Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.05

Authentifizierung und IAM

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.1

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Definition von Anforderungen an das Access und Identity Management. Zusätzlich werden Anforderungen an die Authentisierung und Autorisierung sowie an das Privileged Identity Management festgelegt.

1. Access- und Identity-Management

1.1. Ziel

Das Ziel dieses Kapitels ist es, konzernweit einheitliche Vorgaben und Mindeststandards für Access und Identity-Management (AIM) zu definieren. Das Access- und Identity-Management ist unter dem Dach der IT-Sicherheit des Audi Konzerns zusammengefasst und in den einzelnen Gesellschaften ausgeprägt. Die Richtlinie bildet die Grundlage für weitere gesellschaftsspezifische Vorgaben und ist über Maßnahmen und Anweisungen der einzelnen Gesellschaft zu konkretisieren.

Der Umgang mit Identitäten, Konten, Berechtigungen und Rollen ist derart zu gestalten, dass das Risiko einer Beeinträchtigung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität beim Zugriff auf Daten des Audi Konzerns minimiert wird (Need-to-Know-Prinzip).

1.2. Grundsätze

Folgende allgemeine Rahmenbedingungen bilden die Grundlage für die Umsetzung des Access- und Identity-Managements:

- Die Gesamtverantwortung für Access- und Identity-Management liegt bei der IT-Sicherheit im Konzern[1]; die Marken / Gesellschaften des Konzerns richten sich bei der Umsetzung nach dem Konzernregelwerk.
- Die Nutzung der zentral bereit gestellten Access & Identity Services ist verpflichtend sofern es sich um gesellschafts- bzw. konzernübergreifende Belange handelt. Ausnahmen sind mit der zuständigen Stelle[2] der IT-Sicherheit im Konzern und den entsprechenden Gremien (siehe Kapitel 1.4) abzustimmen. Die grundlegende Architektur der Access & Identity Services umfasst fünf Schichten (siehe Kapitel 1.3). Diese Architektur bildet den Rahmen der Access und Identity Services und ist verbindlich einzuhalten.

Das Access- und Identity Management umfasst mindestens die folgenden Systeme und Komponenten:

- Volkswagen Corporate Directory (VCD)[3]
- Berechtigungsmanagementsysteme zur Steuerung und Vergabe von Zugriffsberechtigungen auf IT Systeme
- Zentralen Systeme und Dienste zur Authentisierung und Autorisierung[4] und deren lokale Ausprägungen

[1] Siehe Anhang B.1.1

[2] Siehe Anhang B.1.1

[3] Meta-Directory auf X.500-Basis

[4] Beispielsweise TAM und K-LDAP

- Alle Systeme und Prozesse zur Anlage, Aktualisierung und Löschung digitaler Identitäten und Zugriffsberechtigungen
- Werkzeuge zur Synchronisation von Berechtigungsnachweisen (Zertifikate, Benutzernamen, Kennwörter, Token, etc.)

Folgende Prinzipien sind beim Access- und Identity Management zu beachten:

- Minimalprinzip: Die Berechtigungsausprägung orientiert sich an dem für die zur Aufgabenstellung unbedingt notwendigen, geringsten möglichen Funktionen bzw. Zugang zu Daten.
- Funktionstrennungsprinzip: Die Notwendigkeit einer zwingenden Aufgabentrennung (Segregation of Duties – SoD) in beteiligten Prozessen ist zu analysieren und ggf. zu definieren, damit ein Mitarbeiter nicht allein den gesamten Prozess bearbeiten kann.
- Genehmigungsprinzip: Sämtliche Beantragungen von Berechtigungen in jedweder Form müssen nachvollziehbar genehmigt und dokumentiert werden.

Diese Regelung trägt dazu bei, zusätzlich erforderliche Services sicher zu entwickeln und das Niveau der bereits angebotenen Access & Identity Services kontinuierlich zu verbessern. Dieses wird erreicht durch:

- Standardisierte und konzernweit gültige Vorgaben
- Nachvollziehbare und konzernweite Umsetzung der Regeln in jeder Organisationseinheit
- Maßnahmen zur Sicherstellung der Wirksamkeit von Regelungen und Vorgaben

Sich daraus ergebene Maßnahmen sind in jeder Gesellschaft operativ umzusetzen und kontinuierlich auf Wirksamkeit zu überprüfen.

1.3. Schichtenmodell

Die AIM Architektur wird durch die Access und Identity Services (AIS) und die entsprechenden Gremien[5] definiert. Die in diesem Kapitel beschriebene Architektur ist bei der Nutzung von Access und Identity Services (AIS) verpflichten zu nutzen. Die grundlegende Architektur umfasst fünf Schichten:

- Identity Administration Schicht
- Identity Consolidation Schicht
- User Management Schicht
- Authentication Schicht
- Authorization and Access Schicht

Das folgende Schaubild stellt die Architektur und die fünf Schichten graphisch dar:

[5] Siehe Kapitel 1.4

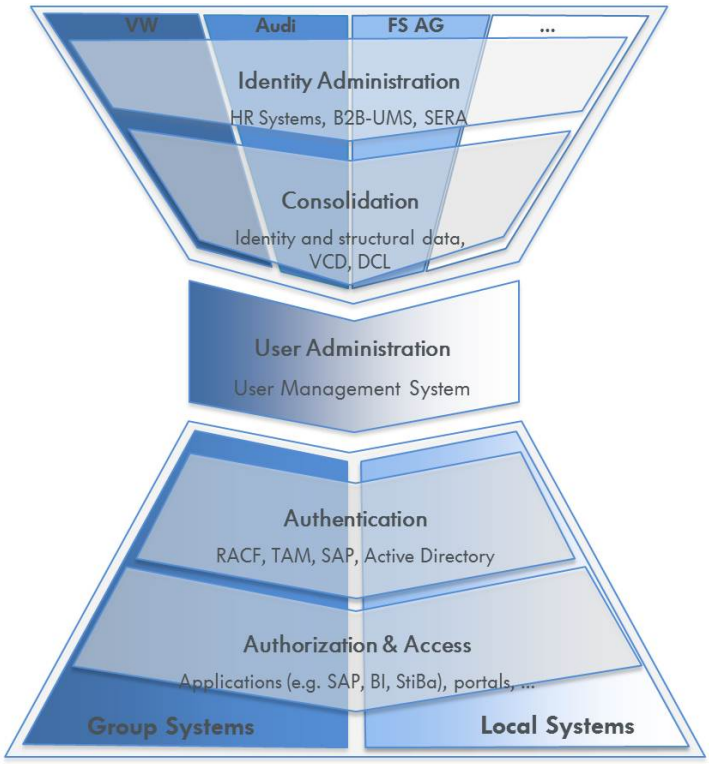


Abbildung 1: AIS Schichtenmodell

Systeme einer höheren Schicht sind führend gegenüber Systemen in niedrigeren Schichten. Im folgenden sind die Schichten detailliert beschrieben.

1.3.1.1 Identity Administration Schicht

In dieser Schicht werden personenbezogene Stammdaten angelegt und verwaltet (z. B. SAP HR). Jeder realen Person muss eine eindeutige persönliche Identifikation entsprechend der Prozesse und Regelungen der verantwortenden Gesellschaft zugeordnet werden.

In Kapitel 2 - Identity Management (Identitätsmanagement sind die geltenden Anforderungen hinsichtlich dieser Schicht beschrieben.

1.3.1.2 Identity Consolidiation Schicht

Die personenbezogenen Stammdaten werden in der Identity Consolidation Schicht agregiert. Jede Person wird durch eine Identität im Volkswagen Corporate Directory (VCD) repräsentiert und mit einer global eindeutigen ID (GID) versehen. Die Korrelation zwischen der persönlichen eindeutigen Identifikation und einem PKI-Zertifikaten findet ebenfalls in dieser Schicht statt.

Der Zugriff auf IT Systeme des Konzerns darf nur auf Grundlage einer Identität aus der Identity Consolidation Schicht erfolgen.

In Kapitel 2 - Identity Management (Identitätsmanagement sind die Anforderungen hinsichtlich dieser Schicht beschrieben.

1.3.1.3 User Administration Schicht

In der User Administration Schicht werden die Rollen und Berechtigungen für Zugriffe auf IT Systeme des Konzerns verwaltet. Hier findet im Berechtigungsmanagementsystem (User Management System - UMS) die Zuordnung von Rollen und Berechtigungen zur Identität statt.

Alle Änderungen müssen revisionssicher und gemäß den landes- oder gesellschaftsspezifischen Vorgaben[6] protokolliert und archiviert werden.

In Kapitel 3- Access Management (Berechtigungsmanagement) sind die Anforderungen hinsichtlich dieser Schicht beschrieben.

1.3.1.4 Authentication Schicht

In der Authentication Schicht sind die IT Systeme angesiedelt, die einen Benutzer anhand seiner Personendaten für einen Systemzugriff authentisieren. Beispiele dafür sind: RACF, TAM, Active Directory, UNIX.

In Kapitel 4- Authe sind die Anforderungen hinsichtlich dieser Schicht beschrieben.

1.3.1.5 Authorization & Access Schicht

Hier prüfen Systeme wie Portale und Applikationen, ob der sich anmeldende Benutzer die passende Berechtigung zum Systemzugriff hat.

1.4. Übergreifende Verantwortlichkeiten und Gremien

Um eine gute Qualität der AIS sowie deren Rollout in die einzelnen Gesellschaften sicherzustellen wird folgendes Zusammenarbeitsmodell innerhalb der AIS-Kompetenzorganisationen im Konzern festgelegt.

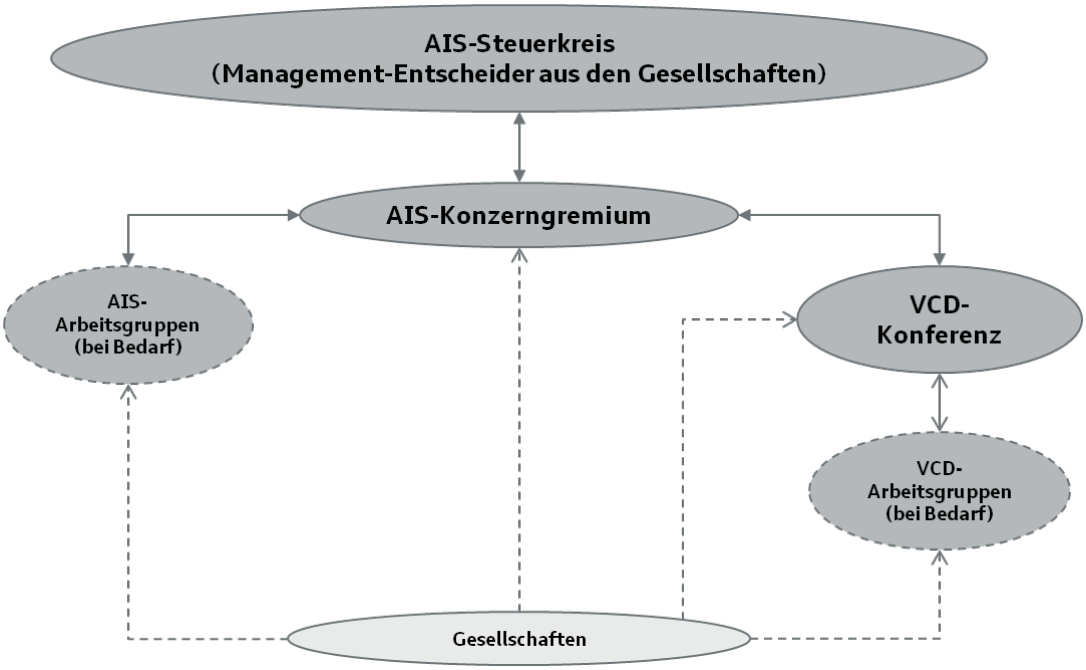


Abbildung 2: AIS-Gremienstruktur

AIS-Steuerkreis

Der AIS-Steuerkreis setzt sich aus den Management-Entscheidern der einzelnen Konzerngesellschaften zusammen.

