Security requirement

IAM

Deutsche Telekom Group

Version	47 (internal)
Date	Jun 13, 2024
Status	In work

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	3.69	Security requirement
Version	**State**	**Status**
47 (internal)	Jun 13, 2024	In work
Contact	**Validity**	**Released by**
Telekom Security psa.telekom.de		

Summary
An Identity and Access Management (IAM) framework ensures central management of identities and access rights for different systems and applications. Authentication and authorization of users are central functions of the IAM framework. The IAM framework continues to address the management of user data associated with individuals. The identity is a collection of personal attributes that the person who uses this identity individualizes. IAM is a generic term for all processes and applications that are responsible for administering identities and managing access rights to various applications, systems, and resources. In order to ensure a simple and centrally administrable solution, special IAM architectures are used, which consist of several software components.

Copyright © 2024 by Deutsche Telekom AG.
All rights reserved.

Table of Contents

1.	Introduction	4
1.1.	General Introduction	4
1.2.	Scope	4
1.3.	Definition IAM Framework	5
1.4.	Glossary	5
1.5.	Notes	7
2.	IAM Framework	8
2.1.	System	8
3.	Identity Management	11
3.1.	Identity Lifecycle Management	11
3.2.	Access Governance	13
3.3.	Identity Data Integration	18
3.4.	Accounts	19
3.5.	credentials	22
4.	Access management	24
4.1.	Authentication	24
4.2.	Authorization	25
4.3.	Privileged Account Management	26
5.	Processes and workflows	28
5.1.	General specifications for processes and workflows	28
5.2.	Joiner Process	28
5.3.	Mover Process	30
5.4.	Leaver Process	31
5.5.	Reconciliation Process	33
5.6.	Orphan Account Discovery Process	34
5.7.	Recertification Process	35
5.8.	Account usage review Process	37
5.9.	Approval Workflow	37
5.10.	Self Service-Workflow	38
5.11.	Provisioning of authentication and authorization instances	39
6.	Connection of target applications	41
6.1.	Requirements for target applications	41

1. Introduction

1.1. General Introduction

This document was created on the basis of the requirements of the Group Security Policy and the downstream Group Policy for the management of identities, roles and authorizations and covers all aspects of an IAM Framework. The security requirement serves, among other things, as the basis of the subordinate IAM security requirements, which are used for release in the PSA process. It also serves as an implementation recommendation for the requirements of the Group Security Policy in units that do not participate in the PSA process.

The following are the IAM security requirements, which focus specifically on individual aspects of an IAM framework:

- Internal IAM
  - Requirements for an IAM Framework for Internal Employees and External Workers
  - Mandatory requirements: 01 – 70
- Private Customer IAM
  - Requirements for an IAM Framework for Private Customers
  - Mandatory requirements: 01 – 11, 14 – 17, 19 – 23, 25 – 27, 29 – 35, 40 – 42, 51, 52, 54 – 58
- Business Customer IAM
  - Requirements for an IAM Framework for Business Customers
  - Mandatory requirements: 01 - 70
- Connected target applications
  - Requirements for IT/NT systems that connect to an IAM framework
  - Mandatory requirements: 12 – 18, 20, 27, 28, 71 – 75
- Non-connected target applications:
  - Requirements for IT/NT systems that do not connect to an IAM framework
  - Mandatory requirements: 01 - 75

Furthermore, some terms are used in the document, which are defined as follows and should be observed accordingly:

- The term**IT/NT systems**generally refers to all IT and NT systems of an organization. If the NT systems in particular are unable to implement requirements due to a lack of technical prerequisites, the scope is reduced according to the respective requirement.
- The term**organization**is used in this document as a synonym for the following terms (the list is not exhaustive):
  - Group
  - Enterprise
  - Group/Corporate Unit
  - Agency
- For the definition of the term**target application**see glossary

When implementing the security requirement, the priority national, international and supranational law must be observed. If compliance with the described requirements cannot be implemented or can only be implemented to a limited extent in individual cases, a risk assessment must be carried out together with a security and/or data protection expert (in accordance with the relevant requirement) and possible alternative protective measures must be coordinated.

If compliance with or implementation of the defined requirements cannot be implemented or can only be implemented to a limited extent in individual cases, a risk assessment must be carried out together with a responsible IAM Enterprise Architect (according to the affected organizational unit) and security and/or data protection experts (in accordance with the affected requirement) and possible alternative protective measures must be coordinated.

1.2. Scope

Scope of validity
The security requirement applies worldwide to all Group units in the Deutsche Telekom Group, after resolution and entry into force by the responsible for the respective company (Management Board and/or Board of Management).

Local adaptation
When implementing this safety guideline in the Group companies, the respective priority national and supranational law and the respective cultural practices as well as existing participation rights of the responsible or legitimate employee representative bodies must be observed.

Review of this Group Policy
This security policy is reviewed annually for changes.

1.3. Definition IAM Framework

The term IAM Framework refers to the coordinated interaction of all components involved in Identity and Access Management (IAM). For IAM systems within Deutsche Telekom AG, a basic distinction is made between internal and external IAM frameworks. This distinction is based on the identities or accounts that are managed in the respective IAM Framework:

- **Internal IAM**: Identities and accounts of an organization's employees
- **External IAM**: Customer identities and accounts. Outside of Deutsche Telekom AG, the term Customer IAM is also used here.

The components do not necessarily have to be provided by a software manufacturer. Rather, standardized interfaces between components from different manufacturers are used for the purpose of interaction. In addition, processes are also part of an IAM framework.

1.4. Glossary

Access Authorizations (Entitlements)
In the sense of the PSA process, access authorizations are collectively referred to as Physical access authorizations, data usage control and data access control in an IAM framework.

Account
Account of a user for a service offer in a computer network: usually the account consists of a user name and an associated password; Synonyms: user, user ID, identifier, user account, account.

A distinction is made between normal, critical and privileged as well as shadow accounts:

- Normal account: Is an account provided with the necessary entitlements to complete the tasks
- Critical account: A critical account is an account that has critical access permissions within an IT/NT system. This criticality is derived from data privacy and information security criteria and is given at least if access to the following data is possible
    - sensitive / critical data (SCD) from the point of view of the organization
    - Personal data according to EU-GDPR
- Privileged account: A privileged account is an account that has extended access permissions within an IT/NT system, e.g. for administrative purposes
- Shadow accounts: Account that exists in the system in the course of a faulty workflow, but is not correctly correlated to the appropriate identity

Authentication and Authorization Instance / (Central) Access Layer
An authentication and authorization instance is also known as a (Central) Access Layer. This instance provides services that are consumed by target applications that connect to an IAM Framework. Furthermore, it ensures strong authentication and security monitoring.

Corporate ID (CID)
Group-wide unique identifier of an identity.

Data Usage Control
Data usage control prevents the use of a data processing system by unauthorized persons. While physical access authorization prevents physical access, data usage control prevents the use of the system.

Data Access Control
Data Access control ensures that only authorized persons have access to personal data, programs, and documents. The authorization results from the assignment of tasks and the organization of the company. Important: The supervisor of an authorized employee does not automatically have access authorization. An unauthorized reading, copying, modification or deletion of personal data during their processing, use or storage should be expressly prevented.

Diameter
An authentication, authorization, and accounting protocol (triple-A system) for authenticating communication partners on a network.

Entity
An entity can be a physical or legal person, an organization, an active or passive item, a device, software, a service, etc., or a group of these entities.

Identity and Access Management (IAM)
IAM is a generic term for all processes and applications that are responsible for administering identities and managing access rights to various target applications, systems, and resources.

IAM Framework Internally
An IAM framework that only manages identities and associated accounts used within an organization (employees, external workers, service accounts, etc.)

IAM Framework GK (Business Customers)
An IAM framework that manages identities and associated accounts that originate outside the organization (business customers)

IAM Framework PK (Private Customers)
An IAM framework that manages identities and associated accounts that originate outside the organization (private customers)

Identity
The digital image of an entity that can be uniquely identified by appropriate attributes.

Kerberos
A distributed authentication service (network protocol) for open and insecure computer networks

LDAPS
Network protocol for querying and modifying information from distributed directory services over encrypted communication links

OAuth2
Standardized, secure API authorization for desktop, web, and mobile applications

OpenID Connect (OIDC)
Decentralized authentication system for web-based services

Password (Passphrase, PIN)
A password is a string of characters that is used for authentication. This is intended to prove the identity of a person or instance and consequently the access authorization to a resource.

