



# ORP.4 Identitäts- und Berechtigungsmanagement

## 1. Beschreibung

### 1.1. Einleitung

Der Zugang zu schützenswerten Ressourcen einer Institution ist auf berechnigte Benutzende und berechnigte IT-Komponenten einzuschränken. Benutzende und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden. Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet.

Beim Berechnigungsmanagement geht es darum, ob und wie Benutzende oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf ihren Rechten Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechnigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Die Übergänge zwischen den beiden Begriffen sind fließend, daher wird in diesem Baustein der Begriff Identitäts- und Berechnigungsmanagement (englisch Identity and Access Management, IAM) benutzt. Zur besseren Verständlichkeit wird in diesem Baustein der Begriff „Benutzendenkennung“ bzw. „Kennung“ synonym für „Benutzendenkonto“, „Konto“, „Login“ und „Account“ verwendet. In diesem Baustein wird der Begriff „Passwort“ als allgemeine Bezeichnung für „Passphrase“, „PIN“ oder „Kennwort“ verwendet.

### 1.2. Zielsetzung

Ziel des Bausteins ist es, dass Benutzende oder auch IT-Komponenten ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die sie autorisiert sind, und unautorisierten Benutzenden oder IT-Komponenten den Zugriff zu verwehren. Dazu werden Anforderungen formuliert, mit denen Institutionen ein sicheres Identitäts- und Berechnigungsmanagement aufbauen sollten.

### 1.3. Abgrenzung und Modellierung

Der Baustein ORP.4 *Identitäts- und Berechnigungsmanagement* ist für den Informationsverbund einmal anzuwenden.

In diesem Baustein werden grundsätzliche Anforderungen für den Aufbau eines Identitäts- und Berechtigungsmanagements beschrieben.

Anforderungen, die Komponenten eines Identitäts- und Berechtigungsmanagement betreffen, wie Betriebssysteme oder Verzeichnisdienste, sind in den entsprechenden Bausteinen zu finden (z. B. SYS.1.3 *Server unter Linux und Unix*, SYS.1.2.3 *Windows Server*, APP.2.1 *Allgemeiner Verzeichnisdienst*, APP.2.2 *Active Directory Domain Services*).

## **2. Gefährdungslage**

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* von besonderer Bedeutung.

### **2.1. Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement**

Sind Prozesse beim Identitäts- und Berechtigungsmanagement unzureichend definiert oder implementiert, ist nicht gewährleistet, dass Zugriffe auf das erforderliche Maß eingeschränkt sind und so gegen die Prinzipien Need-to-Know bzw. Least-Privilege verstoßen wird. Der IT-Betrieb erhält möglicherweise keine Informationen über personelle Veränderungen, so dass beispielsweise Konten von ausgeschiedenen Mitarbeitenden nicht gelöscht werden. Diese können somit weiterhin auf schützenswerte Informationen zugreifen.

Auch ist es möglich, dass Mitarbeitende, die in eine neue Abteilung versetzt wurden, ihre alten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamtberechtigungen ansammeln.

### **2.2. Fehlende zentrale Deaktivierungsmöglichkeit von Konten**

In Institutionen haben Mitarbeitende oft Konten für diversen IT-Systemen, wie Produktiv-, Test-, Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Zuständigkeitsbereichen und werden oft von unterschiedlichen Administrierenden verwaltet. Das führt unter Umständen dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Kennung verwendet wird und es auch keine zentrale Übersicht über die Konten auf den einzelnen IT-Systemen gibt. In einem solchen Szenario ist es nicht möglich, bei einem Angriff oder einem Passwortdiebstahl in einem Arbeitsschritt alle Konten der betroffenen Mitarbeitenden zu deaktivieren. Auch können in diesem Szenario bei Ausscheiden von Mitarbeitenden aus der Institution nicht in einem Arbeitsschritt alle Zugänge gesperrt werden.

### **2.3. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten**

Wenn die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe. Bei der Einführung von Identitätsmanagement-Systemen oder Revisionen stellt sich häufig heraus, dass verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig sind. Dies führt unter Umständen dazu, dass Benutzende Berechtigungen auf Zuruf erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

### 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Benutzende, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

#### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

##### **ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen (B) [IT-Betrieb]**

Es MUSS geregelt werden, wie Benutzendenkennungen und -gruppen einzurichten und zu löschen sind. Jede Benutzendenkennung MUSS eindeutig einer Person zugeordnet werden können. Benutzendenkennungen, die längere Zeit inaktiv sind, SOLLTEN deaktiviert werden. Alle Benutzenden und Benutzendengruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden. Nicht benötigte Benutzendenkennungen, wie z. B. standardmäßig eingerichtete Gastkonten oder Standard-Administrierendenkennungen, MÜSSEN geeignet deaktiviert oder gelöscht werden.