Er hat folgende Aufgaben und Anforderungen:

[6] Siehe Anhang B.1.3

- Nimmt Projektvorschläge entgegen
- Beauftragt Projekte und gibt Richtlinien für das AIS-Konzerngremium frei
- Ist für die Bereitstellung von Ressourcen und Budgetmittel für die durch ihn beauftragten Projekte verantwortlich
- Dient auch als Eskalationsgremium im Falle von Meinungsverschiedenheiten innerhalb des AIS-Konzerngremiums.
- Tagt mindestens zweimal im Jahr

AIS-Konzerngremium

Das AIS-Konzerngremium setzt sich aus Mitarbeitern der einzelnen Gesellschaften zusammen.

Es hat folgende Aufgaben und Anforderungen:

- Erarbeiten und Abstimmen von Strategie, Richtlinien, Projektvorgaben
- Weitergabe der Ergebnisse zur Entscheidung an den AIS-Steuerkreis
- Führt Aufträge aus dem AIS-Steuerkreis durch
- Tagt mindestens zweimal im Jahr, sowie nach Bedarf

VCD-Konferenz

Die VCD-Konferenz setzt sich aus Mitarbeitern der einzelnen Gesellschaften zusammen. Sie kümmert sich vorrangig um die Prozesse, Architektur, Weiterentwicklung und Betrieb des Volkswagen Corporate Directory (VCD) und stimmt alle notwendigen Themen dazu ab.

Es hat folgende Aufgaben und Anforderungen:

- Erarbeiten und Abstimmen von Strategie, Richtlinien, Projektvorgaben
- Weitergabe der Ergebnisse zur Entscheidung an das AIS-Konzerngremium
- Führt Aufträge aus dem AIS-Steuerkreis durch
- Tagt vier Mal im Jahr

AIS- bzw. VCD-Arbeitsgruppen

Um schnell, effizient und nachhaltig Themen zu bearbeiten, können die Gremien AIS-Konzerngremium und VCD-Konferenz bei Bedarf Arbeitsgruppen einsetzen, die in kleiner Runde ein Thema vorbereiten und zur gemeinsamen Beratung und Verabschiedung an das entsprechende Gremium zurückgeben. Die Mitglieder des Arbeitskreises werden nach Kompetenz für die jeweilige Aufgabenstellung ausgewählt, weitere Fachexperten können den Arbeitskreis beigestellt werden. Die Arbeitsgruppe entscheidet autonom über Häufigkeit und Ort, um die Themenstellung zu bearbeiten. Die Arbeitsgruppe existiert nur bis zum Abschluss ihrer Themenstellung.

2. Identity Management (Identitätsmanagement)

2.1. Ziel

Das Identitätsmanagement ist die zentrale Basis für das Accessmanagement im Konzern und somit elementarer Bestandteil der IT-Sicherheit für Applikationen. Es dient als Grundlage für die Schaffung und Einhaltung eines hohen Sicherheitsniveaus für alle Zugriffe – sowohl von internen als auch externen Mitarbeitern – auf Applikationen im Konzern. Daher ist eine verbindliche Regelung zum Umgang mit Identitäten notwendig, die von allen Konzerngesellschaften akzeptiert und angewendet wird.

Im Folgenden werden Rahmenbedingungen für die Implementierung des Identitätsmanagements im Konzern definiert.

2.2. Grundsätze

Das Identitätsmanagement bildet durch seine Funktionen die Basis für die Vergabe von Zugriffsberechtigungen[7] und dient darüber hinaus als konsolidierter und zentraler Datenspeicher für das Propagieren von Mitarbeiterstammdaten an IT Systeme. Hierfür steht im Konzern ein über alle Gesellschaften standardisiertes Identitätsmanagementsystem zur Verfügung (VCD). Rahmenbedingungen, die den gesamten Lebenszyklus eines Mitarbeiters beschreiben (z. B. Eintritt, Wechsel, Austritt) sind im Identitätsmanagement auf grobgranularer Ebene konzernweit einheitlich abgebildet. Die Lösungsbausteine hierfür stellt AIS zur Verfügung.

2.3. Identitätstypen[8]

Im Identitätsmanagement werden grundsätzlich folgende Identitätstypen unterschieden:

- Interne Mitarbeiter
- Externe Mitarbeiter
- Nicht personalisierte Identitäten

Im Sinne dieser Regelung sind interne Mitarbeiter solche Personen, die Angestellte der Volkswagen AG oder einer Tochtergesellschaft der Volkswagen AG sind, sowie Angestellte von Gesellschaften, an welcher die Volkswagen AG oder eine Tochtergesellschaft der Volkswagen AG eine Mehrheitsbeteiligung (> 50%) besitzt.

Externe Mitarbeiter sind alle Personen, die nicht der Gruppe der internen Mitarbeiter angehören (z. B. Partnerfirmenmitarbeiter, Wirtschaftsprüfer, Mitarbeiter von Behörden).

Nicht personalisierte Identitäten sind entweder technische Identitäten, die für den Systembetrieb erforderlich sind, oder Ressourcen Identitäten, wie z.B. Beamer, Fahrzeuge, Ressourcen Postfächer, etc. Alle genannten Identitätstypen müssen in den zentralen AIS Systemen erfasst werden.

2.4. Anforderungen

Die in diesem Kapitel beschriebenen Anforderungen sind einzuhalten.

---

[7] Siehe Kapitel 3

[8] Definition einer Identität siehe Anhang A.4

2.4.1 Identitäten für interne Mitarbeiter

Für interne Mitarbeiter sind die Personalsysteme (HR-Systeme) der jeweiligen Gesellschaft das führende System. In den Personalsystemen erfolgt hierbei sowohl die Pflege der Mitarbeiter-Stammdaten als auch die Pflege von Personalmaßnahmen. Die Pflege und Fehlerfreiheit der Daten liegt in der Verantwortung der jeweiligen Personalstellen der Gesellschaft. Folgende Personalmaßnahmen sind für das Identitätsmanagement hierbei von Relevanz und müssen an das Identitätsmanagement übermittelt werden:

- Eintritt: Neueintritt eines Mitarbeiters in eine Gesellschaft des Konzerns (vertragliches Verhältnis mit einer Gesellschaft).
- Wechsel: Wechsel eines Mitarbeiters innerhalb einer Gesellschaft z. B. aufgrund organisatorischer Veränderung oder Beförderung
- Austritt: Austritt des Mitarbeiters aus einer Gesellschaft des Konzerns (Auflösung des Vertragsverhältnis mit einer Gesellschaft) oder Übergang in Rente
- Wiedereintritt: Eintritt eines Mitarbeiters in eine Gesellschaft des Konzerns mit welcher bereits ein vertragliches Verhältnis bestand
- Ruhendes Arbeitsverhältnis: Vorübergehende Stilllegung des Arbeitsverhältnisses z.B. durch Elternzeit
- Entsendung: Entsendung eines Mitarbeiters in eine andere Gesellschaft des Konzerns

Für interne Mitarbeiter werden Personalnummern durch die Personalsysteme (HR-Systeme) vergeben. Diese müssen innerhalb einer Gesellschaft eindeutig sein. Personalnummern dürfen nicht an andere Mitarbeiter übertragen oder für andere Mitarbeiter wiederverwendet werden. Personalnummern sind in Kombination mit dem Firmenkurzzeichen (auch Betis-Key oder Company Code) eindeutig im Konzern.

2.4.2 Identitäten für externe Mitarbeiter

Die Stammdaten von externen Mitarbeitern werden in den von der zuständigen Stelle[9] festgelegten Systemen[10] erfasst. Ebenso wird dort der Lebenszyklus der Identitäten externer Mitarbeiter abgebildet. Die Pflege und Fehlerfreiheit der Daten liegt in der Hoheit der jeweiligen Gesellschaft und ist innerhalb der Gesellschaft individuell zu regeln. Grundsätzlich sind für das Identitätsmanagement nur externe Mitarbeiter mit Zugriff auf IT Systeme oder externe Mitarbeiter die den Zugriff beantragt haben von Relevanz. Bei der Pflege der Daten sind mindestens folgende Prozesse abzubilden:

- Eintritt: Eine Beauftragung eines externen Mitarbeiters ist durch eine Konzerngesellschaft erfolgt, der Mitarbeiter benötigt Zugriff auf IT Systeme und muss deshalb als Identität mit seinen Stammdaten erfasst werden
- Wechsel: Ein externer Mitarbeiter wechselt seine Einsatztätigkeit z.B. durch Mitarbeit an einem neuen Projekt oder durch eine organisatorische Veränderung innerhalb der Konzerngesellschaft bei welcher er eingesetzt ist (Umstrukturierung oder ähnliches)
- Austritt: Es liegt keine Beauftragung des externen Mitarbeiters vor und sein Einsatz ist beendet

[9] Siehe Anhang B.2.3

[10] Siehe Anhang B.2.4

Externe Mitarbeiter besitzen keine Stammnummer. Identitätsdaten müssen korrekt und wahrheitsgemäß erfasst werden und dürfen nachträglich nicht derart verändert werden, dass sie eine andere Person repräsentieren. Die Gültigkeit der Identität von externen Mitarbeiter und deren Zuordnung zum jeweiligen Einsatzbereich sind grundsätzlich zeitlich zu begrenzen.

Es ist von der jeweiligen Gesellschaft sicherzustellen, dass die notwendigen Unterlagen wie z.B. Geheimhaltungsvereinbarungen vor Anlage eines externen Mitarbeiters im Identitätsmanagement vorliegen und dokumentiert sind.

2.4.3 Nicht personalisierte Identitäten

Die Erfassung von nicht personalisierten Identitäten erfolgt über die von der zuständigen Stelle[11] festgelegten Systeme. Jede nicht personalisierte Identität muss einem internen Mitarbeiter zugeordnet sein. Bei der Pflege der Daten sind mindestens folgende Prozesse abzubilden:

- Neuanlage: Wird eine nicht personalisierte Identität benötigt, muss diese mit ihren Stammdaten erfasst werden.
- Änderung: Änderungen an den angelegten Stammdaten müssen zeitnah erfasst werden.
- Löschung: Wird die nicht personalisierte Identität nicht mehr benötigt, liegt es in der Verantwortung des zugeordneten internen Mitarbeiters diese zeitnah zu löschen.