Physical access authorization
Physical access authorization defines measures which prevent unauthorized persons from gaining physical access to data processing systems. In the broadest sense, this includes computers of all kinds – servers, PCs, laptops, smartphones, copiers, and other devices which
are suitable for the processing of personal data. Unauthorized persons are all those who do not need to be present at the respective devices based on the tasks assigned to them.

Process

A process is the sequence of different, individual activities. The aim is to achieve a predetermined goal. Belonging to the process and organization of a company, processes can also be part of another process.

Recertification Process

Verification of the accounts and the associated access permissions by the data owner, who can then continue to approve (recertify) or reject them as part of the process. In the latter case, access permissions are revoked and accounts are deleted if necessary.
Based on the recommendations of the GDPR and the BSI, recertification is already required by law in the IAM environment. How implementing a recertification process can protect a company from security breaches and possible fines.

Reconciliation Process

Reconciliation refers to the process of checking consistency and compatibility across different access layers (e.g. Active Directory, different LDAP servers, etc.). In an IAM Framework, the process is related to provisioning and synchronizing accounts into the different access layers.

Security Assertion Markup Language (SAML)

An XML framework for exchanging authentication and authorization information

System for Cross-domain Identity Management (SCIM)

Standard for automated exchange of identities and related information between different IAM or IT/NT systems

Source Application

Source applications in the sense of the IAM Framework are, for example, HR systems that provide the data for the identities.

Target application, connected

Connected target applications in the sense of the IAM Framework are IT/NT systems and services that can be connected to an IAM Framework in two stages:

- Stage 1: Use of the lifecycle management processes for identities and accounts as well as the authentication instance provided by the IAM Framework
- Stage 2: In addition to the services in the 1st level, the management of the access permissions of the IAM Framework is also used by the application

Target application, non-connected

Non-connected target applications within the meaning of the IAM Framework are IT/NT systems and services that are not connected to an IAM Framework and therefore do not use its services. As a result, the non-connected target applications are classified like an IAM Framework in the respective context (internal, PK, GK) and corresponding security requirements are made.

WebAuthN

WebAuthN allows users to be authenticated without a password. It is a W3C standard based on public key procedures and the use of factors such as biometric features, hardware tokens or smartphones.

Workflow

A workflow is a process that is structured from various processes and activities. The workflow considers the operational level.

1.5. Notes

This document provides the general requirements basis for the secure implementation and operation of an IAM Framework. It is used to derive the security requirements for individual aspects of an IAM Framework as described in Chapter 1.1. The requirements listed in this document are thematically subdivided to ensure a structured overview.

2. IAM Framework

2.1. System

Req 1	A login to the systems of an IAM Framework for operational reasons must be done with a Multi Factor Authentication (MFA).

An IAM framework is one of the most important central IT/NT systems, which has a very high protection requirement and therefore requires special security measures. This high level of protection, combined with the fact that 80% of all successful attacks are based on a password attack, means that multi-factor authentication must be used for all logins to IAM Framework IT/NT systems for operational reasons. This requirement extends the basic technical protection requirement to the effect that an IAM Framework must use an MFA for all accounts and not only for privileged (e.g. administrative) accounts as part of the login for operational reasons. The following is a non-exhaustive list of factors that are not defined as part of a safe MFA:

- Using an Organization's Managed Client
- An IP or MAC address of a client in the organization

This requirement is an extension of the Req. 14 ("User accounts must be protected with at least one authentication attribute.") from the document "3.01 Technical Baseline Security for IT/NT Systems ".

Motivation: Reduction of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-1/i47

Req 2	All IT systems of the IAM Framework must be protected with state-of-the-art endpoint protection.

Malware protection, which is mainly based on signature detection, does not provide sufficient protection for the IT systems of an IAM framework that exercises direct control over an organization's identities. Professional attackers use state-of-the-art malware whose signatures are not known. As a rule, several months pass before such an attack is detected and the signatures of the malware used are available for signature-based protection mechanisms. For this reason, all IT systems of the IAM Framework must be operated with modern endpoint protection.
Examples of features of modern endpoint protection include the following:

- Behaviour Monitoring
- Memory Scanning
- Network Monitoring
- Detect fileless and in-memory attacks
- Heuristic Detection
- Emulation/Sandboxing
- AV Scanner

This requirement is an extension of the Req. 23 ("Security software must be kept up to date at all times") from document "3.61 Operations".

Implementation example: Implementation according to the handout of the IT Security Association Germany under https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

Motivation: Reduction of the attack surface and detection as well as early prevention of attacks

Implementation example: Realizing with the Guidelines from the IT Security Association (Bundesverbandes IT Sicherheit e.V.) from https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-2/i47

Req 3	The IT/NT systems of the IAM Framework must be designed and operated in a highly available manner.

An IAM Framework must be able to perform ad hoc actions at any time according to a defined service level, such as immediately disabling accounts in the event of an ongoing attack. In addition, the IAM Framework must be reliably available in the event of both failures and peak loads. For these reasons, the systems of the IAM Framework must be designed and operated in a highly available manner.

Motivation: Ensuring the availability of the IAM framework.

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.69-3/i47

Req 4	The IAM Framework must audit-proof log all operations without exceptions.

The term tamper-proof refers to electronic archiving systems which are in line with the requirements of the German Commercial Code (§ 239, § 257 Handelsgesetzbuches – HGB), the German Fiscal Code (§ 146, § 147 Abgabenordnung – AO), the Principles of Proper Accounting and Storage of Accounts, Recordings, and Documents in Electronic Form and Data Access (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff – GoBD), and other legal stipulations. The essential security requirements are:

- The contents are saved unchanged (original) and in a forgery-proof manner.
- The contents can be found again using a search.
- All actions in the archive are logged for reasons of traceability.

Motivation: After a (successful) attack, it is important to find out afterwards through forensic investigations how the attackers proceeded. Any weak points can be identified and mitigated

For this requirement the following threats are relevant:
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-4/i47

Req 5	An emergency account must be created locally in the IAM Framework in order to access the IAM Framework in the event of a failure of the authentication instance.

To maintain the business operations of the organization, the IAM Framework must enable the login to the IAM Framework locally with an emergency account, bypassing the authentication instance of the IAM Framework. This emergency account must have far-reaching authorizations and must be protected from unauthorized access in the best possible way, for example using very long passwords, and may only be used in the 4-eye principle. The use of this emergency account is subject to the requirements of a Business Continuity Management Plan.

One possible implementation is the use of a password in a vault or the use of a Privilege Access Management (PAM) solution. Both solutions in connection with organizational processes. Prohibited solutions are password management systems that are not approved for the management of privileged accounts, as well as documents such as Excel worksheets, text files, etc.

Motivation: This emergency account should make it possible to access the data of the IAM Framework even in the event of a crisis and to be able to carry out any further steps within the framework of business continuity management. This is intended to reduce or avoid further damage to the organization.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-5/i47

Req 6	The IAM Framework must be connected to a Security Incident and Event Management System (SIEM).

Effective IT security always includes the detection of attacks and misuse of the organization's IT/NT systems. For this reason, Security Incident and Event Management Systems (SIEM) are being established to ensure or significantly improve this detection and to be able to process corresponding security incidents. The detection of misuse of accounts is of immense importance here. In an Active Directory, this monitoring can be implemented, for example, by Microsoft Defender for Identity or similar products that forward corresponding incidents to a central SIEM. For this reason, an IAM Framework must be connected to a SIEM of the organization. For attack and abuse detection, suitable use cases must be defined and implemented on the basis of the log data of the IAM Framework.

Motivation: Significant improvement in the detection of attacks and abuses in order to prevent them as early as possible and thus protect the identities and associated accounts of the organization.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-6/i47

3. Identity Management

3.1. Identity Lifecycle Management

Req 7	Only standardized identity types must be used.

All identity types used in IAM Framework must be standardized in accordance with Deutsche Telekom AG's IAM Governance Group Policy, as the processes of the IAM Framework are based on them. An attacker who brings their own identity type into the IAM Framework could bypass monitoring and detection measures. For this reason, only shared and standardized identity types may be used in the organization, such as:

- Human or natural identities
- Robot Identities
- Legal identities
- System components (e.g. hardware, applications)
- IT/NT objects (e.g. IoT devices)

Motivation: Increasing security through standardization

For this requirement the following threats are relevant:
- Unauthorized use of services or resources

ID: 3.69-7/i47

Req 8	If private e-mail addresses are used in IT/NT systems, they must be verified before use.

