Rail Security Expert Group

Identity and Access Management

25E053
1A
05.02.2026

Modification history

Version	Date	Modification / Description	Editor
1A	05.02.2026	Initial Release published after internal and external (CER/EIM) review	Klas Andren, Christof Jungo, Oliver Lovric, Richard Poschinger, Nicolas Poyet, Patrick Rozijn, Yves Zosso

Table of Contents

Table of Figures

1 Introduction

1.1 Scope

1.1.1.1 The purpose of this document is to describe best practices for IAM. The scope includes the application of EU-Rail Cybersecurity Specifications and considerations for legacy systems.

1.2 References

1.2.1.1 Subsets and EUG publication are referenced directly with their corresponding ID.

Other referenced documents:

[1] EU-Rail System Pillar CyberSecurity Group, „Taxonomy and References 1.00,“ 2025.

[2] S. Bradner, “RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels,” Network Working Group, 1997.

[3] EU-Rail System Pillar CyberSecurity Group, „Secure Component Specification V1.00,“ 2025.

[4] EU-Rail System Pillar CyberSecurity Group, „Shared Cybersecurity Services Specification V1.00,“ 2025.

[5] European Union, „Regulation (EU) 2016/679 - General Data Protection Regulation,“ 2016.

[6] European Union, „Directive (EU) 2022/2555 - NIS 2 Directive,“ 2022.

[7] European Union, „Regulation (EU) 2024/2847 - Cyber Resilience Act,“ 2023.

1.3 Abbreviations

ESI ..... *Enterprise Security Interface*
IAM ..... *Identity and Access Management*
LDAP(S) ..... *Lightweight Directory Access Protocol (Secure)*
MDM ..... *Maintenance and Data Management*
MFA ..... *Multi Factor Authentication*
MNT ..... *Security Maintenance*
NAC ..... *Network Access Control*
OPC-UA ..... *Open Platform Communication - Unified Architecture*
PKI ..... *Public Key Infrastructure*
RA ..... *Registration Authority*
SAML ..... *Security Assertion Markup Language*
SCIM ..... *System for Cross-domain Identity Management*
SCS ..... *Shared Cybersecurity Service*
SDI ..... *Standard Diagnostic Interface*
SLOG ..... *Security Logging*
SMI ..... *Standard Maintenance Interface*
SOC ..... *Security Operations Centre*
SSI ..... *Standard Security Interface*
UAS ..... *User Authentication Service*
VPN ..... *Virtual Private Network*

ERTMS Abbreviations are listed in Subset-023

EU-Rail Abbreviations are listed in [1]

1.4 Authors

1.4.1.1 The Rail Security Expert Group (RSEG) consists of security experts of the following groups:

- ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
- EULYNX Security Cluster – Part of the EULYNX Initiative

1.4.1.2 The following members of the Rail Security Expert Group were involved in creating this document:

- ERTMS User Group (EUG) / EULYNX
  - Richard Poschinger
- SBB
  - Oliver Lovric
  - Christof Jungo
  - Yves Zosso
- Trafikverket
  - Klas Andren
- NS
  - Patrick Rozijn
- SNCF
  - Nicolas Poyet

1.5 Applicability and Document Status

1.5.1.1 To ensure the usability for tender documents, this document is using classifications and requirement key words. This classification does not result in any binding requirements for members of the EUG or other involved parties. The documents will be updated in the future to be adapted to a changed threat landscape, updated standards, and newly developed security solutions.

1.6 Definition of Requirement Types

1.6.1.1 This document uses key words indicating requirement levels according to RFC 2119 [2]. Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified
O	Optional	not mandatory, must be as specified if implemented
I	Informative	included for clarification purposes only
R	Recommendation	included as recommendation

Texts without a tag do not constitute a requirement.