##### **ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen (B) [IT-Betrieb]**

Benutzendenkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden (Prinzip der geringsten Berechtigungen, englisch Least Privileges und Erforderlichkeitsprinzip, englisch Need-to-know). Bei personellen Veränderungen MÜSSEN die nicht mehr benötigten Benutzendenkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeitende Berechtigungen, die über den Standard hinausgehen, DÜRFEN diese NUR nach zusätzlicher Begründung und Prüfung vergeben werden. Zugriffsberechtigungen auf Systemverzeichnisse und -dateien SOLLTEN restriktiv eingeschränkt werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.

##### **ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile (B) [IT-Betrieb]**

Es MUSS dokumentiert werden, welche Benutzendenkennungen, angelegte Benutzendengruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzendenkennungen, angelegten Benutzendengruppen und Rechteprofile MUSS regelmäßig daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt. Dabei MUSS auch geprüft werden, ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzenden entspricht. Die Dokumentation MUSS vor unberechtigtem

Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.

#### **ORP.4.A4 Aufgabenverteilung und Funktionstrennung (B) [IT-Betrieb]**

Die von der Institution definierten unvereinbaren Aufgaben und Funktionen (siehe Baustein ORP.1 *Organisation*) MÜSSEN durch das Identitäts- und Berechtigungsmanagement getrennt werden.

#### **ORP.4.A5 Vergabe von Zutrittsberechtigungen (B) [IT-Betrieb]**

Es MUSS festgelegt werden, welche Zutrittsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Die Ausgabe bzw. der Entzug von verwendeten Zutrittsmitteln wie Chipkarten MUSS dokumentiert werden. Wenn Zutrittsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zutrittsberechtigten SOLLTEN für den korrekten Umgang mit den Zutrittsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechnigte Personen vorübergehend gesperrt werden.

#### **ORP.4.A6 Vergabe von Zugangsberechtigungen (B) [IT-Betrieb]**

Es MUSS festgelegt werden, welche Zugangsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Wenn Zugangsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zugangsberechnigten SOLLTEN für den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechnigte Personen vorübergehend gesperrt werden.

#### **ORP.4.A7 Vergabe von Zugriffsrechten (B) [IT-Betrieb]**

Es MUSS festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden im Rahmen der Zugriffskontrolle Chipkarten oder Token verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Anwendenden SOLLTEN für den korrekten Umgang mit Chipkarten oder Token geschult werden. Bei längeren Abwesenheiten SOLLTEN berechnigte Personen vorübergehend gesperrt werden.

#### **ORP.4.A8 Regelung des Passwortgebrauchs (B) [Benutzende, IT-Betrieb]**

Die Institution MUSS den Passwortgebrauch verbindlich regeln (siehe auch ORP.4.A22 *Regelung zur Passwortqualität* und ORP.4.A23 *Regelung für passwortverarbeitende Anwendungen und IT-Systeme*). Dabei MUSS geprüft werden, ob Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollen, oder ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können.

Passwörter DÜRFEN NICHT mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung MUSS ein eigenständiges Passwort verwendet werden. Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden. Passwörter MÜSSEN geheim gehalten werden. Sie DÜRFEN NUR den Benutzenden persönlich bekannt sein. Passwörter DÜRFEN NUR unbeobachtet eingegeben werden. Passwörter DÜRFEN NICHT auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden. Ein Passwort DARF NUR für eine Hinterlegung für einen Notfall schriftlich fixiert werden. Es MUSS dann sicher aufbewahrt werden. Die Nutzung eines Passwort-Managers SOLLTE geprüft werden. Bei Passwort-Managern mit Funktionen oder Plug-ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, MÜSSEN diese Funktionen und Plug-ins deaktiviert werden. Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

#### **ORP.4.A9 Identifikation und Authentisierung (B) [IT-Betrieb]**

Der Zugriff auf alle IT-Systeme und Dienste MUSS durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzenden, Dienste oder IT-Systeme abgesichert sein. Vorkonfigurierte Authentisierungsmittel MÜSSEN vor dem produktiven Einsatz geändert werden.

