumentieren.

##### **Weitere Informationen**

Die Anforderungen für den Umgang mit sensiblen Identitätsinformationen sind enthalten in

- ISO/IEC 29100 und
- ISO/IEC 29101.

#### **8.2.2 Feststellung der Identitätsinformationen**

##### **8.2.2.1 Zielsetzung**

Festlegen, Dokumentieren und Kommunizieren von Identitätsinformationen.

##### **8.2.2.2 Identitätsdarstellung**

##### **Maßnahme**

Referenzen einer Entität in einem Identitätsmanagementsystem, die für die Dauer, in der die Entität in der/den Domäne(n) des Systems bekannt ist, gleich bleiben, dürfen als „Referenzkennung“ bezeichnet werden. Das Identitätsmanagementsystem muss Maßnahmen für die Identitätsmanagementsysteme dokumentieren, um die eindeutige Unterscheidbarkeit jeder Entität in jeder Domäne des Identitätsmanagementsystems sicherzustellen.

##### **Leitlinien für die Implementierung**

Eine Referenzkennung sollte mindestens für die Dauer der bestehenden Entität in einem Identitätsmanagementsystem bestehen bleiben und darf länger als die Entität bestehen, z. B. für Archivierungszwecke oder den Bedarf der Behörden.

Die Dokumentation des Identitätsmanagementsystems sollte die Verwendung und Wiederverwendung von Identifikatoren beschreiben. Eine Referenzkennung für eine Entität sollte nicht wiederverwendet werden, solange Identitätsinformationen zu dieser Entität, einschließlich archivierter Informationen, im System gespeichert sind.

Ein Referenzkennungsgenerator ist ein Werkzeug, das helfen kann, eindeutige Werte für Referenzkennungen zu liefern.

### **Weitere Informationen**

Um die Pflege der aufgezeichneten Informationen für eine bestimmte Identität zu erleichtern, darf das Identitätsmanagementsystem einen Referenzkennungsgenerator verwenden, um einer hinzugefügten Identität eine eindeutige Aufzeichnungsnummer zuzuweisen.

#### **8.2.2.3 Identitätsinformationen**

##### **Maßnahme**

Die Menge der Werte von Attributen, die erforderlich sind, um Identitätsinformationen zu einer Entität in Domänen eines Identitätsmanagementsystems zusammenzustellen, müssen festgelegt, von den Verifizierern validiert und den vertrauenden Parteien auf Anfrage mitgeteilt werden.

##### **Leitlinien für die Implementierung**

Die Verifizierung der Werte der erforderlichen Attribute einer Identität führt zu einer authentifizierten Identität für eine Entität.

Der Authentifizierungsprozess umfasst Prüfungen eines oder mehrerer von einer Entität bereitgestellten Identitätsattribute durch einen Verifizierer, um deren Korrektheit mit der erforderlichen Vertrauenswürdigkeitsstufe festzustellen.

#### **8.2.2.4 Unterscheidung zwischen verschiedenen Arten von Entitäten**

##### **Maßnahme**

Die Anzahl der unterschiedlichen Entitätsarten in den Domänen eines Identitätsmanagementsystems muss erkannt und mit unterschiedlichen Attributwerten beschrieben werden, die ihre Identität ausmachen.

##### **Leitlinien für die Implementierung**

Elemente innerhalb oder außerhalb eines IKT-Systems, wie z. B. eine Person, eine Organisation, ein Gerät, ein Teilsystem oder eine Gruppe solcher Elemente, die erkennbar in Domänen eines Identitätsmanagementsystems existieren, sind unterschiedliche Entitätsarten, die mit unterschiedlichen Attributwerten beschrieben werden dürfen.

Jede Entitätsart sollte in Bezug auf Semantik und Syntax dokumentiert werden, wobei die Liste der für ihre Identität erforderlichen Attributwerte zu validieren ist.

#### **8.2.2.5 Authentifizieren einer Identität**

##### **Maßnahme**

Ein Prozess muss dokumentiert werden, der die Identitätsinformationen für eine Entität verifiziert.

##### **Leitlinien für die Implementierung**

Ein Authentifizierungsprozess umfasst Operationen eines Verifizierers, mit denen festgestellt werden sollte, dass die Identitätsinformationen für eine Entität so korrekt sind, dass der für die Entität zu erbringende Dienst die erforderliche Vertrauenswürdigkeitsstufe aufweist.

Verifizierer dürfen mit der Identitätsinformationsstelle für eine bestimmte Domäne identisch sein oder in deren Namen handeln.

### **8.2.3 Management von Identitätsinformationen**

#### **8.2.3.1 Zielsetzung**

Sicherstellen, dass Identitätsinformationen in allen Domänen eines Identitätsmanagementsystems gepflegt und geschützt werden, von der ersten Registrierung bis zur Archivierung oder Löschung.