Attackers try in various ways to obtain valid accounts that allow them access to IT/NT systems and the data they contain. One way is the unchecked use of private e-mail addresses, for example when hiring new employees or when creating user accounts, for example in the Private Customer area. Furthermore, an insufficiently verified e-mail address can also be used for unauthorized exfiltration of data, for example if the HR department sends an employee's employment reference to a private e-mail address.

For these reasons, private email addresses must be sufficiently verified before they are used to prove that the person providing the private email address also has full control of that email address.

The necessary verification depends on the information that is sent to this email address. According to the data protection and security recommendations of Deutsche Telekom AG, a verification of a private e-mail address must be carried out at least when using the protection class INTERN. For other organizations outside Deutsche Telekom AG, the regulations applicable there must be observed in a binding manner.

Motivation: Protection of the organization's data

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-8/i47

Req 9	Only sufficiently verified identities may be used in the IAM Framework.

If an attacker succeeds in creating a new identity in the IAM Framework or can gain access to the organization's buildings and IT/NT systems using a false identity, the organization's IT/NT systems are at risk. For this reason, only identities that have previously been verified by a suitable process may be used or created in the IAM Framework.

Internal IAM: With regard to the verification of employees, it is appropriate to validate the identity and professional ref-

erence, especially for persons with security-related tasks and responsibilities (e.g. system administrators, security officers or security guards). The respective examination modality and the result must be documented.

In addition to the IT security requirements, a mandatory verification of identities for the organization results from Regulation (EU) No. 910/2014, Article 26 (requirements for advanced electronic signatures – must be clearly assigned to the signatory and must be able to identify him).
For the unambiguous determination of the identity, the following verification methods are permitted:

- Automatic verification may only be carried out with certified video identification procedures and official photo ID cards.
- Personal verification can be done in two ways:
    - In a video call, the employee in charge of the inspection must check the security features of the official photo ID shown and ensure that the person complies with the entry on the official photo ID. A very high quality of the video call must be guaranteed
    - In a personal interview, the employee in charge of the inspection must check the security features of the presented official photo ID and ensure that the person complies with the entry on the official photo ID

The organization must ensure that the employees who conduct these audits successfully complete training to identify the security features and perform the verification process. Appropriate documentation must be kept and presented during appropriate audits, TÜV tests, etc.

Due to the eIDAS requirements and ETSI guidelines for the issuance of signature and email encryption certificates for employees, the underlying identities must be verified and validated. For this reason, it must be ensured that a video identification procedure to be used is certified by the Bundesnetzagentur (BNetzA).

Identity verification can be performed in an authoritative source upstream of the IAM Framework (such as an HR system) or in the IAM Framework itself.

External IAM: Especially in the Private Customer environment, many processes are based on the registration of an identity by the customer as part of a self-service workflow. For this reason, the necessary verification of an identity must be based on the information to which the customer will gain access and on legal requirements. In doing so, Group units of Deutsche Telekom AG must comply with the requirements of the Group's data protection and security recommendations. For other organizations outside Deutsche Telekom AG, the regulations applicable there must be observed in a binding manner.

Motivation: Increase IT security and reduce the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.69-9/i47

Req 10	Persons and IT/NT objects must be clearly and verifiably mapped as digital identities.

Persons and IT/NT objects must be clearly and verifiably mapped as digital identities. To do this, they must be provided with a unique and unchangeable identifier throughout the organization. Within Deutsche Telekom AG, this is the Corporate ID (CID). This process is carried out according to uniform rules.

The aim is to assign a single digital identity per identity type that applies to all organizational units. Identities must be adequately protected against misuse and theft.

In the context of an IAM framework, the subject is defined as human beings that are related to the organization. Examples include internal or external employees. Objects refer to technical devices such as a laptop or a mobile device.

To make it more difficult for attackers to take over identities, each entity must be assigned its unique identity in the organization that is part of Identity Lifecycle Management. This uniqueness must also be given, for example, with the same first name, surname and date of birth of several subjects.

The following boundaries apply:

- Internal IAM frameworks or non-connected target applications
    - No personal data from the personnel master data may be used for the unique and unchangeable identifier.
    - Personnel numbers may not be used as a unique and unchangeable identifier, as they represent a personal data and thus it is possible to draw conclusions about the identity.
- PK or GK IAM Frameworks
    - No personal data from the customer master data may be used for the unique and unchangeable identifier.

Motivation: By standardizing, increasing security and assigning identities, which facilitates, for example, forensic investigation in the aftermath of an incident.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.69-10/i47

Req 11	The relationship between identity and account must be precisely defined.

The assignment of accounts to identities must be precisely defined and always given, otherwise attackers can succeed in taking over orphaned accounts in order to carry out attacks.

The following boundaries apply to the assignment of accounts to identities:

- Internal IAM frameworks or non-connected target applications
    - Each account is assigned to exactly one identity (1:1, Account:Identity).
    - Multiple accounts can be assigned to each identity (1:n, Identity:Account).
- PK or GK IAM Frameworks
    - An n:m assignment (identity:account) is allowed, but there must be at least a 1:1 (identity:account).
    - Standalone accounts are not allowed.

Motivation: Increasing security through standardization

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-11/i47

3.2. Access Governance

Req 12	The assignment of access rights must ensure a task-related segregation of duties.

The assigned access permissions must not remove the requirement of separation of duties between operational and controlling functions of the employees.

Entitlements must be structured in such a way that there is no mixing of roles that merge the areas of activity "operational" and "controlling". As an example of this, the employee who approves travel expenses is not allowed to process (and approve) his own travel expense report. For this reason, the assignment of access permissions must ensure a task-related segregation of duties.

Regarding target applications connected to an IAM Framework, the following regulations apply:

- Once the implementation of the Segregation of Duties principle is ensured within or through the IAM Framework, no implementation is required.
- If the principle of segregation of duties is implemented within the connected target application, an overview of the assigned entitlements must also be transmitted to the central IAM Framework

Motivation: Prevention of the possibility of abuse and fraud

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-12/i47

Req 13	Redundant access permissions of accounts, groups, and roles must be removed as part of regular checks.

In an IAM Framework, the assigned entitlements must be clearly defined and clearly assigned at all times. If the same access permissions are assigned to an account, a group, and a role, there is a risk that, for example, in a mover process, only the access permissions that are configured for the group and the role will be removed, but the access permissions for the account will be overlooked. If this account is taken over by an attacker, there is a risk that the "forgotten" access permissions will increase the extent of damage. for this reason redundant access permissions must be removed as part of regular checks.

With regard to target applications connected to an IAM Framework, the following regulations apply:

- Once the removal of redundant access permissions within or through the IAM Framework is ensured, no implementation is required.
- If the removal of redundant entitlements is implemented within the connected target application, an overview of the assigned entitlements must also be transmitted to the central IAM Framework.

Motivation: Limitation of the extent of damage in the event of a security incident

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

ID: 3.69-13/i47

Req 14	Accounts may only be able to access the data that is absolutely necessary for the completion of tasks (Need To Know principle).

If an attacker is able to take over an existing account, he has access to the data for which the account is authorized. In order to limit the extent of damage in the event of a security incident, the accounts may only access the data that is absolutely necessary and necessary for the completion of tasks by the regular account holders.

With regard to target applications connected to an IAM Framework, the following regulations apply:

- As soon as the need to know principle is ensured within or through the IAM Framework, no implementation is required.
- If the Need to Know principle is implemented within the connected target application, an overview of the assigned entitlements must also be transmitted to the central IAM Framework.

This requirement is an extension of the Req. 18 ("The permissions for users and applications must be limited to the extent necessary to fulfill their tasks ") from the document "3.01 Technical Baseline Security for IT/NT Systems".

Motivation: Limitation of the extent of damage in the event of a security incident

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.69-14/i47

Req 15	Accounts must only be able to perform the actions on the data that are absolutely necessary for the completion of tasks (Least Privilege principle).

If an account is configured so that it has full access to the data to be processed, attackers who take over the account can not only divert the data, but also change or delete it. For this reason, accounts may only perform the actions on the data that are absolutely necessary for the completion of tasks of the regular account holders.

With regard to target applications connected to an IAM Framework, the following regulations apply:

- As soon as the least privilege principle is ensured within or through the IAM Framework, no implementation is required.
- If the least privilege principle is implemented within the connected target application, reporting to the central IAM framework must also be carried out.

This requirement is an extension of the Req. 18 ("The permissions for users and applications must be limited to the extent necessary to fulfill their tasks ") from the document "3.01 Technical Baseline Security for IT/NT Systems".

Motivation: Limiting the extent of damage in the event of a security incident and ensuring the integrity of the data

For this requirement the following threats are relevant:
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-15/i47

Req 16	Access permissions must be defined atomically and separately from each other.