### **ORP.4.A22 Regelung zur Passwortqualität (B) [IT-Betrieb]**

In Abhängigkeit von Einsatzzweck und Schutzbedarf **MÜSSEN** sichere Passwörter geeigneter Qualität gewählt werden. Das Passwort **MUSS** so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort **DARF NICHT** zu kompliziert sein, damit Benutzende in der Lage sind, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden.

### **ORP.4.A23 Regelung für passwortverarbeitende Anwendungen und IT-Systeme (B) [IT-Betrieb]**

IT-Systeme oder Anwendungen **SOLLTEN NUR** mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel **SOLLTEN** vermieden werden. Es **MÜSSEN** Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so **SOLLTE** geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden.

Standardpasswörter **MÜSSEN** durch ausreichend starke Passwörter ersetzt werden. Vordefinierte Kennungen **MÜSSEN** geändert werden. Es **SOLLTE** sichergestellt werden, dass die mögliche Passwortlänge auch im vollen Umfang von verarbeitenden IT-Systemen geprüft wird. Nach einem Passwortwechsel **DÜRFEN** alte Passwörter **NICHT** mehr genutzt werden. Passwörter **MÜSSEN** so sicher wie möglich gespeichert werden. Bei Kennungen für technische Konten, Dienstkonten, Schnittstellen oder Vergleichbares **SOLLTE** ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.

Bei der Authentisierung in vernetzten Systemen **DÜRFEN** Passwörter **NICHT** unverschlüsselt über unsichere Netze übertragen werden. Wenn Passwörter in einem Intranet übertragen werden, **SOLLTEN** sie verschlüsselt werden. Bei erfolglosen Anmeldeversuchen **SOLLTEN** die passwortverarbeitenden Anwendungen oder die IT-Systeme keinen Hinweis darauf geben, ob Passwort oder Kennung falsch sind.

## **3.2. Standard-Anforderungen**

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie **SOLLTEN** grundsätzlich erfüllt werden.

### **ORP.4.A10 Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen (S) [IT-Betrieb]**

Benutzendenkennungen mit weitreichenden Berechtigungen **SOLLTEN** mit einer Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, geschützt werden.

### **ORP.4.A11 Zurücksetzen von Passwörtern (S) [IT-Betrieb]**

Für das Zurücksetzen von Passwörtern **SOLLTE** ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Die Mitarbeitenden des IT-Betriebs, die Passwörter zurücksetzen können, **SOLLTEN** entsprechend geschult werden. Bei höherem Schutzbedarf des Passwortes **SOLLTE** eine Strategie definiert werden, falls Mitarbeitende des IT-Betriebs aufgrund fehlender sicherer Möglichkeiten der Übermittlung des Passwortes die Verantwortung nicht übernehmen können.

### **ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (S) [IT-Betrieb]**

Es **SOLLTE** ein Authentisierungskonzept erstellt werden. Darin **SOLLTE** für jedes IT-System und jede Anwendung definiert werden, welche Funktions- und Sicherheitsanforderungen an die Authentisierung gestellt werden. Authentisierungsinformationen **MÜSSEN** kryptografisch sicher gespeichert werden. Authentisierungsinformationen **DÜRFEN NICHT** unverschlüsselt über unsichere Netze übertragen werden.

### **ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen (S) [IT-Betrieb]**

Es SOLLTEN dem Schutzbedarf angemessene Identifikations- und Authentisierungsmechanismen verwendet werden. Authentisierungsdaten SOLLTEN durch das IT-System bzw. die IT-Anwendungen bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt werden. Das IT-System bzw. die IT-Anwendung SOLLTE nach jedem erfolglosen Authentisierungsversuch weitere Anmeldeversuche zunehmend verzögern (Time Delay). Die Gesamtdauer eines Anmeldeversuchs SOLLTE begrenzt werden können. Nach Überschreitung der vorgegebenen Anzahl erfolgloser Authentisierungsversuche SOLLTE das IT-System bzw. die IT-Anwendung die Benutzendenkennung sperren.

### **ORP.4.A14 Kontrolle der Wirksamkeit der Benutzendentrennung am IT-System bzw. an der Anwendung (S) [IT-Betrieb]**

In angemessenen Zeitabständen SOLLTE überprüft werden, ob die Benutzenden von IT-Systemen bzw. Anwendungen sich regelmäßig nach Aufgabenerfüllung abmelden. Ebenso SOLLTE kontrolliert werden, dass nicht mehrere Benutzende unter der gleichen Kennung arbeiten.