2.4.4 Pflege der Stammdaten

Bei der Pflege der Stammdaten in den führenden Systemen und der Übermittlung an das Identitätsmanagement gelten folgende Anforderungen, die entsprechenden Maßnahmen sind umzusetzen:

- Die Konzerngesellschaften müssen die aktuell gültigen Identitätsdaten dem Identitätsmanagementsystem zur Verfügung stellen. Die Daten müssen aktuell gehalten und täglich übermittelt werden.
- Die Datenhoheit liegt bei der jeweiligen Gesellschaft. Die Verantwortung für die Korrektheit der Daten in den Personalsystemen liegt bei den Personalbereichen der jeweiligen Gesellschaften.
- Mitarbeiterdatensätze (vorallem Eintritte und Wiedereintritte) sind rechtzeitig an das Identitätsmanagement zu übermitteln um die Einrichtung von Zugriffen auf IT Systeme bis zum ersten Arbeitstag zu ermöglichen. Der erforderliche Vorlauf für die jeweiligen Personalmaßnahmen muss durch die Gesellschaften definiert werden.
- Mitarbeiter Wechsel sind am Tag der Gültigkeit an das Identitätsmanagement zu übermitteln.
- Mitarbeiter Austritte, ruhende Arbeitsverhältnisse und Entsendungen müssen unmittelbar nach dem letzten Arbeitstag in Kraft treten.
- Im Identitätsmanagement muss jederzeit erkenntlich sein, um welchen Typ[12] von Mitarbeiter es sich handelt.

[11] Siehe Anhang B.2.5

[12] Siehe Kapitel 2.3

2.4.5 Datenkategorien

Folgende Datenkategorien für interne und externe Mitarbeiter mit den zugehörigen Attributen müssen an das Identitätsmanagement geliefert werden:

- Mitarbeiterstammdaten (z.B. Stammnummer, Name, Geburtsdatum, Adresse, Firma, Kostenstelle, OE-Zuordnung, Eintrittsdatum, Funktion)
- OE-Strukturdaten (z.B. OE-Bezeichnungen, OE-Hierarchie, OE-Leiter)
- Verrechnungskostenstellen der Mitarbeiter (z. B. Kostenstellenbezeichnung, Kostenstellennummer)

Die exakte Festlegung der Daten, Formate und Liefermethoden erfolgt im Rahmen eines Integrationsprojekts mit der zuständigen Stelle[13] im Konzern.

2.4.6 Zugriff auf Daten im Identitätsmanagement

Auf die Daten im Identitätsmanagement kann Zugriff gewährt werden. Der Zugriff muss schriftlich bei der zuständigen Stelle[14] beantragt werden. Die Freigabe für den Zugriff ist durch von der Gesellschaft autorisierte Stellen zu erteilen (z. B. Datenschutz und/oder Dateneingentümer). Der Zugriff wird durch die zuständige Stelle[15] dokumentiert.

2.5. Verantwortlichkeiten

Das Identitätsmanagement ist durch das Volkswagen Corporate Directory (VCD) abgebildet. Es handelt sich hierbei um einen Verbund[16] aus eigenständigen Datenbereichen. Die Gesamtverantwortung des Verbunds liegt bei der zuständigen Stelle[17] des Konzerns. Die Aufnahme von neuen Gesellschaften ist in Absprache mit dieser Stelle und den entsprechenden Gremien[18] abzustimmen.

[13] Siehe Anhang B.1.2

[14] Siehe Anhang B.2.6

[15] Siehe Anhang B.2.7

[16] Siehe Anhang B.2.1

[17] Siehe Anhang B.2.2

[18] Siehe Kapitel 1.4

3. Access Management (Berechtigungsmanagement)

3.1. Ziel

Das Berechtigungsmanagement hat die Gewährleistung sicherer Systemzugriffe im Konzern zum Ziel und soll die technische Umsetzung der Informationssicherheitsregularien unterstützen.

Eine zentrale Administration und Kontrolle von Berechtigungsregeln wird ermöglicht. Primär sollen Informationen zu Zugangsberechtigungen zentral gehalten werden.

3.2. Grundsätze

Das Berechtigungsmanagement ist integraler Bestandteil der Access & Identity Services (AIS) und nutzt die vom Identitätsmanagement bereitgestellten digitalen Identitäten. Im Rahmen der Vergabeprozesse werden der digitalen Identität entsprechende Berechtigungen zugeordnet und ein Account in den jeweiligen Zielsystemen erstellt. Falls keine technischen Gründe dagegensprechen, wird der Accountname auf Basis der Preferred User-ID der digitalen Identität gebildet.

Auf Basis des Vertragsverhältnisses einer Person wird nicht nur deren jeweilige digitale Identität für den Kontext erstellt, sondern es werden bestimmte Berechtigungen mit der Rolle verknüpft, die der Mitarbeiter ausfüllen soll. Für eine digitale Identität dürfen immer nur so viele Zugriffsrechte beantragt, genehmigt und vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (Minimalprinzip). Das zentrale Berechtigungsmanagementsystem von AIS ist das primäre Werkzeug zur Umsetzung dieser Zuordnung.

3.3. Anforderungen und Verantwortlichkeiten

3.3.1 Anbindung an Access & Identity Services

- Wenn Konzerngesellschaften Zugriffe auf Systeme benötigen, die über das Berechtigungsmanagement der Access und Identity Services verwaltet werden, müssen sie an AIS angebunden sein.
- Die Konzerngesellschaften sind verantwortlich für die Umsetzung einer zentralen Administration und Kontrolle von Berechtigungsregeln.
- Konzernübergreifende Systeme müssen an das Berechtigungssystem des Konzerns (UMS) angebunden werden. Über die Anbindung von lokal genutzten Systemen an das Berechtigungsmanagementsystem entscheidet der Systemverantwortliche. Für die Anbindung sind die standardisierten AIS-Services zu verwenden.
- Der Dateneigentümer eines Systems legt fest, ob Konzerngesellschaften Zugriff auf sein System bekommen.

3.3.2 Vergabe und Verwendung von User-IDs

- Das Berechtigungsmanagementsystem ist das führende System für die Vergabe von User-IDs. Durch die Erstellung an zentraler Stelle ist die Eindeutigkeit der User-IDs im gesamten Konzern sichergestellt.

- Die User-IDs werden entsprechend dem Konzern-Format[19] vom Berechtigungsmanagementsystem automatisch nach einem Zufallsalgorithmus generiert.
- Das Format der User-ID darf nicht zu Auswertungs- oder Steuerungszwecken verwendet werden.
- Die User-ID ist immer an die zugehörige Identität aus dem Identitätsmanagement gebunden. Wird die Identität gelöscht, bleibt die User-ID im Berechtigungsmanagementsystem für eine erneute Vergabe dauerhaft gesperrt. Ein Umbenennen der automatisch generierten User-ID ist nicht zulässig.
- Eine persönliche User-ID darf nicht auf andere Personen übertragen werden und dient als eindeutiges Korrelationskriterium zwischen der Identität im Berechtigungsmanagement und dem Benutzerkonto der Anwendung.
- Die User-ID aus dem Berechtigungsmanagementsystem ist für alle Anwendungen zu verwenden. Ausnahmen hiervon sind von der zuständigen Stelle[20] zu genehmigen.

3.3.3 Allgemeine Regeln für die Vergabe und den Entzug von Berechtigungen

- Für jeden Account muss erkennbar sein, für welchen Verwendungszweck der Account eingesetzt wird. Beispiele für Accounttypen sind: persönlicher Account, technischer Account, administrativer Account, Schulungsaccount usw.
- Die Zuordnung von Rollen, Berechtigungen und die damit einhergehende Zuordnung von Accounts in Zielsystemen sind über die im AIS verankerten Systeme anzustoßen.
- Ein Benutzer kann nur dann Berechtigungen erhalten, wenn er über eine digitale Identität verfügt und dieser digitalen Identität eine Konzern-UserID zugeordnet ist. Alle personenbezogenen Berechtigungen im Kontext eines Vertrages sind auf Basis der Konzern-UserID zu vergeben
- Wenn aus fachlicher Notwendigkeit, eine digitale Identität mehrere Konzern-UserIDs benötigt, muss eine dieser Konzern-UserIDs als „preferred UserID“ gekennzeichnet sein.
- Jede UserID muss eindeutig einer Identität zuordenbar sein.
- Der digitalen Identität einer Person ist nur die jeweils zur Funktion passende Fachbereichsrolle zuzuweisen. Dies sollte vollautomatisch durch korrekte Zuordnung der Person in der Aufbauorganisation unter Nutzung der eingesetzten Werkzeuge zur Attributs- und Rollenverwaltung der Access & Identity Services erfolgen. Die zur „Grundausstattung” gehörende Zuordnung von IT-Ressourcen (Die „Grundausstattung“ ist durch die jeweilige Gesellschaft zu definieren) erfolgt durch die im AIS verankerten Systeme. Weitere Berechtigungen können beantragt werden. Diese müssen gemäß dem Vier-Augen-Prinzips durch den disziplinarischen Vorgesetzen und den Dateneigentümer oder einen benannten Vertreter (z.B. EDV Koordinatoren, Keyuser) freigegeben werden. Die Nutzung eines Werkzeugs zur Automation und Dokumentation (Workflow-Tool) wird empfohlen.
- Die fachlich bezogenen Zugriffsrechte eines Mitarbeiters, der während eines bestimmten Zeitraums mehrere Organisationseinheiten des Konzerns durchläuft (z. B. Auszubildende, Praktikanten) müssen nach Ende des Einsatzes in einer

[19] Siehe Anhang A.1.5

[20] Siehe Anhang B.3.2

Organisationseinheit deaktiviert und nach Ende der Ausbildung komplett entzogen werden. Die „preferred“ User-ID und die personenbezogenen Zugriffsrechte (z. B. Windows-Account, Mailbox, WA@Web, Mitarbeiter-Portal) sollen auch nach der Ausbildung erhalten bleiben. Die Entscheidung über die personenbezogenen Zugriffsrechte liegt bei den Gesellschaften.

- Die Verwaltung von Berechtigungen muss so ausgelegt sein, dass Verantwortlichkeiten möglichst getrennt werden (Segregation of Duty, SoD[21]). Administratoren dürfen sich nicht selbst verwalten können.
- Das direkte Löschen von Accounts in online-angebundenen Systemen ist im Berechtigungsmanagementsystem durch die Administratoren nicht erlaubt. Ein Account darf nur für das Löschen vorgemerkt und somit gesperrt werden. Innerhalb des automatischen Sperr- und Löschprozesses soll das Löschen zeitversetzt nach einem Regelwerk im Berechtigungsmanagementsystem erfolgen. Die Vorgaben für die Sperr- und Löschintervalle sind durch die zuständige Stelle[22] zu definieren.
- Ist ein System nicht direkt an das Berechtigungsmanagementsystem angeschlossen, muss dennoch über das Berechtigungsmanagementsystem eine User-ID beantragt und generiert werden. Diese UserID muss zwingend im Ziel-System erzeugt und genutzt werden.
- Für externe Mitarbeiter muss jeder Zugriff zeitlich eingeschränkte Gültigkeit besitzen.

3.3.4 Berechtigungsvergabe in Konzerngesellschaften

- Die Anbindung von Konzerngesellschaften an das Berechtigungsmanagementsystem hat durch die verantwortliche Stelle[23] gemäß des unten stehenden Verfahrens zu erfolgen.
- Jede Konzerngesellschaft ist für die Berechtigungsvergabe in der Gesellschaft selbst verantwortlich. Das erfordert den Aufbau einer Administration für das Berechtigungsmanagementsystem in der Gesellschaft. Sollte die Konzerngesellschaft keine eigene Administration aufbauen können, kann die Administration für das Berechtigungsmanagementsystem einer anderen Konzerngesellschaft die Aufgabe als Dienstleistung übernehmen. Hierbei ist die Dienstleistung zwischen den beiden Konzerngesellschaften vertraglich unter Berücksichtigung der jeweiligen rechtlichen Grundlagen abzusichern.