To enable effective and secure management of access permissions, access permissions must be atomic and delimited. Otherwise, the probability is very high that an account has too high access permissions, because a higher right, which is actually not needed, is combined with lower rights in one access authorization. For example, atomic access permissions can be grouped into roles.

With regard to target applications connected to an IAM Framework, the following regulations apply:

- As soon as atomic and delimited access permissions within or through the IAM Framework are ensured, no implementation is required.
- If atomic and delimited entitlements are implemented within the connected target application, an overview of the assigned entitlements must also be transmitted to the central IAM Framework.

Motivation: Protection of the organization's data and compliance with the need-to-know and least-privilege principle

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-16/i47

Req 17	Access permissions must have an understandable name and description.

For example, to be able to select the correct and necessary access permissions when assigning access permissions or going through a recertification process, access permissions must have a comprehensible naming and description.

With regard to target applications connected to an IAM Framework, the following regulations apply:

- As soon as the naming of access permissions within or through the IAM Framework is ensured, no implementation is required.
- If the naming of the entitlements is implemented within the connected target application, an overview of the assigned entitlements must also be transmitted to the central IAM Framework.

Motivation: Ensuring the least privilege principle

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources

ID: 3.69-17/i47

Req 18	Granting and modifying access permissions must be done using an approval workflow.

The granting of entitlements must be carried out according to the need-to-know and least-privilege principle, so that the data of the organization is protected with the highest possible level of security. To ensure this protection, the granting and modification of access permissions must be carried out in accordance with the requirements in the chapter "Approval Workflow". Otherwise, attackers could assign extensive access permissions to their created or captured account.

With regard to target applications connected to an IAM Framework, the following regulations apply:

- Once the granting and modification of access permissions within or through the IAM Framework is ensured, no implementation is required.
- If the granting and modification of entitlements is implemented within the connected target application, reporting to the central IAM Framework must also be carried out.

Motivation: Protect the organization's data and minimize the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-18/i47

Req 19	The provisioning of entitlements in connected target applications must be carried out promptly.

In the context of a lateral movement of an attacker after the successful takeover of an IT/NT system, accounts that have high or very far-reaching access rights to data and IT/NT systems are of particular interest. In order to minimize the probability of exploiting such high or far-reaching entitlements, created, changed and revoked entitlements must be provisioned promptly in connected target applications. The provisioning process must be monitored accordingly by the IAM Framework. In addition, processes must be initiated in the event of an error to ensure provisioning. The results of the provisioning runs must be logged.

The following regulations apply:

- **Push mechanism**: Immediately after granting/changing the access permissions in the IAM Framework, they must be provisioned in the connected target applications. This applies equally to internal, PK and GK IAM frameworks.
- **Pull mechanism**: Every 30 minutes, the connected target application must check for created, changed or revoked access permissions in the IAM Framework and provision them. For PK and GK IAM frameworks, this time span can be up to 6 hours. As an example of a pull mechanism, groups stored in an LDAP are used to assign entitlements within a connected target application.
- **Non-connected target applications**: For target applications that are not connected to an IAM Framework, created, modified, and revoked access permissions must be applied immediately.

Motivation: Protect the organization's data and minimize the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-19/i47

Req 20	When using token-based protocols, the tokens may only be used according to the defined standard.

In order to prevent an increase in the attack surface of token-based protocols, such as OAuth2, SAML or OpenID Connect (OIDC), the respective tokens may only be used in accordance with the respective protocol specification and must not be changed.

The following requirements for each protocol must be implemented:

- OAuth2
    - **Access Token**: an access token is used to authorize the client for a specific resource.
- OIDC
    - **ID Token (Session Token)**: The ID token is a security token that contains only information about how an end user is authenticated by an authorization server. ID tokens may not be used for further information,

such as authorization or assigned access permissions.
    - **Access Token**: an access token is used to authorize the client for a specific resource.
- SAML
    - **Authentication Assertion**: The Authentication Assertion contains information regarding the identification of the user and specifies the time of authentication and the authentication method used.
    - **Attributes Assertion**: for example the attributes assertion contains information about the roles that are assigned to the user.
    - **Authorization Assertion**: the authorization assertion specifies whether the user is allowed to use the resource or has not been allowed to use it due to incorrect authentication for example.

Motivation: Protect the organization's data, minimize the attack surface, and increase security through standardization

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-20/i47

3.3. Identity Data Integration

Req 21	When connecting source applications to an IAM Framework, both systems must authenticate each other.

Through unsecured interfaces of the IAM Framework, an attacker could be able to import spoofed identities and/or accounts into the IAM Framework. If the attacker is successful, all downstream target applications that use the corresponding accounts as well as potentially the IAM Framework itself are no longer secured and, for example, data from the target applications could be exfiltrated. For this reason source applications and the IAM Framework must authenticate each other.

Motivation: Protection of the target applications as well as the data contained therein and the IAM Framework against attackers who want to achieve their goal with self-created identities or accounts

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-21/i47

Req 22	Only authorized source applications may be connected to the IAM Framework.

Only authorized source applications are allowed to export data to the IAM Framework to ensure the integrity and authenticity of the imported data. An example is an SAP system whose data forms the basis for the identities to be managed. An authorized source application is defined as follows:
- Written documented interface agreement between the source application and the IAM Framework
- Completed PSA process of the source application with approval by security and data privacy
- Approval of IT

Motivation: To make it more difficult or prevent misuse by an attacker, only authorized source applications may export data to the IAM Framework. thus the attacker would have to compromise the source application(s) before he can intro-

duce fake identities into the IAM Framework.

For this requirement the following threats are relevant:
- Unauthorized modification of data

ID: 3.69-22/i47

Req 23	It must be ensured that an object is imported from exactly one source application.

An object of an IAM Framework must not be imported from different source applications in order to achieve a 1:1 assignment within the IAM Framework, i.e. the import of an object must be assigned exactly to a source application. However, an object may be enriched with information from other source applications as long as the traceability of the enrichment (which information comes from which source application?) is given and the information from the authoritative source from which the object itself was imported is not overwritten. It must be ensured that the attributes of an object do not override or contradict each other. Enrichment may only have a complementary character.

Motivation: To make it more difficult for an attacker to misuse compromised source applications to create unauthorized identities in the IAM Framework

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-23/i47

3.4. Accounts

Req 24	Inactive accounts must be deactivated after 35 days.

In order to prevent or detect misuse of inactive accounts by an attacker, inactive accounts must ideally be deactivated after 30 days, or 35 days at the latest.

Motivation: Minimization of the attack surface and detection of attacks.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-24/i47

Req 25	Only approved and standardized account types may be used.

Approved and standardized account types and their use facilitate the detection of attacks if, for example, an attacker uses a service account to log on to a client computer. For this reason, only approved and standardized account types may be used.
Examples of Standardized Account Types are the following:

- Privileged accounts (e.g. for administrators)
- Normal user accounts in Active Directory or in any target application
- External accounts (e.g.for third-partyservice providers or partners)
- Service accounts (service account required for applications, services, etc.)
- Robot accounts (also known as "bots"; they are used, for example, to automate routine tasks)
- Device accounts (e.g. IoT devices)

- Function accounts (e.g. reception in the building or training computer)

Motivation: Detection of attacks.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-25/i47

Req 26	Account usernames must be pseudonymized.

Attackers typically choose accounts as the target of their efforts that are helpful to them on the way to achieving their goal. This includes all privileged accounts, but also accounts that have access to certain data. Usually, they have already researched this information, such as the name of an employee of the organization responsible for transfers, in advance and are looking for this account specifically.

For this reason, the user names of accounts must be pseudonymized.

Below is a non-exhaustive list of unauthorized user names:

- Personnel numbers, for example from SAP HR systems
- A combination of surnames and first names, including the use of parts thereof or abbreviations
- In general, the use of characteristics that indicate account owner or functionality of the account

Especially in the Active Directoryfield, it is possible for every user to read the information of any account, including an attacker. However, this is only possible after you have successfully logged in, so that an pseudonymized user name protects against the scenario outlined above.

Motivation: Reduction of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-26/i47

Req 27	For privileged access to IT/NT systems, separate personal accounts must be set up and used.

The use of a central privileged account by several people means that operations cannot be clearly assigned to the executing person. Therefore, for each identity that requires privileged access permissions, an additional separate privileged (administrative) personal account must be set up and used.

This requirement is an extension of the Req. 22 ("User accounts must ensure the unique identification of the user") from the document "3.01 Technical Baseline Security for IT/NT Systems".

