

DIN EN ISO/IEC 24760-3

ICS 35.030

**Informationstechnik –
Sicherheitsverfahren –
Rahmenwerk für Identitätsmanagement –
Teil 3: Umsetzung (ISO/IEC 24760-3:2016);
Deutsche Fassung EN ISO/IEC 24760-3:2022**

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

Gesamtumfang 43 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 EN ISO/IEC 24760-3:2022 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 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 24760-2:2015	siehe	DIN EN ISO/IEC 24760-2:2023-03
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002*
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) durch eine Suche nach der Dokumentennummer aufgerufen werden.

* in Überarbeitung; Stand zum Zeitpunkt dieser Veröffentlichung: E DIN EN ISO/IEC 27002:2022-08, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche und Englische Fassung prEN ISO/IEC 27002:2022.*

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 24760-1, *IT-Sicherheit und Datenschutz — Rahmenwerk für Identitätsmanagement — Teil 1: Terminologie und Konzept*

DIN EN ISO/IEC 24760-2:2023-03, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 2: Referenzarchitektur und Anforderungen (ISO/IEC 24760-2:2015); Deutsche Fassung EN ISO/IEC 24760-2:2022*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

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*

– Leerseite –

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 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

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 Auffindungsdialog 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 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: <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*.

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 Identitätsinformationen zu verwalten, die es speichert, verarbeitet und übermittelt. 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 an 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 das 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 Einschreibung einer Entität in einer Domäne, muss eine bestimmte Vertrauenswürdigkeitsstufe erfüllen. Die erreichbare 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 an 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 Identitätsinformationen 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 kann beispielsweise eine Sprachpräferenz in einem Profil für eine Zugangsschnittstelle vorhanden sein und nicht in einem Profil für das Interesse an Büchern.

Ein Identitäts-Template kann als internationaler oder branchenspezifischer Standard festgelegt werden. Die Verwendung eines standardisierten Identitäts-Templates zur Aufzeichnung von Identitätsattributen würde die Verwendung von Identitätsprofilen über verschiedene Domänen hinweg erleichtern.