3.3.5 Prüfung der Zuordnung von Berechtigungen

- Die regelmäßige Überprüfung von Berechtigungen ist gemäß der Informationssicherheitshandlungsleitlinien für Führungskräfte[24] durchzuführen.
- Die Gesellschaften sind verpflichtet einen Prozess zur Rezertifizierung[25] zu definieren und diesen entsprechend umzusetzen. Der Prozess muss mindestens folgende Aspekte definieren:

- Verantwortlichkeiten im Rahmen der Rezertifizierung
- Transparente Beschreibung zur Auswahl von Systemen die zu rezertifizieren sind

[21] Siehe Kapitel 1.2

[22] Siehe Anhang B.3.4

[23] Siehe Anhang B.3.1

[24] Siehe Anhang A.1.2

[25] Siehe Anhang B.3.3

- Zeitintervallen in welchen die ausgewählten Systeme zu rezertifizieren sind
- Detailtiefe auf welcher die Rezertifizierung je System durchgeführt wird (z. B. Rezertifizierung des Zugangs zum System oder Rezertifizierung einzelner Berechtigungen innerhalb des Systems)

3.3.6 Administrative Berechtigungen im Berechtigungsmanagementsystem

- Administratoren von Konzerngesellschaften dürfen im Berechtigungsmanagementsystem nur die Berechtigungen für die Berechtigungsvergabe in ihrem Zuständigkeitsbereich erhalten.
- Administratoren dürfen ihre Berechtigungen nicht weitervererben. Die Berechtigungsvergabe darf nur nach dem dafür geltenden Genehmigungsprozess erfolgen.
- Eine Lesezugriffsberechtigung auf alle Personen im Berechtigungsmanagementsystem durch externe Mitarbeiter ist nur zulässig, wenn die Sicht auf die Daten beschränkt ist, die im Rahmen der Aufgabe erforderlich sind (z. B. Rolle Profile-Verantwortlicher).

3.3.7 Administration im Berechtigungsmanagementsystem von externen Mitarbeitern

- Die Übernahme von Berechtigungen und User-ID bei einem Firmenwechsel eines externen Mitarbeiters ist nur erlaubt, wenn der zuständige Fachbereichsverantwortliche bestätigt, dass der externe Mitarbeiter in derselben Aufgabe weiterhin tätig bleibt. Der externe Mitarbeiter und die neue Firma müssen den Wechsel schriftlich bestätigen. Gesellschaftsspezifische Regelungen bezüglich des B2B-Identity-Prozesses[26] sind zu beachten.
- Es dürfen an externe Mitarbeiter nur Berechtigungen für die Konzerngesellschaft(en) vergeben werden, in der sie tätig sind. Dies muss zumindest organisatorisch sichergestellt werden.
- Wechselt ein externer Mitarbeiter die Firma mit Änderung des Aufgabenbereichs und des Fachbereichsverantwortlichen, müssen ihm alle Berechtigungen entzogen werden.

[26] B2B-Identity ist ein Prozess, der die Verantwortung über die Anlage und Administration der Personendaten von Partnerfirmenmitarbeitern an die Partnerfirma verlagert. Siehe: https://volkswagen-wiki.wob.vw.vwg/wikis/display/aim/B2B-Identity

4. Authentifizierung

4.1. Ziel

Ziel dieses Kapitels ist es, Grundsätze und Anforderungen an die Authentifizierung von Benutzern, technischen Accounts und Geräten zu definieren.

Diese wurden in Übereinstimmung mit dem "NIST Special Publication 800-63B - Digital Identity Guidelines- Authentication and Lifecycle Management" (Stand Juni 2017) definiert.

Wichtiger Hinweis: Bei der Einführung neuer Authentifizierungssysteme sind die detaillierten Anforderungen aus NIST SP 800-63B und den zugehörigen Dokumenten zu beachten.

4.2. Grundsätze

Die digitale Identität eines Benutzers muss zuverlässig ermittelt werden können, damit anhand dieser Identität die Berechtigungen für den Zugriff auf Informationen oder Anwendungen überprüft werden können.

Es existieren verschiedene Authentifizierungsverfahren, die verschiedenen Authentifizierungsstufen zugeordnet sind. Diese Authentifizierungsstufen spiegeln das Vertrauen wider, dass die authentifizierte Person die Person ist, für die das verwendete Authentifizierungsmittel (z. B. Benutzerkennung, Token, Smartcard) ausgestellt wurde (Antragsteller).

Authentifizierungsverfahren müssen entsprechend den Vertraulichkeits- und Integritätsanforderungen des Zielsystems oder der Zielanwendung ausgewählt werden.

Zusätzlich zur Authentifizierung von Benutzern kann auch die Authentifizierung von technische Accounts (z. B. bei einer Anwendung-zu-Anwendung-Authentifizierung) oder Netzwerkgeräten erforderlich sein. Weitere Informationen dazu finden Sie im Kapitel "4.5 Spezielle Authentifizierungsanforderungen".

4.3. Authentifizierungsmerkmale und Authentifizierungsmittel

Die folgenden Merkmale (Authentifizierungsmerkmal) können für eine Authentifizierung verwendet werden:

- etwas, das Sie besitzen (z. B. Besitz eines PKI-Ausweises)
- etwas, das Sie wissen (z. B. Kenntnis des Windows-Passworts)
- eine persönliche Eigenschaft (z. B. ein biometrisches Merkmal[27])

Folgende zusätzliche Faktoren können Risiko- und Authentifizierungsanforderungen beeinflussen, ohne selbst ein Authentifizierungsverfahren zu sein.

- Dimension (z. B. räumliche oder zeitliche Einschränkungen)
- Ort (z. B. Remote Zugriff oder Authentifizierungsversuche von entfernten Orten)
- Verhalten (z. B. ungewöhnliche Anmeldezeiten)

[27] Gesellschaftsspezifische Regelungen sind zu beachten. Siehe Anlage B.4.3

Authentifizierungs-verfahren	**Authentifizierungs-merkmale**	**Authentifizierungs-mittel**
Benutzer-Geheimnis	etwas, das Sie wissen	z. B. Passwort
Look-Up Geheimnis	etwas, das Sie besitzen	z. B. Grid Card oder TAN-Liste
Out-of-Band Token	etwas, das Sie besitzen	z. B. Mobile PIN
Single-Factor One-Time Password (OTP) Token	etwas, das Sie besitzen	z. B. ein Key Chain OTP-Token ohne Passworteingabefeld
Multi-Faktor OTP Token	etwas, das Sie besitzen + • etwas, das Sie wissen oder • eine persönliche Eigenschaft	z. B. ein OTP-Generator oder eine App, welche den Benutzer zur Authentisierung mittels PIN oder biometrischem Merkmal auffordert, bevor ein Einmalkennwort vergeben wird
Single-Factor Cryptographic Software	etwas, das Sie besitzen	z. B. eine kryptografische Schlüsseldatei, welche in einer sicheren Umgebung gespeichert ist, allerdings nicht zusätzlich geschützt ist, z. B. durch eine PIN
Single-Factor Cryptographic Token	etwas, das Sie besitzen	z. B. eine Smartcard, die einen kryptografischen Schlüssel enthält
Multi-Factor Cryptographic Software	etwas, das Sie besitzen + • etwas, das Sie wissen oder • eine persönliche Eigenschaft	z. B. eine kryptografische Schlüsseldatei, die in einer sicheren Umgebung gespeichert ist und zusätzlich durch z. B. eine PIN, ein Passwort oder ein biometrisches Merkmal geschützt ist
Multi-Factor Cryptographic Token	etwas, das Sie besitzen + • etwas, das Sie wissen oder • eine persönliche Eigenschaft	z. B. eine Smartcard, die z. B. durch eine PIN, ein Passwort oder ein biometrisches Merkmal geschützt ist

Der Zweck der obigen Tabelle besteht darin, ein Verständnis der im NIST SP 800-63B definierten Authentifizierungsverfahren zu schaffen. Daher sind insbesondere die in der dritten Spalte aufgeführten Authentifizierungsmittel nur Beispiele.

Die folgenden Kapitel beschreiben verbindliche Anforderungen für jedes Authentifizierungsverfahren.

4.3.1 Benutzer-Geheimnisse (z.B. Passwörter/PINs)

Anforderungen an Länge und Komplexität, die über die hier empfohlenen Anforderungen hinausgehen, erhöhen die Schwierigkeit hinsichtlich Merkbarkeit dieser Geheimnisse erheblich und erhöhen die Frustration der Benutzer. Dies führt dazu, dass Benutzer diese Einschränkungen oft kontraproduktiv wahrnehmen und unsichere Passworte verwenden (z. B. durch Hochzählen). Darüber hinaus sind andere Abwehrmaßnahmen wie Passwort-Blacklists, sichere Passwort-Hash-Speicherung und Begrenzung der mehrfachen Falscheingabe von Passworten bei der Verhinderung moderner Brute-Force-Angriffe effektiver.

In diesem Abschnitt werden die Anforderungen[28] ausschließlich für Benutzer-Geheimnisse und nicht für privilegierte Konten beschrieben. Anforderungen für privilegierte Konten und Systemkonten werden im Kapitel "4.5 Spezielle Authentifizierungsanforderungen" beschrieben.

Siehe "NIST SP 800-63-B Anhang A - Stärke der gespeicherten Geheimnisse" für eine detaillierte Beschreibung.