Motivation: The unique identification of a user is a prerequisite for assigning a user permissions that are necessary for the performance of his tasks on the system. This is the only way to achieve adequate access control to data and services and to prevent abusive access. In addition, it provides better detection of attacks on privileged accounts.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data

- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.69-27/i47

Req 28	Privilegierte Accounts müssen zentral verwaltet werden und einheitlich festgelegten Namenskonventionen entsprechen.

Motivation: Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=1

Jede Benutzerkennung muss eindeutig einem registrierten Benutzer zugeordnet werden können. Sollten Zugriffsberechtigungen vergeben werden, die über den üblichen Standard hinausgehen, muss dies begründet werden. Das kann auch in elektronischer Form erfolgen, z. B. durch ein spezielles Login, dessen Name und Passwort den einzurichtenden Benutzern bekanntgegeben wird. Dort wird ein entsprechendes Programm durchlaufen, das mit einem Logout endet. Die erfassten Daten sollten anschließend überprüft werden, z. B. durch den Vorgesetzten. Ein Passwort, das einem Benutzer für die erstmalige Systemnutzung mitgeteilt wird, muss danach gewechselt werden. Dies sollte vom System initiiert werden. Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die systemspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten. Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppennamen festzulegen (z. B. mit Benutzer-ID, Kürzel der Organisationseinheit, lfd. Nummer usw.). Die Zugriffsberechtigung für Dateien ist auf Benutzer bzw. Gruppen mit berechtigtem Interesse zu beschränken. Wenn mehrere Personen auf eine Datei zugreifen müssen, sollte für diese eine Gruppe eingerichtet werden. Jedem Benutzer muss eine eigene Benutzerkennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten. Bei Kennungen gegenüber Betriebssystemen ist für jeden Benutzer ein eindeutiges Heimatverzeichnis anzulegen.

https://link.springer.com/book/10.1007/978-3-658-10151-0

https://www.wallix.com/de/5-gruende-warum-die-ermittlung-privilegierter-konten-privileged-account-discovery-der-erste-schritt-zu-starker-cyber-sicherheit-ist/

Hallo Max,

das wäre die beste Lösung. Vielleicht kann man Eure beiden Ansätze kombinieren. Bis alle administrativen Accounts zentral gemanaged werden ist sicher ein langer Weg.

„Privilegierte Accounts müssen zentral verwaltet werden und/oder mindestens einheitlich festgelegten Namenskonventionen entsprechen“

Bis das endgültig ausformuliert sein muss ist ja auch noch etwas Zeit. Vielen Dank für Eure Unterstützung hier.

Viele Grüße,
Daniel

Von: *Wallau, Maximilian <[email]Maximilian.Wallau@telekom.de>*
Gesendet: *Freitag, 24. Mai 2024 15:17*
An: *Beck, Oliver <[email]Oliver.Beck@telekom.de>; Limbach, Daniel <[email]daniel.limbach@telekom.de>; Kluth, Martin <[email]M.Kluth@telekom.de>*
Cc: *Salgert, Thomas <[email]thomas.salgert@telekom.de>*
Betreff: *AW: Namenskonventionen für Administrative Accounts - IAM 3.69*

Hi Olli,

ist es möglich das etwas umzuformulieren? Bspw. in „Privilegierte Accounts müssen zentral gemanagt sein.“

Das würde doch eigentlich direkt implizieren, dass diese Accounts auch einheitlichen Namenskonventionen folgen, da die zentralen IAMs das so oder so machen oder?

Ich habe sonst die Befürchtung, dass ansonsten zu viele lokale Admin Accounts auf den Systemen verbleiben, die ungemanagt sind und „nur“ einer Namenskonvention folgen.

Ausnahmen für Break-Glass- und Notfall-Accounts (bspw. “root” und “Administrator”) muss es natürlich weiterhin geben.

Beste Grüße
Max

ID: 3.69-28/i47

Req 29	Active Directory-based service accounts must use Group Managed Service Accounts.

Usually, the operators of IT/NT systems manage the passwords of the service accounts used in the IT/NT system. Despite the complexity requirements for the passwords to be used, it is sometimes possible to crack them via brute force attacks.

For this reason, target applications of an IAM Framework that are connected to an Active Directory must use group Managed Service Accounts (gMSA). When using a gMSA, password management is performed automatically in Active Directory without the operators of the IT/NT system being able to influence it. This significantly minimizes the likelihood of a successful brute force attack.

Documentation regarding gMSA can be found here: https://docs.microsoft.com/de-de/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

Motivation: Prevent brute force attacks on service account passwords

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-29/i47

3.5. credentials

Req 30	No publicly known passwords must be used.

Attackers often use (purchased) password databases or rainbow tables to determine passwords, or their hashes using brute-force attacks or other techniques and use them for their attacks. for this reason, publicly known passwords must not be used in the organization.

To determine publicly known passwords, you can use services available on the internet, such as "ID Guard" from Deutsche Telekom Security GmbH for example to check the new password to see if it is publicly known when an account is changed on a regular password. When using services on the Internet, it must be ensured that only an encrypted hash of the password – and not the password itself – is transmitted.

This requirement is an extension of the Req. 26 ("If a password is used as an authentication attribute, a protection against online attacks like brute force and dictionary attacks that hinder password guessing must be implemented ") from the document "3.01 Technical Baseline Security for IT/NT Systems ".

Motivation: Reduction of security incidents and minimization of the scope for attack.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

ID: 3.69-30/i47

Req 31	If passwords are used as an authentication feature for technical accounts, they must be at least 30 characters long and contain three of the following character categories: lowercase letters, upper-case letters, numbers, and special characters.

Technical accounts, such as service accounts or robot accounts, are usually a worthwhile target for attackers because your passwords are set once and changed very rarely, if ever. This means that the longer such an account is used, the higher the probability that the associated password will be found out by an attacker.

For this reason, passwords from technical accounts must comply with a stronger password policy:

- Password length: 30 characters
- Use of 3 of 4 character classes (a-z, A-Z, 0-9, special characters)

This requirement is an extension of the Req. 22 ("If a password is used as an authentication attribute, it must have at least 12 characters and contain three of the following categories: lower-case letters, upper-case letters, digits and special characters.") from the document „3.01 Technical Baseline Security for IT/NT Systems“.

Motivation: Minimization of the scope for attack.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-31/i47

Req 32	If PGP or S/MIME certificates are used, they must be identity-related and validated.

PGP or S/MIME Email encryption and signing is based on the use of certificates from a PKI. To ensure encrypted e-mail exchange with recipients outside your own organization, certificates from a public PKI are usually used. To prevent the incorrect issuance of certificates or misuse of the certificates, these certificates must be identity-related and the identities must be validated according to the requirements of the requirement "Only sufficiently verified identities may be used in the IAM Framework".

Motivation: Prevention of misuse of certificates or incorrect issuance of certificates

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.69-32/i47

4. Access management

4.1. Authentication

Req 33	An authentication and authorization instance must only use standardized and established protocols.

Self-developed protocols are usually programmed with a focus on functionality rather than security, so they are vulnerable to attacks. For this reason, an authentication and authorization instance must use standardized and established protocols. For example, appropriate protocols for authentication and authorization are the following:

- OpenID Connect
- OAuth2
- SAML
- Kerberos
- WebAuthN
- Diameter

This requirement is an extension of the Req. 5 ("The software and hardware of the system must be covered by the supplier's security vulnerability support") from the document "3.01 Technical Baseline Security for IT/NT Systems".

Motivation: Reduction of the attack surface and associated minimization of the number of security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-33/i47

Req 34	An authentication and authorization instance must be able to log on using several different authentication methods.

Strong authentication requires that you can log in using several different authentication methods (Multi Factor Authentication, MFA). MFA is typically not as easy for attackers to circumvent as, for example, authentication with username and password alone.

For this reason, an authentication and authorization instance in an IAM Framework must enable to log in using several different authentication methods. There should be several methods to choose from, which can then be used for authentication.

The following is a non-exhaustive list of secure authentication methods or MFA factors that can be combined for secure authentication:

- Username/Passwort
- Biometric factors:
    - Fingerprint
    - Palm vein scan
    - Iris scan
    - Face recognition
- Smart cards, FIDO2 (or certificate-based authentication with an HW token)
- Certificates (incl. SSH Certificates)

- Authentication Apps on the Company Phone
- OneTime Token
    - Hardware
    - Software
    - QR Code

If the username/password authentication method is used, another authentication method, such as a smart card with PIN, must be used for authentication

Motivation: Protection of the target applications and the data contained therein

For this requirement the following threats are relevant:
- Unauthorized access to the system

ID: 3.69-34/i47

Req 35	Insecure authentication methods must not be used.

