RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

Position Paper Shared Services

Document id: RCA.Doc.78

Table of contents

List of Figures

Version history

Version	Date	Author	Description
0.1	2022-07-18	Ulrich Meier, Richard Poschinger, Max Schubert	Initial draft
0.2	2022-07-27	Ulrich Meier, Max Schubert	Improvement System wide use, Time, clarification train side, wording, spelling
0.3	2022-09-08	Ulrich Meier, Ulrich Schöni, Max Schubert	Integration of RCA Review comments and adaption to RCA template

1 Introduction

1.1 Release information

Basic document information:

RCA-Document Number: 78
Document Name: Position Paper Shared Services
Cenelec Phase: 1
Version: 0.3
RCA Baseline set: BL1R0
Approval date: 2022-09-30

1.2 Imprint

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)

Support and Feedback:
For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu.

1.3 Disclaimer

This issue is a preliminary version of this document. The content of this document reflects the current ongoing specification work of RCA. Formal requirements management and change management will be introduced in future iterations. The content may be unfinished, will likely contain errors and can be changed without prior notice.

1.4 Purpose of this document

The purpose of this document is to present the principle and a basic concept of Shared Services for the whole Reference CCS Architecture (RCA).

The document follows the specification principles and thus uses “shall” for requirements, “should” for recommendation and “could” or “might” for options.

1.5 Terms and Abbreviations

The terms and abbreviations are listed in RCA terms and abstract concepts [9] or in the EULYNX Glossary [8].

1.6 References

Reader’s note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references.

The following references are used in this document:

[1] EULYNX Baseline 4 Release 1

[2] Eu.Doc.117 Shared Security Interface [1]

[3] Eu.Doc.121 Shared Security Platform [1]

[4] Eu.Doc.114 Security Specification [1]

[5] Eu.Doc.115 Security Parameter Specification [1]

[6] Eu.Doc.116 Security Treat & Risk Analysis [1]

[7] Eu.Doc.15 Security Concept [1]

[8] Eu.Doc.9 Glossary [1]

[9] RCA.Doc.14 Terms and abstract concepts

2 Shared Services

This section is based on work done for EULNYX [1] with specific reference to Eu.Doc.117 “Shared Security Interface” [2] and Eu.Doc.121 "Security Service Platform [3]. Basis of the definition are the requirements documents Eu.Doc.15 - Security Concept - and Eu.Doc.114 [4] - Security Specification -. The overall source is the performed Threat and Risk Analysis, documented in Eu.Doc.116 [6]. Additional definitions have been included, where useful and known from best practices.

Shared Services support the implementation of security measures protecting safety functionality and support operation of the overall system. The shared services are non-safety as the safety is ensured and controlled by safety of the respective subsystem or operational procedure. The Shared Services are categorized in Shared Security Services and Shared Supportive Services. Shared Security Services directly implement services to implement security measures. Shared Supportive Services offer broader, procedural supportive services, used in management or diagnostic use cases.

The Shared Services are a logical group of services used to support management and security functionality and measures. The Shared Services shall be provided based on the same definition and principles to the whole CCS system. No difference shall be made between the different areas like ERTMS, On-board or trackside equipment.

The presented Shared Services structure and definition allow the migration of existing shared services, that are currently available in TSI subsets. One example is key management for ERTMS. A parallel operation of a current online key management and future identity/certificate management system is possible and allows step-by-step migration toward the target state, based on the latest technology and knowledge. This approach also allows further development towards future requirements.

2.1 Shared Services: Purpose

The Shared Services definition does not require that each service is only presented once (single system) in the whole system. Additionally, it is also allowed that one system covers multiple services, e.g., a Maintenance and Diagnostic Management System could provide the services Backup, Asset Configuration, Software and Config Repository and Monitoring.

The following Shared Security Services are provided:

- Time (TIME)
- Security Logging (SLOG)
- Identity and Access Management (IAM)
- Public Key Infrastructure (PKI)
- Security Incident and Event Management (SIEM)
- Backup (BKP)

The following Shared Supportive Services are provided or shall be available:

- Asset Management (AM)
    - Asset Inventory (AM-INV)
    - Asset Configuration (AM-CFG)
- Software and Config Repository (REPO)
- Diagnostic Logging (DLOG)
- Monitoring (MON)
- Data Prep
- Diagnostic Data Analytics (DDA)

Within RCA, the Shared Services are located in the Generic Functional Layer (see). As can be seen in , some of the Shared Services defined in this document already exist in RCA (DLOG, MON, SLOG, IAM, REPO, AM) others are not yet defined in RCA (DDA, PKI, TIME, SIEM, BKP).