[28] Für Systeme die die Anforderungen nicht erfüllen können gelten die Anforderungen aus B.4.4

Anforderung Passwörter	**Beschreibung**
Basis-Anforderungen	Es müssen folgende Mindestanforderungen erfüllt sein: • Mindestlänge: 12 Zeichen für Benutzerpasswörter • Komplexität: es dürfen keine “einfachen” Passwörter wie Wörterbucheinträge, sich wiederholende oder sequentielle Zeichenfolgen (z.B. “aaaaaa”, “123456abcdefg”), kontext-spezifische Wörter (z.B. persönliche Daten wie Spitzname, Geburtsdatum) verwendet werden. Die Verwendung von passphrases wird empfohlen. • Änderungsintervall max. 365 Tage
Systemanforderung	Authentifizierungssysteme müssen ein mindestens 32- oder höherstelliges Passwort akzeptieren können.
Erlaubte Zeichen	Printable ASCII, Unicode, Leerzeichen sollten akzeptiert werden. Anwender, die ein Passwort mit Unicode Zeichen verwenden, sollten darauf hingewiesen werden, dass einige Zeichen in Systemen unterschiedlich dargestellt werden könnten. Dies kann eine erfolgreiche Anmeldung beeinflussen.
Anwender Information	Bei der Anmeldung sollte der Anwender informiert werden über: • Letzte erfolgreiche Authentifizierung
Begrenzung der mehrfachen Falscheingabe	Mechanismen zur erfolgreichen Begrenzung der Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche müssen implementiert werden um Brute-force-Attacken abzuwehren. Die Anzahl der Fehlversuche muss auf 20 limitiert sein. Nach Erreichen der Anzahl muss eine der nachfolgenden Maßnahmen[29] umgesetzt werden: • Der Account wird gesperrt und der Anwender muss einen Entsperrprozess durchlaufen oder • der Anwender muss ein CAPTCHA ausfüllen oder • der Account ist für 20 Minuten deaktiviert
Passwortkürzung durch das System	Eine systembedingte Passwortkürzung ist verboten.
Normalisierung von Unicode-Zeichen	Der Normalisierungs-Prozess für „Stabilized Strings“ unter Verwendung der NFKC oder NFKD Normalisierung sollte wie in Kapitel 12.1 Unicode Standard Annex 15 [UAX 15] eingesetzt werden

Passwort-Hinweise	Es dürfen nicht authentifizierten Anwendern keine Hinweise zu Passwörtern gegeben werden.
Passwort black lists	Potentielle Passwörter sollten im Rahmen der Vergabe gegen Listen mit oft verwendeten, leicht errat baren, oder bereits kompromittierten Passwörtern verglichen werden. Die Liste sollte beispielsweise folgenden Inhalt haben (kein Anspruch auf Vollständigkeit): • Passwörter die bereits aus erfolgten Angriffen bekannt sind • Wörterbucheinträge • sich wiederholende oder sequentielle Zeichenfolgen (z.B. ‘aaaaaa’, ‘1234abcd’). • kontext-spezifische Wörter, wie beispielsweise der Name des Systems, der Benutzername oder Abwandlungen davon. Falls das gewählte Passwort in der Liste enthalten ist, sollte der CSP (Credential Service Provider) oder die Prüfinstanz den Benutzer unter Angabe des Grundes dazu auffordern ein anderes Passwort zu wählen.
Anwender Unterstüzung	Der Anwender sollte im Rahmen der Passwortvergabe mit Hilfsmitteln wie einem „password-strength meter“ bei der Wahl eines starken Passwortes unterstützt werden.
Verschlüsselte Übertragung	Der Übertragungsweg im Rahmen der Authentifizierung muss verschlüsselt sein.
Passwortspeicherung	Passwörter müssen geschützt gegen offline Attacken aufbewahrt werden. Passwörter müssen mit Hilfe von Salt und Hash Methodiken so gespeichert werden, dass diese nicht wieder herstellbar sind. Der Salt muss dabei mindestens 32 bits länge haben und willkürlich gewählt sein, um die Wahrscheinlichkeit einer Wiederholung des gleichen Hash Wertes zu minimieren. Der Salt und der resultierende Hashwert müssen mittels einem memorized secret authenticator gespeichert werden. (Bsp,PBKDF2)

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Chapter 5.1.1.

[29] Siehe Anhang B.4.5

Anforderung PINs	Beschreibung
Basis-Anforderungen	Es müssen folgende Mindestanforderungen erfüllt sein: • Eine PIN muss aus mindestens 6 Ziffern bestehen. • Es sind keine trivialen PINs zulässig (z.B. „111111“) oder PINs mit persönlichem Bezug (z. B. Geburtsdatum) zulässig.

4.3.2 Lookup Secrets

In der Regel wird ein gedruckter oder elektronischer Authentifikator benötigt, um das / die entsprechende (n) Geheimnis(e) nachzuschlagen, um auf die Aufforderung einer Authentifizierungsinstanz zu antworten. Zum Beispiel kann ein Benutzer aufgefordert werden, einen bestimmten Teil der Ziffern- oder Zeichenfolgen, die auf einer Karte/Tabelle aufgeführt sind, einzugeben.

Diese Art der Authentifizierung wird derzeit im Konzern nicht verwendet.

4.3.3 Out-of-Band

Das Out-of-Band-Authentifizierungsmittel ist ein physisches Gerät, das eindeutig adressierbar ist und sicher mit der Authentifizierungsinstanz über einen bestimmten (sekundären) Kommunikationskanal kommunizieren kann. Das Gerät ist im Besitz und der Kontrolle des Benutzers. Es fällt unter das Authentifizierungsmerkmal "etwas, das du besitzt". Out-of-Band kann als eine der folgenden Arten eingesetzt werden:

- Der Benutzer empfängt über das Out-of-Band-Gerät (z. B. Mobilgerät) ein Geheimnis und gibt es in ein Authentifizierungsformular ein.
- Die Authentifizierungssitzung enthält ein Geheimnis (z. B. eine PIN oder einen QR-Code), der Benutzer gibt dieses Geheimnis in das Out-of-Band-Gerät ein oder scannt das Geheimnis, welches das Gerät über den zweiten Kanal zurückgibt. Dann vergleicht das zentrale Authentifizierungssystem die Geheimnisse.
- Der Benutzer vergleicht die vom primären und vom sekundären Kanal empfangenen Geheimnisse und bestätigt die Authentifizierung über den sekundären Kanal.

Anforderungen	Beschreibung
Dedizierter Kanal	Der Out-of-Band-Authentifikator muss einen separaten Kanal mit der Authentifizierungsinstanz einrichten, um das Out-of-Band-Geheimnis oder –die Authentifizierungsanforderung abzurufen. Dieser Kanal wird als „Out-of-Band“ in Bezug auf den primären Kommunikationskanal betrachtet (selbst wenn er auf demselben Gerät endet), vorausgesetzt, das Gerät gibt keine Informationen von einem Kanal zu dem anderen ohne die Genehmigung des Antragstellers aus. Der dedizierte Kanal muss gegen Angriffe widerstandsfähig sein und eine Manipulationssicherheit bieten.
Out of band authenticator Kommunikation	Das Out-of-Band-Gerät sollte eindeutig adressierbar sein und die Kommunikation über den sekundären Kanal sollte verschlüsselt sein (sofern es nicht über das öffentliche Telefonnetz (PSTN) gesendet wird). Weitere Authentifikatoranforderungen, die für das PSTN spezifisch sind, siehe NIST SP 800-63B Kapitel 5.1.3.3.
Out of band Authenticator Authentifizierung	Der Out-of-Band-Authentifikator muss sich bei der Kommunikation mit der Authentifizierungsinstanz eindeutig authentifizieren: Der Aufbau und die Nutzung eines authentifizierten und geschützten Kanals für die Authentifizierungsinstanz hat mit freigegebenen kryptografischen Standards zu erfolgen. Die Speicherung des verwendeten Schlüssels erfolgt in einem geeigneten, sicheren Speicher, der für die Authentifizierungsapplikation verfügbar ist (z. B. Schlüsselspeicher, TPM, TEE, sicheres Element). Wenn ein Geheimnis von der Authentifizierungsinstanz an das Out-of-Band-Gerät gesendet wird, sollte das Gerät das Authentifizierungsgeheimnis nicht anzeigen, während es gesperrt ist (d. h. es erfordert die Eingabe einer PIN, eines Passcodes oder eines biometrischen Merkmals).

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Chapter 5.1.3.

4.3.4 Single-Factor OTP Device

Ein OTP-Gerät erzeugt Einmalkennworte. Es gibt Hardwaregeräte und softwarebasierte OTP-Generatoren, die auf Geräten wie Mobiltelefonen installiert sind. Diese Geräte verfügen über ein fest integriertes Geheimnis, das als „Seed“ für die Generierung von OTPs verwendet wird und keine Aktivierung durch einen zweiten Faktor erfordert. Das Einmalkennwort wird auf dem Gerät angezeigt und manuell zur Übertragung an die Authentifizierungsinstanz eingegeben, wodurch Besitz und Kontrolle des Geräts bewiesen werden. Ein OTP-Gerät kann beispielsweise 6 Zeichen gleichzeitig anzeigen. Das Geheimnis wird basierend auf einer Nonce, die zeitbasiert sein kann, oder von einem Zähler auf dem Authentifikator und der Authentifizierungsinstanz berechnet. Ein OTP-Gerät ist etwas, das Sie besitzen, wie z.B. RSA-Token.

Anforderungen	Beschreibung
Geheimer Schlüssel und Algorithmus	Der geheime Schlüssel und der Algorithmus müssen mindestens die in der Informationssicherheitsregelung „Kryptografie“[30] angegebene Mindestsicherheitsstärke aufweisen. Die Länge muss so groß sein, dass sichergestellt ist, dass sie für jeden Betrieb des Geräts während seiner gesamten Lebensdauer einmalig ist. Das Klonen von Schlüsseln und Geräten (z. B. Soft-Token) darf nicht möglich sein.
Algorithmen	Es dürfen nur zugelassene Blockchiffren oder Hash-Funktionen sollen verwendet werden, um Schlüssel und Nonce (Zufallszahl) auf sichere Weise zu kombinieren. Es kann ab der 6 Ziffer abgeschnitten werden.
Secret Gültigkeit des Geheimnisses	Wenn der Code/Token zeitbasiert ist, sollte sie sich mindestens nach 2 Minuten ändern (SecureID-Tokens ändern sich jede Minute). Ein Code/Token (PIN) darf nur einmal akzeptiert werden.
Schutz des symmetrischen Schlüssels	Authentifizierungssysteme müssen die geheimen Tokenschlüssel stark schützen.
Schlüsselaustausch	Im Rahmen der der Token-Initialisierung müssen Authentifizierungssysteme freigegebene kryptographische Verfahren verwenden.
Verschlüsselte Übertragung	Es dürfen nur freigegebene Verschlüsselungsverfahren und authentifizierte Kanäle für die Überprüfung des Geheimnisses verwendet werden.

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Chapter 5.1.4.

4.3.5 Multi-Factor OTP Device / Multi-Faktor-OTP-Gerät

Multi-Faktor-OTP-Authentifikatoren arbeiten in ähnlicher Weise wie Ein-Faktor-OTP-Authentifikatoren (siehe vorheriger Abschnitt), außer dass sie die Eingabe eines Geheimnisses (PIN oder Passwort) oder die Verwendung eines Biometrischen Merkmals erfordern, um das Einmalkennwort vom Authentifikator zu erhalten. Daher sind die Anforderungen an Multi-Faktor-OTP-Geräte vergleichbar denen von Single-Faktor-OTP-Geräten (vorheriger Abschnitt). Darüber hinaus gibt es folgende Anforderungen:

[30] Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

Anforderungen	Beschreibung
Re-authentication	Jede Verwendung des Authentifikators muss die Eingabe des zweiten Faktors erzwingen
Activation Secret	Der unverschlüsselte Schlüssel und das Aktivierungsgeheimnis oder alle biometrischen Informationen müssen unmittelbar nach der Erzeugung eines Einmalkennwortes gelöscht werden.

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Chapter 5.1.5.

4.3.6 Single-Factor Cryptographic Software

Ein kryptographischer Ein-Faktor-Authentifikator aud Softwarebasis ist ein kryptografischer Schlüssel, der auf der Festplatte oder einem anderen Medium gespeichert ist. Der kryptografische Software-Authentifikator gehört zum Authentifizierungsmerkmal „etwas, das Sie besitzen“.

Anforderungen	Beschreibung
Schutz des Schlüssels	Der Schlüssel muss in einem geeigneten, sicheren Speicher gespeichert werden (z. B. Schlüsselspeicher, TPM oder TEE falls verfügbar). Der Schlüssel muss stark gegen unbefugte Weitergabe und Vervielfältigung geschützt sein.
Andere Anforderungen	Die Anforderungen an eine kryptografische Ein-Faktor-Software-Authentifizierungsinstanz sind identisch mit denen für einen kryptografischen Ein-Faktor-Geräte-Authentifizierungsinstanz, der im folgenden Abschnitt beschrieben wird.