2 Use Cases

2.1.1.1 The following chapters describe the use cases defined for IAM in the EU-Rail scope and in other railway systems. **(I)**

2.1.1.2 The IAM is used to eliminate “the need for credential stores on individual components” [3] and hence provides the capability to centrally distribute unique identities. **(I)**

2.2 EU-Rail IAM

2.2.1.1 The EU-Rail Shared CyberSecurity Services Specification [4] is defining two interfaces in the scope of IAM. **(I)**

2.2.2 SCS-IAM

2.2.2.1 The SCS-IAM service and its corresponding interface is used to manage identities of human users and secure components (including their software processes). **(I)**

2.2.2.2 Authorisations provided by the SCS-IAM service are used by the following interfaces: **(I)**

- OPC-UA-based interfaces (SDI/SMI/SSI-MNT)
  machine-to-machine communication and optionally human-to-machine access for the following cases:
  - to MDM via SDI/SMI and
  - to SCS-MNT via SSI-MNT
- SSI-NAC
- SSI-PKI RA

2.2.2.3 Using an HMI-based access to MDM and SCS-MNT with authentication via SSI-UAS is recommended (instead of using direct human user access via OPC-UA including authentication via SSI-IAM). **(R)**

2.2.2.4 The SCS-IAM service can be connected to an Asset Management and an Identity Provider / Corporate Directory via the proposed ESI-IAM interface. **(I)**

2.2.3 SCS-UAS

2.2.3.1 The SCS-UAS service and its corresponding interface is used to authenticate and authorise human users. **(I)**

2.2.3.2 Authorisations provided by the SCS-UAS service are used by the following interfaces: **(I)**

- All interfaces with human user access
  (excluding direct OPC-UA human user access which is authenticated using SCS-IAM)

  This is not applicable to status information visible to personnel on-site. Access by reading optical displays or pushing physical buttons is excluded from this requirement. This access is controlled by physical access control.

- Systems not using human user access are amongst others:
  - EULYNX field element Subsystem
    (Maintenance interface deactivated in operation)
  - ETCS On-Board (without DMI)
  - ATO On-Board
- Physical access control (e.g. door locks) is not in scope of the EU-Rail Security Specifications
  - ETCS Balise and LEU Maintenance Interface
- Systems which might use human user access are amongst others:
  - MDM
  - SCS
  - TCS / TMS
  - ETCS DMI (DMI-authentication using SCS-IAM is depending on decisions for TSI CCS input)
  - KMC
  - RBC (Maintenance Access)
  - EIL (Maintenance Access)

2.2.3.3 The SCS-UAS service can be connected to an Identity Provider / Corporate Directory via the proposed ESI-UAS interface. **(I)**

2.2.4 On-Board IAM/UAS

2.2.4.1 For on-board usage of the SCS-IAM and SCS-UAS services, a local instance of these services can be installed, which is providing cached data in case the connection to the central instance (or the central instance itself) is not available. **(I)**

2.3 Legacy Use Cases

2.3.1 Network Access Control (NAC)

2.3.1.1 NAC capabilities are usually already available in the infrastructure network components and its management. **(I)**

2.3.1.2 Usage of NAC by e.g. servers is still limited and OT-components are only partially implementing NAC capabilities. **(I)**

2.3.2 Infrastructure Applications

2.3.2.1 Systems that already use IAM include, among others: **(I)**

- Network Management
- Newly installed Remote Access systems via e.g. Jump Hosts
- Maintenance and Data Management (MDM) – Vendor Specific

2.3.2.2 Systems that are not yet using IAM include, among others: **(I)**

- Traffic Management
- Interlockings
- Train Protection System

2.3.3 On-Board Applications

2.3.3.1 The usage of IAM solutions in On-Board systems is currently mainly limited to comfort applications controlling access to e.g. non-CCS and non-safety services for train staff or Wi-Fi access (NAC). **(I)**

2.3.3.2 Systems that already use IAM include, among others: **(I)**

- Passenger Information System
- Passenger and Employee On-Board Wifi
- Train driver support systems
- Newly installed Remote Access systems via e.g. Jump Hosts

2.3.3.3 Systems that are not yet using IAM include, among others: **(I)**

- Train Control Management System
- Train Protection System

2.3.3.4 IAM could be used to control maintenance access to legacy On-Board applications. **(I)**

2.4 Additional Use Cases

2.4.1.1 Physical access control systems can use the IAM. **(I)**

3 Infrastructure

3.1 Protocols

3.1.1.1 The following protocols are standardized (e.g. using RFCs) and widely supported by client and server applications/libraries. **(I)**

3.1.2 EU-Rail Security Specifications

3.1.2.1 Details on SCS-IAM and SCS-UAS are available in Chapter 2.2. **(I)**

3.1.2.2 SSI-IAM is using SCIM version 2.0 (System for Cross-domain Identity Management). SCIM is a REST based protocol transferred via HTTPS. **(I)**