Insecure authentication methods not only allow an attacker to log on to IT/NT systems without permission, but also potentially deny access to the regular user due to their unreliability or inaccuracy. For this reason, insecure authentication methods must not be used. As an example of this, the following are mentioned:

- Behavioral token
    - Gestures
    - Keyboard stroke
    - Voice print
- Biometric token
    - Hand topography
    - Retina scan
    - Hand geometry

Motivation: Reduction of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.69-35/i47

4.2. Authorization

Req 36	Authorizing a user must be clear and reproducible.

If inconsistent states occur during the assignment of access permissions to an account in the course of authorization in such a way that increased access permissions are granted from time to time that are not required for the tasks to be performed, attackers can exploit this circumstance in a targeted manner. For this reason the authorization of a user must be clear and reproducible.

Motivation: Reduction of the attack surface and ensuring least privilege principle

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

ID: 3.69-36/i47

4.3. Privileged Account Management

Req 37	The provisioning of the PAM must be automated and carried out exclusively by the IAM Framework.

The ability to create privileged accounts must be reduced to make it more difficult for the attackers to extend their existing rights. Privileged accounts may not be created in the PAM solution itself, i.e. there must be no possibility to create privileged accounts on the fly in the PAM solution bypassing the approved process in order to use them for access to IT/NT systems. If the PAM solution operates its own identity management, all requirements for an internal IAM framework must be met. For this reason, the provisioning of far-reaching access permissions or privileged accounts must be automated and carried out exclusively by the IAM Framework.

Motivation: Reducing the attacker's ability to extend his rights

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-37/i47

Req 38	It must be possible to assign accounts and entitlements for a limited period of time or for a limited period of time.

An attacker strives to gain full control over the target of the attack. He achieves this, among other things, by taking over accounts with privileged access permissions. If you now shorten the period of time in which the privileged access permissions are available or are assigned to an account in which you set a start and an end time for the use of these access permissions, you reduce the possibilities for the attacker to obtain these access permissions. For this reason, it must be possible to assign accounts and entitlements for a limited period of time.

Motivation: Reduce the attack surface for obtaining privileged access permissions or privilege escalation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-38/i47

Req 39	If an automatic rotation of passwords is offered by the PAM solution, it must be used.

An automated change of passwords by the PAM solution makes it almost impossible for an attacker to use captured credentials. The passwords are changed after a single use by the PAM solution and stored encrypted in the password vault. In this way, not even the authorized privileged user knows the password. For this reason, the automatic rotation of passwords must be used if the PAM solution offers this.

The following requirements must be taken into account:
- Password length: 30 characters
- Use 3 of 4 character classes (a-z, A-Z, 0-9, special characters)

- A password is valid for exactly one user login

Motivation: Preventing an attacker from spying on credentials from privileged accounts and thus reducing the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-39/i47

Req 40	The allocation of privileged accounts and associated access permissions must be performed using an approval workflow.

Privileged accounts – especially the associated access permissions – are a sought-after target for attackers. Because with them it is usually possible to get access to other accounts and associated data. To prevent misuse, the privileged accounts and associated access permissions must be allocated using an approval workflow. The security requirements of the chapters "General requirements for processes and workflows" and "Approval workflow" must be met, provided that the PAM solution implements the approval workflow itself. Otherwise, you must use the approval workflow of the respective IAM Framework that provides the PAM solution.

Motivation: Reduction of the attack surface and associated protection of privileged accounts and associated access permissions. At the same time, this gives you a traceability of the use of privileged accounts in order to be able to carry out forensic investigations in case of suspicion.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-40/i47

5. Processes and workflows

5.1. General specifications for processes and workflows

Req 41	All automated process and workflow steps of an IAM framework must be monitored and corresponding errors or deviations must be alerted.

In order to ensure the availability of the IAM Framework and to detect attackers who exploit errors in the process or workflow chain, permanent monitoring of all automated process and workflow steps of an IAM Framework must be implemented. Detected errors or deviations must be alerted. Ideally, this monitoring should be implemented by a SIEM, if technically feasible.

Motivation: Increase the availability of the IAM Framework and early detection of attack attempts.

For this requirement the following threats are relevant:
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-41/i47

Req 42	All IAM Framework processes and workflows must be documented and approved.

Especially with an IAM Framework, it is important to pay attention to the security of the processes, so that it is not possible to influence the IAM Framework or to misuse the IAM Framework through organizational or procedural errors. For this reason, all processes must be documented and approved by the respective security management of the organization.

Motivation: Reduction of the possibilities for an attacker to exploit errors in the process chain for misuse. Further increase the availability of the IAM Framework, as fewer failed processes lead to fewer failures in the IAM Framework.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-42/i47

5.2. Joiner Process

Req 43	A joiner process must be established.

For an attacker, it can be advantageous if he can independently create new identities and accounts as part of his attack. These can be used, for example, for further privilege escalations or obfuscation of data exfiltration. In addition, there are legal and regulatory requirements that require certain characteristics of identities and accounts. For this reason, a joiner process must be established for new employees of an organization, which has been documented and released as part of the PSA process by Data Privacy and IT security.

This joiner process must implement the requirements of this chapter and include the following steps for an internal IAM Framework:

- Import of identities/identity data from authorized source applications
- Creation of necessary accounts, credentials, certificates, etc. through automated processes and provisioning of the same in compliance with the necessary security requirements
- Secure transmission of the necessary information to the new employee

For IAM frameworks from the Private Customer or Business Customer environment, similar processes have to be created but with different requirements. The following questions can help:

- How does the customer create his identity/account?
- With which information should the identity/account be enriched?
- How to verify your email address?
- Which identity data is necessary? How are these verified?

Non-connected target applications that are used by internal employees must meet the requirements for an internal IAM framework.

Motivation: Reduction of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-43/i47

Req 44	The activation of all accounts as well as physical and data access authorizations assigned to the new employee must take place no later than 30 days after delivery to the person responsible for the issue.

If the new employee has not activated all assigned accounts as well as physical and data access authorizations after 30 days, the accounts as well as physical and data access authorizations must be deleted or invalidated. This measure reduces the number of accounts provided, but not activated or unused, as well as physical and data access authorizations. Otherwise, these could be misused by attackers. The monitoring of the deadline must be ensured by the respective IAM Framework.

Motivation: Reduction of the possibilities for the attacker to gain unauthorized access to premises and access to IT/NT systems

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-44/i47

Req 45	By default, no critical access permissions may be set when creating accounts for new employees.

In order to avoid unnecessary or excessive access permissions and to reduce the risk of attackers using "forgotten" accounts for attacks on IT/NT systems, newly created accounts for new employees must not be configured with critical access permissions by default. This requirement applies to connected or non-connected target applications as well as to all IAM Frameworks (Internal, Private Customer, Business Customer).

Motivation: Reduce the risk that forgotten or overlooked accounts can be misused for attacks. Furthermore, the necessary access permissions are reduced to a minimum so that accounts are not accidentally equipped with too large access permissions.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-45/i47

5.3. Mover Process

Req 46	A mover process must be established.

It can be advantageous for an attacker if he can use accounts with very high or far-reaching access permissions resulting from a change of the workplace of an employee within the organization without an established mover process as part of his attack. These can be used, for example, for further privilege escalations or obfuscation of data exfiltration. For this reason, a mover process must be established for internal employees of an organization, which has been documented and released as part of the PSA process by Data Privacy and IT security. This mover process must meet the requirements of this chapter for an internal IAM framework.

Non-connected target applications that are used by internal employees must also meet the requirements of this chapter for an internal IAM framework.

Motivation: Reduction of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-46/i47

Req 47	When changing jobs within the organization, the recertification process must be carried out for the employee concerned.

If an employee within the organization changes his workplace and the entitlements as well as physical and data access authorizations that were necessary for the old task are not deleted or deactivated, an attacker, after having taken over the identity and the associated accounts, would be able to compromise significantly more IT/NT systems and, for example, exfiltrate data than with the necessary entitlements of the employee. would have been possible.

For this reason, when changing jobs within the organization, the recertification process must be carried out, the following conditions apply.:

- the process must be carried out no later than three working days after the change of workplace
- Entitlements as well as physical and data access authorizations that are no longer required must be deleted or deactivated.

The recertification process must be part of the mover process.

Motivation: Reduce the extent of damage in the event of a security incident and limit the possibilities for an attacker

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data

- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-47/i47

Req 48	If entitlements as well as physical and data access authorizations are reassigned as part of a change of workplace in the organization, these must be personally activated by the employee within 30 days.