4.3.7 Single-Factor Cryptographic Devices

Ein kryptographisches Ein-Faktor-Gerät ist ein Hardware-Gerät, das kryptografische Operationen unter Verwendung geschützter kryptografischer Schlüssel durchführt und das Ergebnis über eine direkte Verbindung auf dem Benutzerendgerät bereitstellt. Das Gerät verwendet eingebettete symmetrische oder asymmetrische kryptografische Schlüssel und muss nicht über einen zweiten Authentifizierungsfaktor aktiviert werden. Es gehört zum Authentifizierungsmerkmal “etwas, das Sie besitzen”.

Anforderungen	Beschreibung
Schutz des Schlüssels	Häufig verwendete Verschlüsselungsgeräte sind Smartcards, USB-Geräte oder TPM-Module. Diese Module müssen die FIPS 140-Anforderungen der jeweiligen Authentifizierungsstufe erfüllen, für die sie verwendet werden sollen. Das kryptographische Gerät muss das Exportieren / Klonen des geheimen Schlüssels verhindern.
Schutz des symmetrischen Schlüssels	Der Schlüssel und der eingesetzte Algorithmus müssen mindestens die in der Informationssicherheitsregelung „Kryptografie“[31] angegebenen Anforderungen erfüllen. Nur freigegebene kryptographische Maßnahmen dürfen eingesetzt werden.

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Chapter 5.1.7.

4.3.8 Multi-Factor Cryptographic Software

Im Gegensatz zur software basierten Ein-Faktor-Verschlüsselungslösung erfordert die software basierte Mehrfaktor-Verschlüsselungslösung die Eingabe entweder eines Geheimnisses (Passwort oder PIN) oder einer biometrischen Authentifizierung für den Zugriff auf den geheimen Schlüssel. Der kryptografische Authentifikator gehört zum Authentifizierungsmerkmal “etwas, das Sie besitzen” und er sollte entweder durch etwas, das Sie kennen oder etwas, das Sie sind, aktiviert werden.

Requirement	Description
Wieder-/ Neuauthentifizierung Re-authentication	Jede Verwendung des Authentifikators muss die Eingabe des zweiten Faktors erzwingen
Activation Secret	Der unverschlüsselte Schlüssel und das Aktivierungsgeheimnis oder das biometrische Merkmal sowie alle biometrischen Informationen, die aus dem biometrischen Merkmal abgeleitet werden, müssen unmittelbar nach der Erzeugung einer Authentifizierungstransaktion gelöscht werden.

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Kapitel 5.1.8.

4.3.9 Multi-Factor Cryptographic Device

Ein kryptografisches Multi-Faktor-Gerät ist vergleichbar mit einem kryptografischen Ein-Faktor-Gerät, erfordert jedoch die Aktivierung durch einen zweiten Authentifizierungsfaktor, der ein Geheimnis (Passwort oder PIN) oder ein biometrischer Faktor sein kann. Daher sind

[31] Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

auch die Anforderungen vergleichbar mit denen für kryptografische Ein-Faktor-Geräte. Darüber hinaus gibt es folgende Anforderungen:

Anforderungen	Beschreibung
Wieder-/ Neuauthentifizierung	Jede Verwendung des Authentifikators muss die Eingabe des zweiten Faktors erzwingen
Activation Secret	Der unverschlüsselte Schlüssel und das Aktivierungsgeheimnis oder das biometrische Merkmal sowie alle biometrischen Informationen, die aus dem biometrischen Merkmal abgeleitet werden, müssen unmittelbar nach der Erzeugung einer Authentifizierungstransaktion gelöscht werden.

Weitere Details und Hintergrundinformationen siehe NIST SP 800-63B Kapitel 5.1.9.

4.4. Authentifizierungsstufen und Authenticator Assurance Levels

Es sind vier Authentifizierungsstufen definiert, von denen 3 den entsprechenden NIST Authenticator Assurance Levels (AAL) zugeordnet werden können. Die geeignete Authentifizierungsstufe muss entsprechend den Informationen, auf die zugegriffen wird, und / oder ihrer Vertraulichkeitsklassifizierung ausgewählt werden:

- Sehr schwache Authentifizierung
- Schwache Authentifizierung (AAL1)
- Starke Authentifizierung (AAL2)
- Sehr starke Authentifizierung (AAL3)

Öffentliche Informationen erfordern keine Authentifizierung als Sicherheitsanforderung und werden daher nicht explizit behandelt.

4.4.1 Sehr schwache Authentifizierung

Eine sehr schwache Authentifizierung ist jede Art von Authentifizierung, die nicht die Mindestanforderungen der schwachen Authentifizierung oder höher erfüllt. Für diese Art der Authentifizierung gibt es keine detaillierten Anforderungen, da sie nur für Zwecke verwendet werden darf, bei denen eine Authentifizierung aus der Sicherheitsperspektive nicht erforderlich ist, z. B. Aktionscodes.

Anforderungen	Schwache Authentifizierung
Verwendung zulässig für	• Authentifizierung zu öffentlichen Informationen • Jeder andere Zweck, der aus Sicherheitsgründen keine Authentifizierung erfordert
Zulässige Authentifizierungsverfahren	• Benutzerkennung ohne Passwort oder jede andere Art) • Geteilte PIN z. B. für einen Scanner • Geteiltes Passwort • Alles sonstige
Für diese Art der Authentifizierung gibt es keine weiteren Anforderungen.	

4.4.2 Schwache Authentifizierung (AAL1)

Eine schwache Authentifizierung bietet eine gewisse Sicherheit, dass der Antragsteller einen Authentifizierer überprüft, der an das Konto des Teilnehmers gebunden ist. Folgende Anforderungen müssen erfüllt sein:

Anforderungen	**Schwache Authentifizierung**
Verwendung zulässig für	Authentifizierung durch Systeme und / oder Applikationen, die als "intern" eingestuft sind
Zulässige Verwendung	• Memorized secret • Look-up secret • Out-of-band device • Single-factor OTP device • Oder jedes andere Verfahren das höhere Sicherheit bietet Die übliche Form der Anmeldung mit Benutzerkennung und Passwort ist daher als schwache Authentifizierung zu bewerten.
Zulässige Authentifizierungsverfahren	• One-time-password token (e. g. SecurID card) ohne PIN • Software Zertifikat mit/ohne Passwort • Zentral definierte Benutzerkennung mit Passwort
Neu-/Wieder-Authentifizierung	nach maximal 12 h
Session Timeout	nach maximal 30 min
Sicherheitsvorgaben	NIST SP 800-53 Low baseline (or company specific equivalent)
Widerstandsfähigkeit gegen Man-in-the-middle Angriffe	Erforderlich
Authentifizierungsinstanz - Widerstandsfähigkeit gegen Identitätswechsel	Nicht erforderlich
Authentifizierungsinstanz - Widerstandsfähigkeit gegen Kompromittierung	Nicht erforderlich
Widerstandsfähigkeit gegen Replay Attacken	Nicht erforderlich
Authentication intent	Nicht erforderlich
Aufbewahrungsrichtlinie für Datensätze	Erforderlich
Datenschutz-Vorgaben	Erforderlich

4.4.3 Starke Authentifizierung (AAL2)

Eine starke Authentifizierung (AAL2) stellt sicher, dass der Benutzer bei der Registrierung durch eine oder mehrere Instanzen überprüft wurde. AAL2 wird als ausreichend für Systeme und Applikationen angesehen, die als "vertraulich" klassifiziert sind. Die starke Authentifizierung wird als Identitätsprüfung definiert, die auf mindestens zwei Faktoren (Authentifizierungsmerkmale) basiert und diese kombiniert ("etwas, was Sie wissen" sowie "etwas, was Sie besitzen“)

Anforderungen	**Starke Authentifizierung**
Verwendung zulässig für	Authentifizierung durch Systeme und / oder Applikationen, die als "vertraulich" eingestuft sind
Zulässige Authentifizierungsverfahren	• Multi-Factor OTP Device • Multi-Factor Cryptographic Software • Multi-Factor Cryptographic Device • **oder** Memorized Secret **plus** o Look-Up Secret o Out-of-Band Device o Single-Factor OTP Device o Single-Factor Cryptographic Software o Single-Factor Cryptographic Device
VOLKSWAGEN Standard Authentifizierungsmittel für diese Stufe	• VOLKSWAGEN PKI Karte mit PIN • One-Time-Password token (e. g. SecurID card) mit PIN • OTP Software + Password
Neu-/Wieder-Authentifizierung	• 12 Stunden • oder 15 min Inaktivität Nutzung eines einzelnen Authentifizierungsfaktors ist zulässig
Sicherheitsvorgaben	NIST SP 800-53 Moderate Baseline
Widerstandsfähigkeit gegen Man-in-the-middle Angriffe	Erforderlich
Authentifizierungsinstanz - Widerstandsfähigkeit gegen Identitätswechsel	Nicht erforderlich
Authentifizierungsinstanz - Widerstandsfähigkeit gegen Kompromittierung	Nicht erforderlich
Widerstandsfähigkeit gegen Replay Attacken	Erforderlich
Authentication intent	Empfohlen
Aufbewahrungsrichtlinie für Datensätze Records retention policy	Erforderlich
Datenschutz-Vorgaben Privacy controls	Erforderlich

4.4.4 Sehr starke Authentifizierung (AAL3)

Eine sehr starke Authentifizierung (AAL3) wird im Konzern als Identitätsprüfung definiert, die eine Multi-Faktor-Authentifizierung erfordert, wobei mindestens einer dieser Faktoren ein Hardware-Gerät ist.

Anforderung	**Sehr starke Authentifizierung**
Verwendung zulässig für	Authentifizierung durch Systeme und / oder Applikationen, die als "geheim" eingestuft sind
Zulässige Authentifizierungsverfahren	• Multi-Factor Crypto Device • Single-Factor Crypto Device plus Memorized Secret • Single-Factor OTP Device plus MF Crypto Device oder Software • Single-Factor OTP Device plus SF Crypto Software plus Memorized Secret
VOLKSWAGEN Standard Authentifizierungsmittel für diese Stufe	• VOLKSWAGEN PKI Karte mit PIN
Neu-/Wieder-Authentifizierung	• 12 Stunden • oder maximal 5 Minuten Inaktivität **Muss** beide Faktoren zur Authentifizierung nutzen
Sicherheitsvorgaben	NIST SP 800-53 High Baseline
Widerstandsfähigkeit gegen Man-in-the-middle Angriffe	Erforderlich
Authentifizierungsinstanz - Widerstandsfähigkeit gegen Identitätswechsel	Erforderlich
Authentifizierungsinstanz - Widerstandsfähigkeit gegen Kompromittierung	Erforderlich
Widerstandsfähigkeit gegen Replay Attacken	Erforderlich
Authentication intent	Erforderlich
Aufbewahrungsrichtlinie für Datensätze Records retention policy	Erforderlich
Datenschutz-Vorgaben Privacy controls	Erforderlich

4.5. Spezielle Anforderungen an die Authentifizierung

4.5.1 Remote Access/VPN

Die Anforderungen der Regelung „Netzwerkzugänge“[32] sind zu beachten.