3.1.2.3 SSI-UAS is using OpenID Connect 1.0. OpenID Connect is specifying a REST based protocol transferred via HTTP. This protocol is used to transfer OAuth 2.0 tokens. OpenID Connect is used with the Authorization Code Flow. The usage of Authorization Code Flow with Proof Key for Code Exchange (PKCE) is optional. **(I)**

3.1.2.4 SSI-UAS is providing authentication using the following options: **(I)**

- X.509 Certificate + Additional Factor
- Password + Additional Factor
- Passwordless authentication + Additional Factor

3.1.3 Legacy Protocols

3.1.3.1 LDAP/LDAPS

Lightweight Directory Access Protocol (LDAP) works by allowing clients to query and modify the directory data stored in a centralized server, typically in a hierarchical structure, often called a ‘directory tree’. LDAP was established as an industry standard in the 1990s and is among the oldest identity and access management protocols. It runs above the TCP/IP stack. LDAP is regarded as complex regarding scalability, administration and not regarded as a future proof solution. **(I)**

3.1.3.2 SAML

Security Assertion Markup Language (SAML) is an open standard that enables the secure exchange of authentication and authorization data between parties. It supports Single Sign-On (SSO). It is transferring XML formatted data via HTTPS. It is not regarded as a future proof protocol, as newer standards like e.g. OpenID Connect are getting more widely accepted. **(I)**

3.1.3.3 Other Implementations of OAuth/OpenID

OpenID might be used in older versions for legacy implementation. Furthermore, OpenID Connect 1.0 can be implemented using other authorization flows compared to the definition of EU-Rail SSI-UAS. In addition, other usages of OAuth tokens might appear in existing installations. **(I)**

3.2 Platforms

3.2.1.1 Table 1 provides an overview of IAM platforms and their compliance with the EU-Rail Cybersecurity Specifications. It also presents the option to install these platforms on-premises.. This is just a selection of platforms and shows the status according to the release date of this document. **(I)**

3.2.1.2 As indicated in Table 1 some vendors are providing cloud and on-premises solutions in parallel. When considering on-premises solutions, take into account the potential shift in vendor product strategies towards further developing cloud products **(I)**

Product Name	Description	On-Premises	Open Source	SSI-UAS	SSI-IAM	EU-Rail Compliant
AWS Identity and Access Management	AWS Identity and Access Management is the default directory service (cloud-based) from Amazon used in Amazon Web Services (AWS).			✓	✓	✓
ForgeRock Identity Platform	ForgeRock Identity Platform which can be installed on-premises	✓		✓	✓	✓
Gluu	Gluu is an open-source directory service.	✓	✓	✓	✓	✓
bKeycloak	Keycloak is an open-source directory service which can be installed on premises	✓	✓	✓	(✓)[1]	✓
Microsoft Active Directory (AD)	Microsoft Active Directory (AD) is one of the most used directory services for enterprise environments.	✓		✓[2]		
Microsoft Entra ID	Microsoft Entra ID (formerly Azure AD) is the default directory service (cloud-based) from Microsoft used in amongst others Microsoft Azure and Microsoft (Dynamics) 365			✓	✓	✓

[1] By installing a plugin (licensed, non-open-source) SCIM (SSI-IAM) support can be added.
[2] ADFS needs to be used to provide SSI-UAS

Product Name	Description	On-Premises	Open Source	SSI-UAS	SSI-IAM	EU-Rail Compliant
Okta	Okta is a widely used cloud-based directory service.			✓	✓	✓
Oracle Identity and Access Management Suite	Oracle Identity and Access Management Suite is an on-premises directory service	✓		✓	✓	✓
Oracle Identity Cloud Service	Oracle Identity Cloud Service is providing a cloud-based directory service.			✓	✓	✓
WSO2 Identity Server	WSO2 Identity Server is an open-source directory service which is also offered in the cloud	✓	✓	✓	✓	✓

Table 1: IAM Platforms

4 Identities

4.1 Identity Structures

4.1.1.1 Identities are structured as displayed in Figure 1 containing user, user groups, roles, permissions and resources. **(I)**