#### **8.2.3.2 Vertrauen in die Erhebung und Management von Identitätsinformationen**

##### **Maßnahme**

Alle Zuständigkeiten für die Informationssicherheit bei der Erhebung und Management von Identitätsdaten müssen festgelegt und zugewiesen werden.

##### **Leitlinien für die Implementierung**

Die Zuweisung von Zuständigkeiten im Bereich der Informationssicherheit für die Erhebung und das Management von Identitätsinformationen muss im Einklang mit den Informationssicherheitsstrategien erfolgen. Die Zuständigkeiten für den Schutz individueller Identitätsinformationen und für die Durchführung spezifischer Informationssicherheitsprozesse zur Erhebung und zum Management von Identitätsinformationen sollten festgelegt werden.

Die Zuständigkeiten für das Risikomanagement im Bereich der Informationssicherheit und insbesondere für die Akzeptanz von Restrisiken bei der Festlegung von Vertrauenswürdigkeitsstufen bei der Erhebung von Identitätsinformationen sollten festgelegt werden.

Die Aktivitäten des Identitätsmanagements sollten Folgendes umfassen:

- Anwendung(en), die ein Identitätsregister implementieren;
- Sicherstellung der Korrektheit der Identitätsinformationen mit einer festgelegten Vertrauenswürdigkeitsstufe;
- die Festlegung der Ursprungsdomäne bestimmter Attributwerte in Identitätsinformationen;
- Pflege der Identitätsinformationen während des gesamten Lebenszyklus der Identität;
- die Authentifizierung der Identität;
- Minderung des Risikos des Diebstahls oder Missbrauchs von Identitätsinformationen.

##### **Weitere Informationen**

Der Informationssicherheitsbeauftragte einer Organisation sollte, sofern vorhanden, die Gesamtverantwortung für die Entwicklung und Implementierung der Vertrauenswürdigkeitsstufen zur Unterstützung der Erhebung von Identitätsinformationen und für das Management von Identitätsinformationen übernehmen.

#### **8.2.3.3 Definition und Kontrolle des Identitätslebenszyklus**

##### **Maßnahme**

Ein formalisierter Prozess, der den Lebenszyklus von Identitäten in Domänen definiert und pflegt und den Status jeder Identität in jeder Domäne kontrolliert, muss dokumentiert werden.

### **Leitlinien für die Implementierung**

Der Lebenszyklus von Identitätsinformationen beginnt mit der Registrierung und endet, wenn alle Identitätsinformationen für eine Entität aus dem System gelöscht werden, einschließlich aller archivierten Informationen.

### **Weitere Informationen**

Die folgenden Phasen des Lebenszyklus von Identitäten werden nach ISO/IEC 24760-1 ermittelt:

- unbekannt;
- festgestellt;
- aktiv;
- ausgesetzt;
- archiviert;
- gelöscht.

## **8.3 Architekturkomponenten für die Maßnahme**

### **8.3.1 Einrichtung eines Identitätsmanagementsystems**

#### **8.3.1.1 Zielsetzung**

Sicherstellen, dass ein System für das Management von Identitätsinformationen eingeführt und gut dokumentiert wird.

#### **8.3.1.2 Dokumentierung eines Identitätsmanagementsystems**

### **Maßnahme**

Ein Identitätsmanagementsystem muss vor seiner Implementierung dokumentiert werden.

### **Leitlinien für die Implementierung**

Die dokumentierte Gestaltung der Architektur eines Identitätsmanagementsystems sollte das System in seinem Einsatzkontext auf der Grundlage der definierten Interessengruppen und Akteure sowie der festgelegten Anforderungen festlegen.

Die dokumentierte Gestaltung sollte die Anforderungen sowohl der Akteure als auch der Nicht-Akteure berücksichtigen.

### **Weitere Informationen**

Die dokumentierte Gestaltung muss Folgendes erschöpfend beschreiben:

- Anforderungen an die Akteure;
- Anforderungen der Interessengruppen;
- Sichtweisen;

- Modelle;
- Komponenten;
- Instandhaltungsprozesse; und
- Informationsflüsse und Aktionen.

Die Liste der Akteurstypen und ihre Interaktionen mit den Systemen sollte ebenfalls dokumentiert werden.

Die dokumentierte Gestaltung sollte das Szenario angeben, das für das Identitätsmanagementsystem verwendet wird, z. B. Unternehmen, fördert, Dienst oder heterogen. Die Gestaltung sollte die Komponenten und Abläufe des gewählten Szenarios entsprechend festlegen.

### 8.3.1.3 Identifizierung einer Identitätsregistrierungsstelle

#### Maßnahme

Für jedes Identitätsmanagementsystem muss eine Identitätsregistrierungsstelle bestimmt werden.