4.5.2 Drucken

Für das Ausdrucken vertraulicher Dokumente ist keine starke Authentifizierung erforderlich, sofern diese Dokumente auf Basis einer starken Authentifizierung erstellt und zum Ausdrucken gesendet wurden. In diesem Fall ist eine schwache Authentifizierung am Drucker basierend auf Besitz (z. B. Auflegen des Werksausweises) oder Wissen (z. B. eine PIN) ausreichend.

Wenn ein ausreichender physischer Zugriffsschutz vorhanden ist, kann auf eine Authentifizierung verzichtet werden.

4.5.3 Authentifizierung von administrativen Benutzerkonten

Weitere Informationen im Kapitel “Administratoren-Authentisierung“ 5.3

4.5.4 Technische Benutzerkonten

Technische Benutzerkonten, auch systembezogene Konten genannt, werden üblicherweise von Applikationen verwendet, um sich z. B. bei Datenbanken oder anderen Backend-Diensten zu authentisieren. Aufgrund der fehlenden Benutzerinteraktion können diese Konten nur über eine der folgenden Methoden authentifiziert werden. Wo technische Benutzerkonten den Zugang zu vertraulichen oder geheimen Daten erlauben, muss ein ganzheitliches Sicherheitskonzept ein angemessenes Sicherheitsniveau gewährleisten. Dies kann umfassen, ist aber nicht darauf beschränkt:

- Einschränkung der Quelladressen
- Sperren des Kontos nach einer vordefinierten Anzahl aufeinanderfolgender fehlgeschlagener Anmeldeversuche (siehe Kapitel 4.3.1)
- Speicherung der Authentifizierungsdaten für technische Benutzerkonten in sicheren Speicherbereichen oder Geräte (z. B. Hardware Security Modulen (HSM))
- Passwortverwaltung innerhalb eines Privileged Identity Management (PIM) z. B. CyberArk.

Es ist verboten, technische Benutzerkonten außerhalb der vorgesehenen Nutzung zu verwenden. Technische Benutzerkonten dürfen nicht für interaktive Anmeldungen von persönlichen Benutzern verwendet werden.

[32] Informationssicherheit Regelung Nr. 03.02.04 Netzwerkzugänge

Authentifizierungsmittel	Anforderungen
Pre-shared Secret (Passwort)	• mindestens 16 Zeichen (Empfehlung mindestens 24 Zeichen) • generiert durch einen Zufallspasswort-Generator • Komplexität: 3 von 4 Kriterien (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen) • Änderungsintervall mindestens jährlich
Kryptografischer Schlüssel (z. B. kryptographische Software oder kryptografische Hardware)	• Ein kryptografischer Schlüssel, der auf dem Authentifizierungssystem in einer Applikation oder einer kryptografischen Hardware gespeichert ist

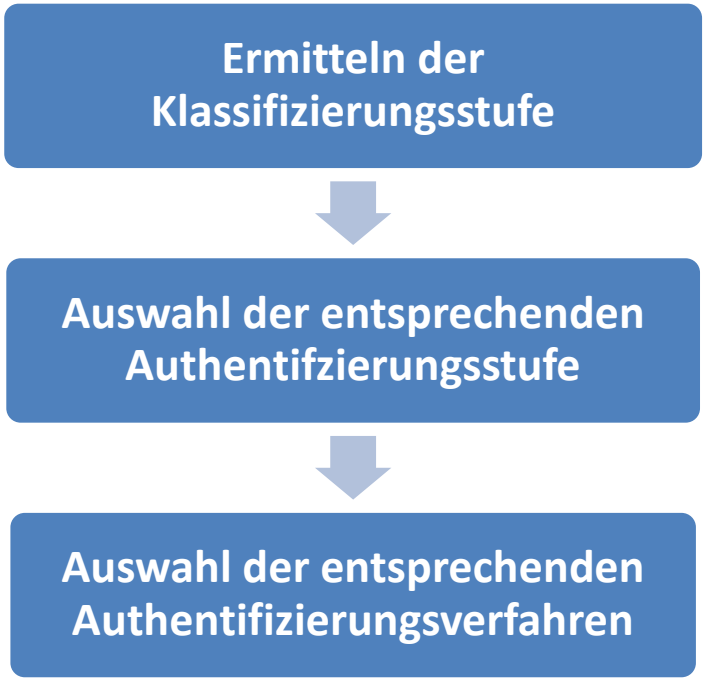
4.5.5 Geräte-Authentifizierung

Für Geräte (z. B. Mobiltelefone), die die Authentifizierungsanforderungen gemäß Kapitel 4.4 nicht unterstützen, muss ein ganzheitliches Sicherheitskonzept erstellt werden, welche ein angemessenes Informationssicherheitsniveau gewährleistet. Dies kann folgende Punkte umfassen, aber auch darüber hinausgehen

- Mobilgeräteverwaltung mit Geräteverschlüsselung und Software-Richtlinien
- Sperren oder Löschen von Geräten nach einer definierten Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche (siehe 4.3.1)
- Verbot, vertrauliche oder geheime Daten zu speichern oder darauf zuzugreifen.

4.6. Allgemeiner Prozess für neue Applikationen und Systeme

In diesem Kapitel wird der allgemeine Prozess zum Auswählen einer geeigneten Authentifizierungsmethode durch den System- oder Applikationsverantwortlichen während der IT-Projektentwurfsphase dargestellt.



1. **Ermitteln der Klassifizierungsstufe**

Die Klassifizierung von Informationen in Anwendungen muss in Übereinstimmung mit dem Prozess der Informationsklassifizierung[33] definiert werden

2. **Auswahl der entsprechenden Authentifizierungsstufe**

Die Authentifizierungsstufe definiert die Sicherheitsstufe der zugehörigen Authentifizierungsmittel und muss entsprechend der Klassifizierung der Informationen[34] ausgewählt werden, die in der authentifizierenden Anwendung oder dem System gespeichert sind. Wenn technische oder geschäftliche Einschränkungen die Implementierung einer geeigneten Authentifizierungsstufe verhindern, ist der Ausnahmeprozess gemäß Regelung Nr. 03.01.09 Ausnahmeprozess durchzuführen.

3. **Auswahl der entsprechenden Authentifizierungsverfahren**

Der System- oder Applikationsverantwortliche wählt das geeignete Authentifizierungsverfahren entsprechend der erforderlichen Authentifizierungsstufe aus. Eine Liste der innerh. VOLKSWAGEN Group verfügbaren und geeigneten Authentifizierungsverfahren muss zentral gepflegt werden[35].

---

[33] Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter, Kapital „3.1 Klassifizierung“

Informationssicherheitshandlungsleitlinien für Systementwickler, Kapitel „5.1 Sicherheitsanforderungen für Informationssysteme"

Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren, Kapitel „7.1 Sicherheitsanforderungen für Informationssystemen"

[34] Informationssicherheitshandlungsleitlinien für Systementwickler, Kapitel „5.1 Sicherheitsanforderungen von Informationssystemen"

Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren, Kapitel „7.1 Sicherheitsanforderungen von Informationssystemen"

[35] Die Liste steht im K-SIS intranet zur Verfügung: -link-

Wenn keine der verfügbaren Authentifizierungsmethoden oder -systeme durchführbar ist, kann der Verantwortliche entweder eine Ausnahme implementieren oder den Ausnahmegenehmigungsprozess (Regelung Nr. 03.01.09 Ausnahmeprozess) auslösen, um die Genehmigung für die Verwendung einer Methode zu erhalten, die zu einer niedrigeren Authentifizierungsebene gehört.

International anerkannte und standardisierte Authentifizierungsverfahren (z. B. 802.1x, SAML oder Kerberos) sollten überall dort verwendet werden, wo dies möglich ist. Für die Verwendung proprietärer Erweiterungen oder spezifischer Änderungen durch Hersteller ist eine Ausnahmegenehmigung (Regelung Nr. 03.01.09 Ausnahmeprozess) erforderlich.

4.7. Authentifizierungssysteme

Die zur Authentifizierung eingesetzten Systeme müssen in Abstimmung mit den zuständigen Konzernstellen[36] geplant und betrieben werden. Dies bedeutet nicht, dass ein einziges System die Authentifizierung für alle Benutzer durchführen muss. Wenn mehrere oder verteilte Systeme betrieben werden, muss sichergestellt sein, dass alle diese Systeme auf die gleiche Datenstruktur (z. B. LDAP-Schema) zugreifen und dies somit die Grundlage für ein Single-Sign-On ist.

Der Zugriff seitens Zielsystem auf das Authentifizierungs-Repository darf nur verschlüsselt und "read-only" erfolgen.

Zentrale Authentifizierungssysteme müssen redundant und hochverfügbar sein.

Authentifizierungssysteme müssen die Anforderungen für die jeweilige Authentifizierungsstufe erfüllen, für die sie verwendet werden sollen. Das Kapitel "4.4 Authentication Levels und Authenticator Assurance Levels" gibt einen Überblick über die Anforderungen. Details finden Sie in NIST SP 800-63B und in zugehörigen Dokumenten.

[36] Siehe Anhang B.4.2

5. Privileged Identity Management

Priviligierte Accounts stellen den Benutzern erweiterte Berechtigung zur Verfügung und müssen daher mit besonderer Vorsicht behandelt werden. Die nachfolgenden Anforderungen definieren höhere Sicherheitsstandards für diese Accounts.

Privilegierte Berechtigungen (Definition):

Privilegierte Berechtigungen gehen über die Berechtigungen eines Standardnutzers hinaus, ohne systemgefährdende Tätigkeiten zuzulassen.

Sie dürfen nach Beantragung zusätzlich zu den standardmäßigen Berechtigungen durch einen Administrator an einen Nutzer vergeben werden und sind nicht per se einem Konto zugeordnet.

Mit privilegierten Berechtigungen lassen sich Tätigkeiten ausführen, Daten verändern oder Informationen einsehen, die mit den Berechtigungen eines Standardnutzers nicht abrufbar wären.

Administrator/administrative Berechtigungen (Definition):

Ein Administrator ist ein Benutzer, der über zusätzlich spezielle Berechtigungen verfügt. Diese Berechtigungen stellen ihm Werkzeuge zur Verfügung, mit denen bestimmte Verwaltungsaufgaben eines IT-Systems, einer Applikation, einer Schnittstelle oder eines Betriebssystems vorgenommen werden können. Die Möglichkeiten reichen über die eines Benutzers bei der täglichen Arbeit hinaus. Die Rolle „Administrator" und die Anwendung der damit verbundenen Berechtigungen ist unabhängig von Sicherheitszonen, Netzwerksegmenten, der eingesetzten Technik und von den Netzwerk-Sites (wie z.B. Intranet oder Internet). Alle Berechtigungen, die den Administrator von einem Standardnutzer unterscheiden, sind administrative Berechtigungen (z.B. Benutzerverwaltung, Änderungen am Betriebssystem, etc.).

Um die genannten Maßnahmen umzusetzen, müssen folgende Dinge vorhanden sein:

- Prozesse zur Inventarisierung, Provisionierung und Dokumentation von Accounts,
- Prozesse zur Rollen- und Berechtigungsvergabe,
- ein zentraler, netzbasierter Authentisierungsdienst sowie
- eine Dokumentation aller operativen und funktionalen Rollen in den Geschäftsprozessen.