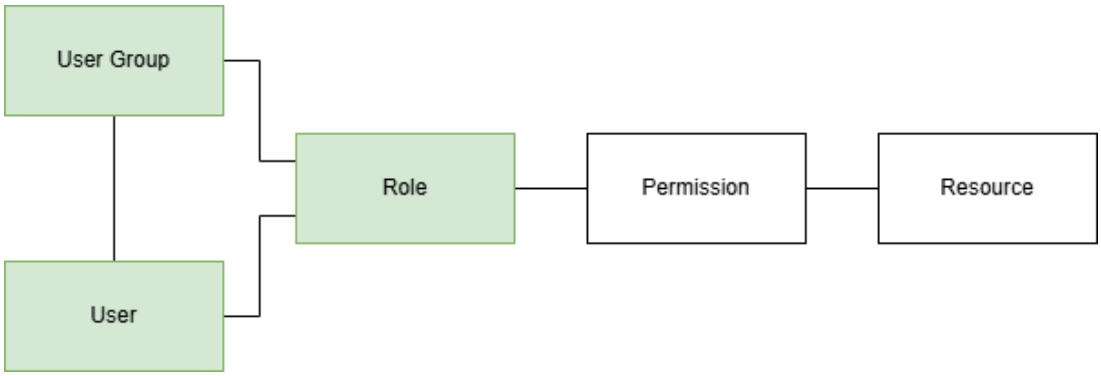

Figure 1: Identity Structure Overview

(identities shown in green)

4.1.2 User

4.1.2.1 A user in an IAM system refers to either a human user or a machine entity (including software processes) that is granted access to the organisation's resources and systems. **(I)**

4.1.2.2 In the EU-Rail Cybersecurity specifications the following examples for IAM users exist: **(I)**

- Human Users
  (Human to Machine access controlled via SCS-UAS)
  - Administrators / Maintenance Personnel
  - Traffic Control System Operators
  - Train Drivers
  - (Foreign) KM Domain Operators
  - Users of the Trackworker Safety System
- Machine Entities
  (Machine to Machine access controlled via SCS-IAM)
  - MDM
  - EULYNX Field Element Subsystem and Interlocking (for SMI/SDI connections)
  - NAC
  - PKI

4.1.2.3 A user is typically associated with a unique identity, which in turn is connected to specific attributes. **(I)**

4.1.3 User groups

4.1.3.1 User groups within an IAM system are groups of user entities organised to allow easier management of authorisations and access control. **(I)**

4.1.3.2 User groups can be categorized as follows: **(I)**

- **Static groups:**
  - **Definition:** Users are manually added or removed, which provides precise control.
  - **Use Case:** Stable groups which are not changed often or are highly sensitive
  - **Example:** Administrators or Traffic Control System Operators
- **Dynamic groups:**
  - **Definition:** Membership is assigned automatically based on rules using user attributes, which minimises the administrative efforts
  - **Use Case:** Department-based access where employees frequently join, leave, or move teams.
  - **Example:** Maintenance Personnel using diagnostic systems
- **Nested groups:**
  - **Definition:** Groups that include other groups
  - **Use Case:** Useful for organising users in hierarchical permissions model.
  - **Example:** Combining different maintenance groups (e.g. Point, RBC, EIL) into one nested maintenance and diagnostic group
  - **Recommendation:** A maximum of one nested group layer is recommended to reduce complexity and increase traceability.

4.1.4 Permissions

4.1.4.1 Permissions control access to resources and what actions users can perform regarding this resource. **(I)**

4.1.4.2 Typical permissions are: **(I)**

- Read: View resource
- Write: Modify or create resource
- Execute: Run program or function

4.1.4.3 OPC-UA Permissions used in the EU-Rail interfaces are e.g.: **(I)**

- Browse: See reference to node
- Read: Read value
- ReceiveEvents: Receive event of a node
- Call: Call a method on the object

4.1.4.4 IAM specific permissions can be linked to application specific permissions. E.g. in the EU-Rail SSI interfaces the permission “eu.rail.ssi.security-read” is mapped to the following OPC UA permissions: **(I)**

- Browse
- Read
- ReceiveEvents

4.1.5 Roles

4.1.5.1 Roles are sets of permissions which can be assigned to users or user groups. **(I)**

4.1.5.2 For example, human user categories mentioned in Chapter 4.1.2 can be regarded as roles. **(I)**

4.2 Administration / Workflow Services

4.2.1 Self Service

4.2.1.1 Identity Self Service allows users to manage their own identity-related tasks eliminating the need for IT support or administrators. These services can be used in SCS-UAS. **(I)**