If, after 30 days, all assigned accounts as well as means of physical and data access authorizations have not been activated by the employee when changing jobs, the accounts as well as physical and data access authorizations must be deleted or invalidated. This measure reduces the number of accounts provided, but not activated or unused, as well as physical access and data access authorizations. Otherwise, these could be misused by attackers. The monitoring of the deadline must be ensured by the respective IAM Framework.

Motivation: Reduction of the possibilities for the attacker to gain unauthorized access to premises and access to IT/NT systems

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.69-48/i47

5.4. Leaver Process

Req 49	A leaver process must be established.

It can be advantageous for an attacker to be able to use accounts with very high or far-reaching access permissions for privilege escalations or obfuscation of data exfiltration as part of his attack, which have not been at least deactivated after an employee leaves the organization.

For this reason, a leaver process must be established for departing employees of an organization, which has been documented and released as part of the PSA process by data protection and IT security. This leaver process must meet the requirements for a leaver process from this chapter for an internal IAM framework.

For IAM frameworks from the Private Customer or Business Customer environment, similar processes only have to be created with different requirements. The following questions can help:

- How does the customer deactivate/delete his identity/account?
- Should he be able to do this at all?
- How long is the retention period of the data?

Non-connected target applications that are used by internal employees must meet the requirements for an internal IAM framework.

Motivation: Reduction of the attack surface.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-49/i47

Req 50	In the event of a longer absence of the employee, entitlements as well as physical and data access authorizations must be deactivated.

If, for example, an employee is absent for a long time due to a sabbatical or parental leave as well as a foreseeable course of illness, all entitlements as well as physical and data access authorizations must be deactivated either at the beginning of a planned absence or at the time of becoming aware of an unplanned absence. Otherwise, they could be used unnoticed by attackers.

Motivation: Reduce the attack surface and prevent security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

ID: 3.69-50/i47

Req 51	If an employee leaves, all access authorizations as well as physical and data access authorizations must be returned and deactivated on the day of departure.

In order to prevent access authorizations as well as physical and data access authorizations of the departing employee from being misused beyond his or her resignation date, they must all be deactivated on the day of withdrawal.

The following conditions must be met:
- Deactivation of all accounts, access tokens and authentication factors at 23:59 (11:59 PM) of the exit date (Valid is the time zone in which the employee was employed)
- Return of all physical authentication factors and access tokens at the latest when leaving the workplace for the last time
- Private keys for encryption must be kept secure for 6 months so that encrypted documents can be recovered.

Motivation: Reduce the attack surface and avoid security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-51/i47

Req 52	After an employee leaves the organization, all accounts assigned to him must be deprovisioned after 30 days at the latest.

All accounts of a retired employee must be deprovisioned from the target applications as well as the authentication and authorization instances after 30 days at the latest. Otherwise, they can be used by an attacker (after activation) to gain unauthorized access to protected data, for example. Care must be taken to only deprovision the accounts, but

not to delete them in the IAM Framework.

Motivation: Reduce the attack surface and avoid security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-52/i47

Req 53	An emergency leaver process must be established.

In order to immediately avert damage to the organization, for example by using compromised accounts for the data exfiltration during an attack, it must be possible to deactivate accounts and/or identities immediately, i.e. within a maximum of 5 minutes after detection and confirmation of the attack, so that no further damage can be caused. For this reason, an Emergency Leaver process must be defined.

Motivation: Reduction of the extent of damage in the event of security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-53/i47

Req 54	If an active directory is used the e-mail address and user principal name (UPN) of the retired employee must be blocked for at least 6 months before they can be reused.

To ensure access to data of a retired employee, the e-mail address assigned to him and the UPN are required. For this reason, the e-mail address and UPN of the departed employee must be blocked for at least 6 months before they can be used again.

Motivation: Ensuring access to required data.

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.69-54/i47

5.5. Reconciliation Process

Req 55	A reconciliation process must be established.

Reconciliation refers to the process of checking consistency and compatibility across different access layers (e.g. Active Directory, different LDAP servers, etc.). In an IAM Framework, the process is related to provisioning and synchronizing accounts into the different access layers. In particular, duplicate accounts of the same identity pose a high risk of non-transparent access permissions.

For this reason, a reconciliation process must be established that examines the IAM Framework and runs regularly.

If the IT/NT system is a non-connected target application, a corresponding report on the implementation of the reconciliation process including the results must be created and made available.

Motivation: Prevention of security incidents such as data exfiltration, lateral movement, privilege escalation.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-55/i47

5.6. Orphan Account Discovery Process

Req 56	A process must be established to identify orphaned accounts.

Orphaned accounts are not used by any identity for a login and are usually not monitored, i.e. they are not associated with an identity. Attackers usually use these "forgotten" accounts to log in to target applications without permission and, for example, to exfiltrate data there. For this reason, a process must be established that examines the IAM Framework for orphaned accounts and runs regularly. In general, such a process is part of the reconciliation process.

If the IT/NT system is a non-connected target application, a corresponding report must be created and made available regarding the execution of the process for determining orphaned accounts, including the results.

Motivation: Prevention of security incidents such as data exfiltration, lateral movement, privilege escalation.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-56/i47

Req 57	Orphaned accounts must be deactivated and a responsible body alerted within 5 working days of becoming aware of them at the latest.

Any orphaned account identified as part of the reconciliation process can be assumed to potentially be used for an attack. For this reason, each identified orphaned account must be deactivated without delay, within 5 working days after becoming aware of it, and a responsible body must be alerted.

Motivation: Prevention of security incidents such as data exfiltration, lateral movement, privilege escalation.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-57/i47

Req 58	The process for detecting orphaned accounts must be completed every 30 days at the latest.

The earlier an abandoned account is identified, the lower the probability that it has been used, is currently being used or will be used in future for an attack. Therefore, the process for detecting orphaned accounts must be carried out every 30 days.

Motivation: Detect potential attacks and reduce the attack surface.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-58/i47

Req 59	If orphan accounts have been discovered, it must be investigated whether they were used for registration..

Identified orphaned accounts may have been misused in the past for attacks that were not detected by other detection measures. For this reason, each orphaned account identified must be determined whether it has been used for an attack or is currently being misused for ongoing attacks.

Motivation: Detect potentially ongoing attacks and improve the detection of attacks and mitigate any vulnerabilities that have been used for an attack.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-59/i47

5.7. Recertification Process

Req 60	A recertification process must be established.

In practice, it can happen that an account is assigned unneeded access permissions. This can be done, for example, by incorrectly defined mover processes or by assigning access permissions outside the defined processes. For this reason, a recertification process must be established that is performed for all accounts without exception and meets the following requirements in this chapter.

Motivation: Reduce the extent of damage in the event of an attack and ensure the integrity of the data in the target applications.

For this requirement the following threats are relevant:

- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-60/i47

Req 61	The recertification process must be carried out regularly.

The sooner elevated or incorrect access permissions are detected in an IAM Framework, the less likely it is that attackers or employees will be able to view or modify data for which they are not normally authorized. For this reason, the recertification process must be carried out every 12 months at the latest. Depending on the criticality of the target application or the data contained therein, shorter distances should be selected for this period.

For non-connected target applications, the recertification process must be carried out every 3 months at the latest. A corresponding report regarding the implementation of the recertification process, including the results, must be prepared and made available.

Target Applications	Cycle
Target application connected to a central, internal IAM	1 time a year / every 12 months
Applications with Internal Control System - Relevance (ICS IT) or TOP66 applications	2 times a year / every 6 months
Target applications that are not connected to a central, internal IAM	4 times a year / every 3 months

Motivation: Reduce the extent of damage in the event of an attack and ensure the integrity of the data in the target applications.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-61/i47

Req 62	Unneeded entitlements must be removed within 5 working days of becoming aware of it at the latest.

Unnecessary entitlements are a violation of the least privilege principle and can be misused for data exfiltration as part of an attack. For this reason, unnecessary entitlements must be removed as part of the recertification process without delay, at the latest within 5 working days after becoming aware of it, in order to minimize the likelihood of misuse of these increased entitlements. Start time for the deadline is the completed recertification process.

Motivation: Reduce the extent of damage in the event of an attack and ensure the integrity of the data in the target applications.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data

- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-62/i47

Req 63	The recertification process must be established in the mover process.

The sooner elevated or incorrect access permissions are detected in an IAM Framework, the less likely it is that attackers or employees will be able to view or modify data for which they are not normally authorized. For this reason, the recertification process in the mover process must be established in such a way that when an employee changes, the recertification process is carried out on a case-by-case basis.