#### Leitlinien für die Implementierung

Eine Identitätsregistrierungsstelle hat die Pflicht und die Möglichkeit, operative Richtlinien für die Erhebung, Aufzeichnung und Aktualisierung von Identitätsinformationen festzulegen und durchzusetzen.

Zu den Aufgaben einer Identitätsregistrierungsstelle gehören die folgenden:

- Änderung, Erstellung oder Aufhebung von Betriebsrichtlinien;
- Genehmigung der Änderung von Mechanismen zur Schaffung einer erforderlichen Vertrauenswürdigkeitsstufe bei der Authentifizierung von Entitäten für den Zugriff auf Identitätsinformationen und Systemkontrollfunktionen;
- Genehmigung von Änderungen an der Art der im Verzeichnis gespeicherten Informationen;
- Genehmigung zur Änderung der im Verzeichnis gespeicherten Identitätsinformationen.

#### Weitere Informationen

Wenn dies nicht der Fall ist, sollte der Informationssicherheitsmanager die Rolle der Identitätsregistrierungsstelle übernehmen.

### 8.3.2 Steuerung eines Identitätsmanagementsystems

#### 8.3.2.1 Zielsetzung

Sicherstellen, dass ein Identitätsmanagementsystem Mechanismen zur Bewahrung und Pflege von Identitätsinformationen umfasst.

#### 8.3.2.2 Zugang zu einem Identitätsmanagementsystem

#### Maßnahme

Der Zugang zu einem Identitätsmanagementsystem ist auf die Personen beschränkt, die mit der Wartung des Systems betraut sind, auf die Anbieter von Identitätsinformationen und auf die vertrauenden Parteien sowie auf Einzelpersonen zur Abfrage von Informationen, die im Rahmen des Datenschutzes über ihre Person erhoben wurden.

### **Leitlinien für die Implementierung**

Ein Informationsmanagementsystem sollte die erforderlichen Schnittstellen entwickeln, um den Zugang zu den erforderlichen Stellen mit den entsprechenden Rechten zu ermöglichen, die von der Identitätsinformationsstelle oder der Identitätsregistrierungsstelle genehmigt werden.

#### **8.3.2.3 Erforderliche Komponenten eines Identitätsmanagementsystems**

##### **Maßnahme**

Ein Identitätsmanagementsystem muss mindestens Folgendes umfassen:

- ein Repository von Identitätsinformationen zu den in seinen Domänen erkannten Entitäten, möglicherweise unter Verwendung von Identitäts-Templates;
- ein Managementsystem, das im Rahmen einer einheitlichen Politik arbeitet und in der Lage ist, Identitätsinformationen aus verschiedenen validierten Quellen (Attribute der Ursprungsdomänen) zu erheben und die Informationen zu löschen, wenn die Bedingungen für die Speicherung von Identitätsinformationen nicht mehr gegeben sind;
- Managementschnittstellen für den Zugang zu Identitätsinformationen; und
- eine Speicherkomponente, die die Informationen über nicht mehr existierende Entitäten archiviert.

### **Leitlinien für die Implementierung**

Identitätsmanagementsysteme dürfen je nach dem für ihre Umsetzung entwickelten Modell unterschiedliche Komponenten aufweisen. Es ist auch sehr üblich, eine Identitätsmanagementfunktion auf einem System zu sehen, das für die Ausführung organisatorischer Funktionen bestimmt ist, wie z. B. das Personalmanagement oder das Beschaffungsmanagement, da diese Systeme die wichtigsten maßgeblichen Quellen für ein IMS darstellen. Ein Identitätsmanagementsystem sollte jedoch unabhängig von allen anderen IT-Systemen in einer Domäne bleiben, da es auf funktionale Anforderungen reagiert, die sich von diesen anderen Managementfunktionen weitgehend unterscheiden.

#### **8.3.2.4 Auditierung eines Identitätsmanagementsystems**

##### **Maßnahme**

Ein Identitätsmanagementsystem muss regelmäßig beurteilt oder geprüft werden (standardmäßig jährlich).

### **Leitlinien für die Implementierung**

Das Audit oder die Beurteilung sollte bestätigen, dass das Identitätsmanagementsystem in Übereinstimmung mit den dokumentierten Richtlinien und Verfahren arbeitet und mit den gesetzlichen und anderen extern auferlegten Anforderungen, z. B. dem Datenschutz, übereinstimmt.

Beurteilungen oder Audits sollten

- Aussagen enthalten, in denen die vom Identitätsmanagementsystem durchgeführten Vorgänge beschrieben werden, insbesondere im Hinblick auf die Einhaltung betrieblicher Richtlinien, und
- validieren, dass das Identitätsmanagementsystem über bestimmte Vorgänge, z. B. Schwachstellen, meldet, beurteilen, ob die Vorgänge den geltenden Richtlinien, z. B. zur Kontrolle des Datenschutzes, entsprechen, und auf etwaige Unstimmigkeiten hinweisen.