4.2.1.2 Password Management allows users to change or reset their passwords. SCS-UAS offers several authentication options including passwordless authentication. Depending on the operator's selection of allowed authentication methods, password management may not be required. **(I)**

4.2.1.3 Authenticator Management refers to the processes and tools involved in securely managing authentication methods. This includes e.g managing TOTP (time-based one-time passwords) or Passkeys as specified for SSI-UAS. Activities include Set-up and Enrolment, Token Management and Change of Authenticator Method. **(I)**

4.2.1.4 Profile Management allows end users to e.g. change personal information or contact details. **(I)**

4.2.1.5 Access Request Service enables users to request access to applications, systems and resources which is then followed by an approval process. However, due to a comparable static assignment of access rights for operational and safety-related railway systems and as well as the possible risks of these processes, usage of these capabilities is not recommended. Internal request services for the Management might still be applicable for systems in scope of this document. **(I)**

4.2.2 Application and Integration Procedure

4.2.2.1 The following application and integration procedure is recommended for adding systems (e.g. systems of the EU-Rail scope) to the IAM. This process does not include previous management decisions on commissioning the system. **(I)**

1. Check compliance to the security requirements of the operator and/or the EU-Rail Security Specifications
   (Identify any security related risks or gaps that need to be addressed.)
2. Check compliance to the interface of the IAM (SSI-IAM and SSI-UAS if EU-Rail specifications are used).
   (Document the integration with the IAM including related data flows.)
3. Check required additional permissions for the affected systems (e.g. if using SSI-UAS)
   (Review the roles and access levels necessary for the system to function correctly).
4. Check if the system is available and documented in the asset inventory
5. Perform tests to ensure the system integrates with the IAM.
   (Verify that the system works as intended with the IAM and ensure no security related issues remains. Start the testing procedure in isolated dedicated test environments).
6. Integrate the system and add permissions/roles accordingly.

4.2.2.2 The following application and integration procedure is recommended for adding users to the IAM. This process does not include previous management decisions on employing the user and its organisational assignment to departments and roles. **(I)**

1. Check if the user is available, sufficiently identified and fully profiled in the corporate directory.
2. Integrate the user and add permissions/roles accordingly.

4.2.3 Authorization process

4.2.3.1 The Authorization process in IAM systems is critical for ensuring that users have the appropriate access rights to perform their roles and responsibilities, while also maintaining security. **(I)**

4.2.3.2 The following example for a human user authorisation process can be used. The process is based on previous steps described in Chapter 4.2.2: **(I)**

1. Role is requested by the user her/himself or another user.
2. Superior checks and can confirm the request.
3. Resource owner checks and can approve the request.
4. If the requested role affects critical roles, a second person (e.g. Deputy Resource Owner) checks and can approve the request. (Dual Control/Quorum Principle)

4.2.3.3 Critical Roles affected by the Dual Control Principle are e.g.: **(I)**

- SCS-MNT Administrator Role (including eu.rail.ssi.security-execute permission)
- MDM Administrator Role (including permission to update software/configuration)
- Operator Role on the Traffic Control System (including permissions to set routes and auxiliary signals)
- KMC Operator Role (including permissions to delete KMACs)

4.2.4 Delegated Administration

4.2.4.1 Delegated administration provides a convenient way for users to perform most IAM Identity Centre administrative tasks. Hence e.g. a Resource Owner who is not an Administrator can be assigned roles to perform tasks described in Chapter 4.2.3. **(I)**

4.2.5 User Management

4.2.5.1 User metadata (e.g. username, entity identifier, email address) are provided by other connected systems like the asset management or a corporate directory. **(I)**

4.2.5.2 To maintain data integrity, user and IAM data need to be kept consistent with other systems using master data synchronisation, to avoid duplicate data. **(I)**

4.3 Federation

4.3.1.1 Federation is a process that allows users to access systems and applications across organizational boundaries using their existing credentials. **(I)**

4.3.1.2 Since OT environment work in clearly defined organizational boundaries, federation is not applied in this context. **(I)**

4.4 Compliance

4.4.1.1 In the context of EU law, compliance in Identity and Access Management (IAM) involves adhering to regulations such as the General Data Protection Regulation (GDPR) [5], the Network and Information Systems Directive (NIS2) [6] and the Cyber Resilience Act (CRA) [7]. **(I)**