Motivation: Reduce the extent of damage in the event of an attack and ensure the integrity of the data in the target applications.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-63/i47

5.8. Account usage review Process

Req 64	An account usage review process must be established.

If, for example, an employee leaves the organization, the accounts directly assigned to his identity must be deprovisioned. For this reason, it must be ensured at all times that there is an overview showing in which IT/NT system the respective account is used, so that it is possible to deprovision the respective account.

Motivation: Preventing the outflow of data and preventing the takeover of orphaned accounts.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-64/i47

5.9. Approval Workflow

Req 65	An approval workflow must be established.

In an IAM Framework, entitlements are typically granted or denied on request in an approval workflow. However, other areas in an IAM Framework can also be equipped with an approval workflow. This serves to provision the entitlements granted in the approval workflow (to stay with the example) comprehensibly and securely for the account in question in order to make it more difficult for an attacker to assign entitlements to the account he has taken over. For this reason an approval workflow must be established that meets the following requirements in this chapter.

Motivation: Prevention of the fraudulent acquisition of (far-reaching) access authorizations to prevent e.g. data exfiltration and manipulation as well as identity misuse.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-65/i47

Req 66	The roles of applicant and approver must be performed by different natural identities.

As part of an approval workflow, those in the role of approver exercise a controlling function by deciding whether, for example, the applicant needs the requested entitlements or not. This control function can only be exercised to a very limited extent by technical identities, such as robots ("bots"). In addition, technical, automated processes can be manipulated by attackers. For this reason, the roles of applicant and approver must be exercised of natural identities. In addition, the roles of applicant and approver must be performed by different natural identities. This prevents applicants from being able to assign access permissions to themselves on their own.

Motivation: Prevention of manipulation of approval workflows with subsequent illegal assignment of (elevated) access permissions.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-66/i47

Req 67	When assigning critical entitlements, the 4-eyes principle must be used for the role of the approver.

Especially when assigning critical entitlements, the 4-eyes principle for the role of the approver must be implemented in the form that at least two different natural identities must approve the assignment of critical entitlements. This is intended to make it even more difficult to gain access to infrastructures and data that are critical to the organization.

For Deutsche Telekom AG, definitions for critical entitlements can be found in the Group Security Policy in Chapter 3.3 "Technology & Products" (keyword "Roles and Access Rights") and in Chapter 3.6 "Business Continuity" (keyword "Business Continuity Management").

Motivation: Prevention of the fraudulent acquisition of (far-reaching) access authorizations to prevent e.g. data exfiltration and manipulation as well as identity misuse.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.69-67/i47

5.10. Self Service-Workflow

Req 68	The self-registration of an identity or an account must not be possible.

Attackers must not be able to create their own identities and accounts in an internal IAM framework (self-registration). Otherwise, these accounts could be used for attacks on the target applications. This requirement is also based on requirements from the internal audit department and external auditors of an organization.

Business Customer IAM: If the IAM for business customers is operated by the organization itself, employees must not be able to create their own identities and accounts analogous to an internal IAM framework. If the Business Customer IAM is operated by the customer, the customer's security requirements apply.

Private Customer IAM: Self-registration of identities and accounts by private customers is permitted.

Motivation: Reduction of the attack surface and associated reduction of the probability of occurrence of security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-68/i47

5.11. Provisioning of authentication and authorization instances

Req 69	When provisioning authentication and authorization instances, standardized and established protocols must be applied using up-to-date encryption technology.

Self-developed protocols are usually programmed with a focus on functionality rather than security, so they are vulnerable to attack. For this reason, the provisioning of authentication and authorization instances must apply standardized and established protocols using up-to-date encryption technology. An example of this is SCIM. In addition, the use of standardized protocols reduces potential vendor lock-in, making it easier to switch to another IAM Framework vendor if required in the future.

This requirement is an extension of the Req. 7 ("Data in need of protection must be protected against unauthorized viewing and modification during transmission and storage.") from the document "3.01 Technical Baseline Security for IT/NT Systems ".

Motivation: Reduction of the attack surface and associated minimization of the number of security incidents.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-69/i47

Req 70	The IAM Framework and the authentication and authorization instance must authenticate each other during provisioning.

Also and especially when communicating between two IT/NT systems, mutual authentication of the communication partners must be ensured, so that, for example, a man-in-the-middle attack cannot be carried out. Furthermore, this prevents an attacker from contributing his own accounts to the authentication and authorization instance. for these reasons the IAM Framework and the authentication and authorization instance must authenticate each other during provisioning.

Motivation: Prevention of man-in-the-middle attacks and introduction of fake accounts into the authentication and authorization instance.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-70/i47

Req 71	Only one provisioning system may be used per authentication and authorization instance.

If two or more IAM Frameworks provision or change objects in the authentication and authorization instance, there is a risk of inconsistent state and/or reducing the availability of the authentication and authorization instance. For this reason, only exactly one IT system may be used provisioning per authentication and authorization instance.

Motivation: Increase the availability of the authentication and authorization instance and reduce inconsistent states that can affect the security or production of the organization.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities

ID: 3.69-71/i47

6. Connection of target applications

6.1. Requirements for target applications

Req 72	The central authentication and authorization instance of the IAM Framework must be used.

To ensure strong authentication and authorization as well as central security monitoring, the central authentication and authorization instance of the IAM Framework must be used.

The following is a list of protocols that should be offered by a central authentication and authorization instance in accordance with IAM Security Requirements:

- OAuth2
- OpenID Connect
- SAML
- Kerberos
- WebAuthN
- Diameter

Motivation: High protection of the accounts used as well as better detection of misuse of the accounts

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.69-72/i47

Req 73	After a logout or after the end of the session lifetime, the session and/or token must be invalidated.

During the runtime of an active session with a web application, the validity of the session is stored in a token. This is done, for example, by storing the session data in a cookie or a JSON web token (JWT). After the end of a user's session due to an active logout or the expiration of the session, the corresponding token, in which the data of the session is stored, must be invalidated.

This requirement is an extension of the Req. 20 ("The system must allow users to log out of their current session.") and Req. 21 ("Sessions must be automatically terminated after a period of inactivity adapted to the intended use") from the document "3.01 Basic Technical Protection".

Motivation: Attackers could take over the token and, if necessary, misuse for a replay attack, for example to divert data from the organization or to misuse the account for further attacks.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-73/i47

Req 74	An emergency account must be created locally in the target application in order to be able to access the target application in the event of a failure of the authentication and authorization instance of the IAM Framework.

To maintain the business operations of the organization, the target application must enable it to log in locally with an emergency account in the event of an emergency, bypassing the authentication and authorization instance of the IAM Framework. This emergency account must have extensive entitlements and must be protected in the best possible way against unauthorized access. The emergency account must meet at least the password policy for service accounts (see documents "3.75 IAM – Internal", Requirement "If passwords are used as an authentication feature for technical accounts, they must be at least 30 characters long and contain three of the following character categories: lowercase letters, uppercase letters, numbers and special characters."). The use of this emergency account is subject to the requirements of a Business Continuity Management Plan.

Motivation: This emergency account should make it possible to access the data of the target application even in the event of a crisis and to be able to carry out any further steps within the framework of business continuity management. This is intended to reduce or avoid further damage to the organization.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.69-74/i47

Req 75	If a target application is connected to an Active Directory Forest with several domains, the target application must support multidomain capability.

All target applications that are or will be connected to an Active Directory Forest with several domains now or in the future must be designed in such a way that they are multi-domain capable. In this context, multi-domain capability means that accounts and their groups from several domains of an Active Directory forest can be used in a target application.

If the target application is connected to a central access layer provided by the IAM Framework, it is the task of the central access layer to ensure multi-domain capability..

Target applications with legal and/or contractual exceptions listed below, which may therefore only be connected to a single domain, are excluded from this requirement.:

- German Eyes Only (GEO)
- VS-NfD (Geheimschutz)

Motivation: Prevention of the creation of so-called duplicate accounts as a bypass to legal and/or contractual regulations

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-75/i47

Req 76	When using a central authentication and authorization instance, it must be ensured that user accounts cannot natively log on to a target application.

With the connection of the target application to an IAM framework, all locally existing accounts – except for the emer-

gency account – are usually removed from the target application. If this has not been done, an attacker is able to access the target application using a local account and, for example, exfiltrate data. For this reason, when using a central authentication and authorization instance, it must be ensured that only the emergency account can log in natively to the target application.

Motivation: Reduction of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.69-76/i47