Für die Umsetzung der Anforderungen des Regelwerks sind gesellschaftsspezifische Prozesse und Maßnahmen[37] der verantwortlichen Fachbereiche zu beachten.Dokumentation bzw. Inventarisierung der Administratoren-Accounts und Berechtigungsprofile

5.1.1 Erfassung und Überprüfung von administrativen und privilegierten Berechtigungen

- Für jedes IT-System müssen die zugeordneten privilegierten Accounts und deren Berechtigungen detailliert erfasst werden.
- Jede Änderung an diesen Accounts ist ebenfalls zu protokollieren.

[37] Siehe Anhang B.5.3

- Die Aktualität der Accounts und Berechtigungen muss mindestens in halbjährigen Abständen überprüft werden.

5.1.2 Dokumentation von administrativen und privilegierten Berechtigungen

- Alle Accounts mit administrativen und privilegierten Berechtigungen müssen vollständig (einschließlich des zugewiesenen Berechtigungsumfangs und der einzelnen zugewiesenen Berechtigungen) erfasst und dokumentiert sein.
- Die Dokumentation muss aktuell gehalten werden.
- Für die gesamte Erfassung der Berechtigungen muss ein einheitliches Dokumentationssystem verwendet werden.

5.1.3 Berechtigungs-Management

- In jedem IT-System sind die Sessions der Accounts bei administrativen Tätigkeiten mindestens mit den systemeigenen Protokollierungsmöglichkeiten aufzuzeichnen.

5.2. Protokollierung der Administrationstätigkeiten[38]

- Tätigkeiten des Systemadministrators sind so zu protokollieren, dass die Protokolle nicht durch den Systemadministrator oder Dritte verändert werden können.
- Die Protokolle müssen durch einen Mitarbeiter ausgewertet werden, der nicht der Verursacher der Protokolleinträge ist.
- Bei der Auswertung von Audit-/Aktivitätsprotokollen sind die notwendigen Genehmigungsverfahren[39] einzuhalten.
- Zur Einsicht in personenbezogene Daten in Protokolldateien gelten die Regelungen und Betriebsvereinbarungen der jeweiligen Konzerngesellschaft.

5.3. Administratoren-Authentisierung

- Administrative Tätigkeiten sind, soweit technisch möglich, stark zu authentisieren (2-Faktor-Authentisierung mittels Wissen und Besitz)[40].
- Die Mindestanforderung für administrative Accounts mit Zugriff auf vertrauliche und geheime Daten sowie besonders geschäftsrelevante IT-Systeme (Top-Applikationen) ist eine starke Authentisierung.

5.4. Überprüfungs-Zyklus für Accounts mit administrativen bzw. privilegierten Berechtigungen

- Alle Administrator-Accounts bzw. Accounts mit privilegierten Berechtigungen müssen regelmäßig, mindestens halbjährlich in den IT-Systemen überprüft werden. Eine ggf. anschließende Bereinigung ist durchzuführen.
- Zusätzliche Anlässe für ein Review außerhalb des regulären Zyklus können z. B. Systemwechsel, Patches, Updates, Changes etc. sein.

[38] Für weitere Informationen zur Protokollierung siehe A.1.7

[39] Siehe Anhang B.5.1

[40] Siehe Anhang A 1.4

5.5. Funktionstrennung bei privilegierten Konten

- Auf auszuführende und prüfende administrative Tätigkeiten ist das Prinzip der Funktionstrennung (Segregation of duties) anzuwenden um Unvereinbarkeitskonflikte auszuschließen. D. h. die ausführende und prüfende Person müssen verschieden sein.
- Zwischen den beteiligten Personen darf kein Unterstellungsverhältnis bestehen (z. B. darf die Person, die die Anlage eines administrativen bzw. privilegierten Accounts genehmigt, den Account nicht einrichten oder Admin-Berechtigungen auf dem System besitzen). Dies gilt besonders für Tätigkeiten an IT-Systemen die für die Aufrechterhaltung der Geschäftsprozesse relevant sind.
- Operative Funktionen sind meist nicht mit kontrollierenden Funktionen vereinbar. Daher sind Zuordnungen festzulegen, zu dokumentieren und aktuell zu halten. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.
- Für vorhersehbare (Urlaub, Dienstreise, etc.) und unvorhersehbare Fälle (Krankheit, Unfall, Kündigung, etc.) des Personenausfalls muss eine Vertretungsregelung etabliert werden, welche die Fortführung der Aufgabenwahrnehmung ermöglicht.

5.6. Umgang mit integrierten Administratorkonten

5.6.1 Mindestanforderungen für Super-User-Accounts

- Für alle Super-User-Accounts gelten Mindestanforderungen hinsichtlich der Sicherheit, welche über die der Accounts mit administrativen bzw. privilegierten Berechtigungen noch hinausgehen[41].
- Alle in IT-Systemen vorhandenen sogenannten Default-, Installations-, System- oder Service-Accounts dürfen keiner Person zugewiesen (personalisiert) werden und müssen sofort nach Installation entweder gelöscht, deaktiviert oder durch Passwörter, die der aktuellen Passwortrichtlinie[42] entsprechen, geschützt werden.

5.7. Umgang mit Notfallnutzerkonten mit administrativen bzw. privilegierten Berechtigungen

Vor dem Einrichten eines Notfalluseraccounts in einem IT-System ist in einem Prozessdokument[43] schriftlich mindestens zu definieren,

- was ein Notfall ist,
- wer wann den Notfalluseraccount verwenden/aktivieren darf,
- wie das (Einmal-)Passwort eingerichtet (Länge, Komplexität) wird und
- wie es sicher (z. B. versiegeltes Passwort im Umschlag im Tresor) unter Verschluss zu halten ist

[41] Siehe Anhang A.1.4

[42] Siehe Anhang A.1.4

[43] Siehe Anhang B.5.3

- wie der Einsatz und die Aktivitäten des Accounts zu protokollieren und zu dokumentieren sind.
- Nach dem Einsatz ist der Notfalluser-Account umgehend wieder zu deaktivieren.

II. Verantwortlichkeiten

II.I Kapitel 1: Access- und Identity-Management

Diese Regelung ist von allen Planern, Entwicklern und Betreibern von Komponenten im Zusammenhang mit einem Access- und Identity-Management anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.II Kapitel 2: Identitätsmanagement (Identitätsmanagement)

Diese Regelung ist von allen Planern, Entwicklern und Betreibern von Komponenten im Zusammenhang mit Identitätsmanagement anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.III Kapitel 3: Access Management (Berechtigungsmanagement)

Diese Regelung ist von allen Planern, Entwicklern und Betreibern von Komponenten im Zusammenhang mit Access Management anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.IV Kapitel 4: Authentifizierung

Diese Regelung ist von allen Stellen, die Authentisierungs- oder Autorisierungsmechanismen oder Anwendungen bereitstellen, anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.V Kapitel 5: Privileged Identity Management

Diese Regelung ist von allen Stellen, die Authentisierungs- oder Autorisierungsmechanismen oder Anwendungen bereitstellen, sowie von allen Stellen die priviligierte Berechtigungen vergeben, anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Führungskräfte

A.1.3 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.4 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.1.5 Handbuch für Systemarbeit 706 Namenskonventionen für Plattform-übergreifende Schlüssel

A.1.6 AIS Glossar https://volkswagen-wiki.wob.vw.vwg/wikis/display/aim/AIS+Glossary

A.1.7 Informationssicherheit Regelung Nr. 03.01.04 Sicherheitsprotokollierung und –monitoring

A.1.8 Anlage 2 zu 03.01.05 Authentifizierung und IAM

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA
Access control policy	3, 4	A.9.1.1	A.11.1.1	
User registration and de-registration	2.4.1, 2.4.2, 2.4.3,	A.9.2.1	A.11.2.1, A.11.5.2	11.1, 11.9
Privilege management	5	A.9.2.3	A.11.2.2	11.2
Review of user access rights	3.3.5	A.9.2.5	A.11.2.4	-
Administrator and operator logs	5.2	A.12.4.3	A.10.10.4	10.16

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.4 Abkürzungen und Definitionen

Siehe A.1.6 AIS Glossar

A.5 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 01.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[44].

A.6 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht
1.1	Andreas Walter	B/FP	01.10.2020	Anpassung A.1 Mitgeltende Unterlagen

[44] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Access- und Identity-Management

B.1.1 IT-Architektur

B.1.2 IT-Architektur

B.1.3 Gemäß KSU (Klassifizierung für Unterlagen)

B.2 Kapitel 2: Identitätsmanagement

B.2.1 Der Verbund besteht derzeit aus folgenden Datenbereichen:

- VW-VCD - Volkswagen AG
- FSAG-VCD – Financial Services AG
- Skoda-VCD – Skoda
- Audi-VCD (ZEBRA) – Audi AG

B.2.2 Für den Gesamtverbund: K-SIS-O/3 Bei AUDI: IT-Architektur (fachlich), Webcenter Services (betrieblich)

B.2.3 User Management

B.2.4 Zukünftig soll das SERA-System durch den B2B-Identity Prozess ersetzt werden. Dieser befindet sich zum Zeitpunkt der Erstellung dieser Richtlinie in der Pilotierung. Im B2B-Identity Prozess wird die Pflege der Stammdaten von Partnerfirmenmitarbeitern an die Partnerfirma verlagert. Die Einsatztätigkeit bei einer Gesellschaft des Konzerns muss durch einen internen Paten bestätigt werden.

B.2.5 IT

B.2.6 Webcenter Services über IAM-Service-Antrag

B.2.7 Webcenter Services über IAM-Service-Antrag

B.3 Kapitel 3: Access Management

B.3.1 IT in Abstimmung mit AIS in K-SIS-O/3

B.3.2 IT

B.3.3 Rezertifizierungsprozesse sind mit IT abzustimmen

B.3.4 Für die Sperr- und Löschintervalle gelten die Vorgaben des Handbuchs für Systemarbeit

B.4 Kapitel 4: Authentisierung und Autorisierung

B.4.1 IT-Sicherheit

B.4.2 IT-Sicherheit

B.4.3 Abstimmung mit CISO, DPO und Rechtsservice erfoderlich

B.4.4 Für Systeme die die Anforderungen nicht erfüllen können gelten die nachfolgenden Vorgaben:

Das Passwort muss aus mindestens 8 Zeichen bestehen und mindestens 3 der folgenden 4 Zeichenarten enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

- Insbesondere sind keine trivialen Passwörter zulässig (z.B. „Test1234“) oder Passwörter mit persönlichem Bezug (z. B. Namen, Geburtsdatum).

- Das Passwort ist bei der ersten Verwendung zu ändern sowie spätestens nach 90 Tagen (Letzteres gilt nur für Passwörter).

- Erfordern bestimmte Systeme oder Anwendungen komplexere Passwörter dann sind diese Vorgaben zu erfüllen.

B.4.5 Nach Erreichen einer bestimmten Anzahl an Fehlversuchen muss eine wirksame Maßnahme umgesetzt werden, um einen Brutforce Angriff zu unterbinden. Die in dieser Anforderung dargestellten Maßnahmen sind als Beispiele zu verstehen. Bei der Sperrung des Accounts muss die Möglichkeit eines Denial of Service Angriffs abgewogen werden.

B.5 Kapitel 5: Privileged Identity Management

B.5.1 Bei der Auswertung von Audit-/Aktivitätsprotokollen sind die Vorgaben des Rechtsservice zu beachten.

B.5.2 Keine weiteren Details

B.5.3 Keine weiteren Details