5 Security

5.1 Policies

5.1.1.1 IAM policies are formal rules that define a set of permissions, specifying which actions are allowed or denied for users, groups, or roles within a system. **(I)**

5.1.1.2 Policies may allow access during a specific range of times and/or dates. Following use cases could be applied: **(I)**

- External Maintenance Personnel
  If external maintenance is requested, access can be activated temporarily (just for the expected maintenance period).
  (This could also allow active monitoring by railway staff during the maintenance period.)
- Restrict to office hours
  Access can be restricted to office hours. Office hours are usually depending on division and tasks. E.g. regular administrators might be able to gain access between 7:00 and 19:00, but the SOC team is not restricted to office hours as they perform 24/7 duties. Railway specific examples:
  - On-Line KM Administrators:
    Regular business hours (e.g. 7:00 - 19:00)
  - Network Administrators without 24/7 duties:
    Regular business hours (e.g. 7:00 - 19:00)
- Supervisory override
  An IAM supervisory override can be used to bypass standard access restrictions in case of emergencies. These overrides can be defined per user group / user and be time restricted. The supervisory override can be used to:
  - Extend permissions to additional personnel in the department if e.g. on-duty administrators require additional support from other department members, which do not usually have access to the affected system.
  - In case of emergencies restrictions to office hours can be removed, e.g. to provide access for all required members of the department.

5.1.1.3 Policies may allow the enabling and disabling of access from regions (locations). As locations can be forged, this is only an additional layer of protection. It can be used for e.g. the following use cases: **(I)**

- Access can be restricted to the railway operator's country. In this case additional countries could be added if e.g. access by foreign maintenance personnel of the supplier is requested or if support is required from e.g. an administrator who is on holiday/workation.
- Furthermore, also the Supervisory Override (allow by exception) can be restricted to e.g. block access from non-EU/EEA/EFTA countries.

To enforce these restrictions blocking well-known VPN-providers is recommended.

5.1.1.4 Policies may allow the enabling or disabling access from specific IP address ranges. This could allow restriction of critical access from internal networks only. **(I)**

5.1.1.5 Certain sensitive operations and functions require the cooperation of multiple parties before execution. This multi-party control can be enforced by requiring k out of n individuals (a quorum) to be authenticated and authorised prior to performing the requested action. Use cases can include for example: **(I)**

- Granting administration access
- Trigger Restore / Reset
- Deleting all KMACs (in KMC)
- Granting high privilege access like e.g. Interlocking Control Centre Operator or MDM access

5.1.1.6 Polices may define the usage of MFA (Multi factor authentication). A strong recommendation is to apply MFA wherever possible. **(I)**

5.1.1.7 Conditional access policies are a set of rules that control who can access what resources, and under what conditions. **(I)**

- If a defined user location is detected, then a policy checking the login behaviour is enforced.
- If a certain device type is used, then a policy that requires a system state such as system hardening.

5.1.1.8 System hardening policies are e.g. requiring a minimum system version, active anti-virus and disk encryption. **(I)**

5.1.1.9 Policy Control are mechanisms and processes used to manage, enforce, and audit implemented system policies. The policies define access rules and security requirements, whilst policy control makes sure that the rules are applied and monitored. **(I)**

5.2 IAM Validation

5.2.1.1 IAM validation rules are vital for maintaining a secure, compliant, and streamlined IAM system that meet your organisations policies over its lifecycle. By enforcing robust validation checks at various stages of identity lifecycle management, organisations can minimise risks related to for example identity fraud, unauthorised access and data breaches. **(I)**

5.3 Traceability

5.3.1.1 Proper traceability ensures that all access to systems, resources, and sensitive data is logged and auditable, providing accountability, transparency, and compliance with regulatory requirements. Logging can be implemented using the SSI-SLOG interface. **(I)**

5.3.1.2 Depending on legislation and working council agreements regarding privacy, a separation of access to log data might be required. The separation could e.g. include the following roles: **(I)**

- Administrator / SOC
  Can access log data without revealing identifiers of the human users.
- Investigation Access
  Full log data access (including identifiers of human users)
  This access is highly restricted, only available few authorised employees and only used for access which has been permitted by law (e.g. by judicial authorisation during an investigation).

5.3.1.3 Additional information regarding logging can be found in 23E177 (Security Logging and SIEM Guideline). **(I)**