### **ORP.4.A15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement (S) [IT-Betrieb]**

Für das Identitäts- und Berechtigungsmanagement SOLLTEN folgenden Prozesse definiert und umgesetzt werden:

- Richtlinien verwalten,
- Identitätsprofile verwalten,
- Benutzendenkennungen verwalten,
- Berechtigungsprofile verwalten sowie
- Rollen verwalten.

### **ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle (S) [IT-Betrieb]**

Es SOLLTE eine Richtlinie für die Zugriffs- und Zugangskontrolle von IT-Systemen, IT-Komponenten und Datennetzen erstellt werden. Es SOLLTEN Standard-Rechteprofile benutzt werden, die den Funktionen und Aufgaben der Mitarbeitenden entsprechen. Für jedes IT-System und jede IT-Anwendung SOLLTE eine schriftliche Zugriffsregelung existieren.

### **ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (S) [IT-Betrieb]**

Beim Einsatz eines Identitäts- und Berechtigungsmanagement-Systems SOLLTE dieses für die Institution und deren jeweilige Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf geeignet sein. Das Identitäts- und Berechtigungsmanagement-System SOLLTE die in der Institution vorhandenen Vorgaben zum Umgang mit Identitäten und Berechtigungen abbilden können. Das ausgewählte Identitäts- und Berechtigungsmanagement-System SOLLTE den Grundsatz der Funktionstrennung unterstützen. Das Identitäts- und Berechtigungsmanagement-System SOLLTE angemessen vor Angriffen geschützt werden.

### **ORP.4.A18 Einsatz eines zentralen Authentisierungsdienstes (S) [IT-Betrieb]**

Um ein zentrales Identitäts- und Berechtigungsmanagement aufzubauen, SOLLTE ein zentraler netzbasierter Authentisierungsdienst eingesetzt werden. Der Einsatz eines zentralen netzbasierten Authentisierungsdienstes SOLLTE sorgfältig geplant werden. Dazu SOLLTEN die Sicherheitsanforderungen dokumentiert werden, die für die Auswahl eines solchen Dienstes relevant sind.

## **ORP.4.A19 Einweisung aller Mitarbeitenden in den Umgang mit Authentisierungsverfahren und -mechanismen (S) [Benutzende, IT-Betrieb]**

Alle Mitarbeitende SOLLTEN in den korrekten Umgang mit dem Authentisierungsverfahren eingewiesen werden. Es SOLLTE verständliche Richtlinien für den Umgang mit Authentisierungsverfahren geben. Die Mitarbeitenden SOLLTEN über relevante Regelungen informiert werden.

### **3.3. Anforderungen bei erhöhtem Schutzbedarf**

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

## **ORP.4.A20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System (H) [IT-Betrieb]**

Es SOLLTE geprüft werden, inwieweit ein ausgefallenes Identitäts- und Berechtigungsmanagement-System sicherheitskritisch für die Geschäftsprozesse ist. Es SOLLTEN Vorkehrungen getroffen werden, um bei einem ausgefallenen Identitäts- und Berechtigungsmanagement-System weiterhin arbeitsfähig zu sein. Insbesondere SOLLTE das im Notfallkonzept vorgesehene Berechtigungskonzept weiterhin anwendbar sein, wenn das Identitäts- und Berechtigungsmanagement-System ausgefallen ist.

## **ORP.4.A21 Mehr-Faktor-Authentisierung (H) [IT-Betrieb]**

Es SOLLTE eine sichere Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, zur Authentisierung verwendet werden.

## **ORP.4.A24 Vier-Augen-Prinzip für administrative Tätigkeiten (H) [IT-Betrieb]**

Administrative Tätigkeiten SOLLTEN nur durch zwei Personen durchgeführt werden können. Dazu SOLLTEN bei Mehr-Faktor-Authentisierung die Faktoren auf die zwei Personen verteilt werden. Bei der Nutzung von Passwörtern SOLLTEN diese in zwei Teile zerlegt werden und jede der zwei Personen enthält einen Teil.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology-Security techniques-Information security management systems-Requirements“ im Anhang A.9 Zugangssteuerung Vorgaben für die Identitäts- und Berechtigungsmanagement.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 29146:2016 “Information technology - Security techniques - A framework for access management“ Vorgaben für die Identitäts- und Berechtigungsmanagement.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.4 Identity and Access Management Vorgaben für die Identitäts- und Berechtigungsmanagement.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-53A, insbesondere Bereiche AC und IA, Hinweise für Identitäts- und Berechtigungsmanagement.