

DIN EN ISO/IEC 29146:2023-12 (D)

Informationstechnologie - Sicherheitstechniken - Ein Rahmenwerk für die
Zugangsverwaltung (ISO/IEC 29146:2016 einschließlich Änderung 1:2022); Deutsche
Fassung EN ISO/IEC 29146:2023

| Inhalt | Seite |
|----------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort..... | 7 |
| Vorwort..... | 8 |
| Einleitung..... | 9 |
| 1 Anwendungsbereich..... | 10 |
| 2 Normative Verweisungen..... | 10 |
| 3 Begriffe..... | 10 |
| 4 Abkürzungen..... | 14 |
| 5 Konzepte..... | 15 |
| 5.1 Ein Modell für die Steuerung des Zugriffs auf Ressourcen..... | 15 |
| 5.1.1 Überblick..... | 15 |
| 5.1.2 Beziehung zwischen Identitätsverwaltungssystem und Zugangsverwaltungssystem..... | 16 |
| 5.1.3 Sicherheitsmerkmale des Zugangsverfahrens..... | 17 |
| 5.2 Beziehungen zwischen logischer und physischer Zugangssteuerung..... | 18 |
| 5.3 Funktionen und Prozesse des Zugangsverwaltungssystems..... | 18 |
| 5.3.1 Überblick..... | 18 |
| 5.3.2 Zugangssteuerungsrichtlinie..... | 18 |
| 5.3.3 Rechteverwaltung..... | 20 |
| 5.3.4 Verwaltung richtlinienbezogener Attributinformatoren..... | 21 |
| 5.3.5 Autorisierung..... | 22 |
| 5.3.6 Überwachungsmanagement..... | 23 |
| 5.3.7 Alarmverwaltung..... | 24 |
| 5.3.8 Föderierte Zugangssteuerung..... | 24 |
| 6 Referenzarchitektur..... | 25 |
| 6.1 Überblick..... | 25 |
| 6.2 Grundlegende Komponenten eines Zugangsverwaltungssystems..... | 26 |
| 6.2.1 Authentisierungsendpunkt..... | 26 |
| 6.2.2 Richtlinienentscheidungspunkt (PDP)..... | 26 |
| 6.2.3 Richtlinieninformationspunkt (PIP)..... | 26 |
| 6.2.4 Richtlinienverwaltungspunkt (PAP)..... | 27 |
| 6.2.5 Richtliniendurchsetzungspunkt (PEP)..... | 27 |
| 6.3 Zusätzliche Dienstekomponenten..... | 27 |
| 6.3.1 Allgemein..... | 27 |
| 6.3.2 Subjektzentrierte Implementation..... | 27 |
| 6.3.3 Unternehmenszentrierte Implementation..... | 29 |
| 7 Zusätzliche Anforderungen und zu beachtende Punkte..... | 31 |
| 7.1 Zugang zu administrativen Informationen..... | 31 |
| 7.2 AMS-Modelle und Richtlinien..... | 31 |
| 7.2.1 Zugangssteuerungsmodelle..... | 31 |
| 7.2.2 Richtlinien in der Zugangsverwaltung..... | 32 |
| 7.3 Rechtliche und behördliche Anforderungen..... | 32 |
| 8 Praxis..... | 33 |

| | | |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------|----|
| 8.1 | Prozesse | 33 |
| 8.1.1 | Autorisierungsprozesse | 33 |
| 8.1.2 | Rechteverwaltungsprozesse..... | 33 |
| 8.2 | Bedrohungen | 34 |
| 8.3 | Maßnahmenziele..... | 35 |
| 8.3.1 | Allgemein..... | 35 |
| 8.3.2 | Validierung des Zugangsverwaltungsrahmenwerks..... | 35 |
| 8.3.3 | Validierung des Zugangsverwaltungssystems..... | 38 |
| 8.3.4 | Validierung der Pflege eines implementierten AMS..... | 42 |
| Anhang A (informativ) Übliche Zugangssteuerungsmodelle..... | | 46 |
| A.1 | Allgemein..... | 46 |
| A.2 | Zugangssteuerungsmodelle..... | 46 |
| A.2.1 | Allgemein..... | 46 |
| A.2.2 | Benutzerbestimmbare Zugriffssteuerung (DAC)..... | 46 |
| A.2.3 | Systembestimmte Zugangssteuerung (MAC) | 46 |
| A.2.4 | Identifikatorbasierte Zugangssteuerung (IBAC) | 47 |
| A.2.5 | Rollenbasierte Zugangssteuerung (RBAC)..... | 47 |
| A.2.6 | Attributbasierte Zugangssteuerung (ABAC)..... | 48 |
| A.2.7 | Pseudonymbasierte Zugangssteuerung (PBAC)..... | 48 |
| Literaturhinweise | | 49 |
| | | |
| Bilder | | |
| | | |
| Bild 1 | — Modellhafte Abfolge der Zugangssteuerung..... | 15 |
| Bild 2 | — Beziehung zwischen Identitätsverwaltungssystem und Zugangsverwaltungssystem | 16 |
| Bild 3 | — Autorisierung des Zugriffs durch Delegierte..... | 23 |
| Bild 4 | — Föderierte Zugangssteuerung..... | 25 |
| Bild 5 | — AMS-Referenzarchitektur..... | 26 |
| Bild 6 | — Interaktionen der Komponentendienste in einer subjektzentrierten Situation | 28 |
| Bild 7 | — Interaktionen der Komponentendienste in einer unternehmenszentrierten Situation | 30 |