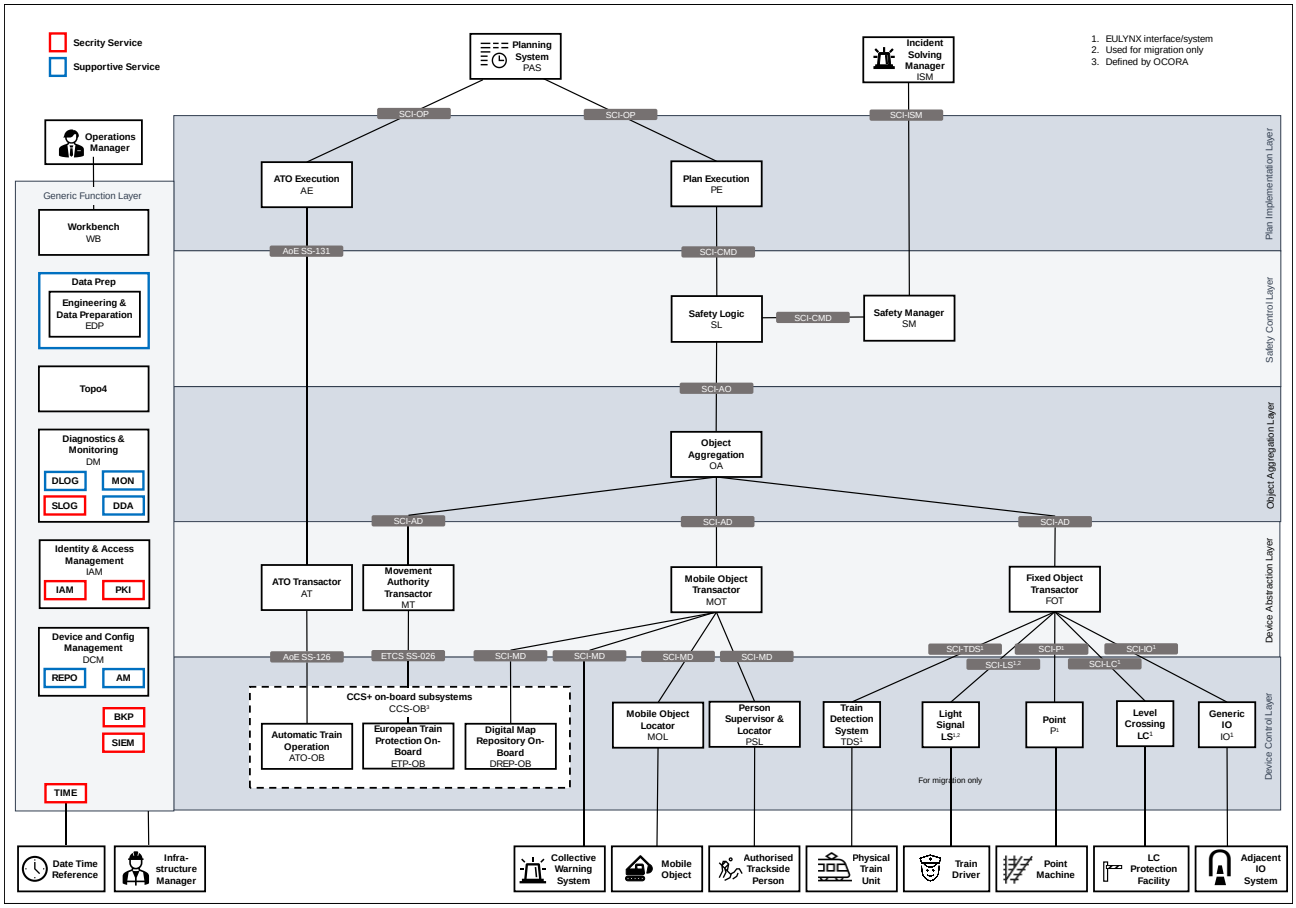

Figure 1: Shared Services in RCA architecture

It also shows that the Shared Services shall be used rail system wide, including rolling stock.

As an example, in EULYNX a similar Shared Services model is published with BL4R1, see Figure 2.

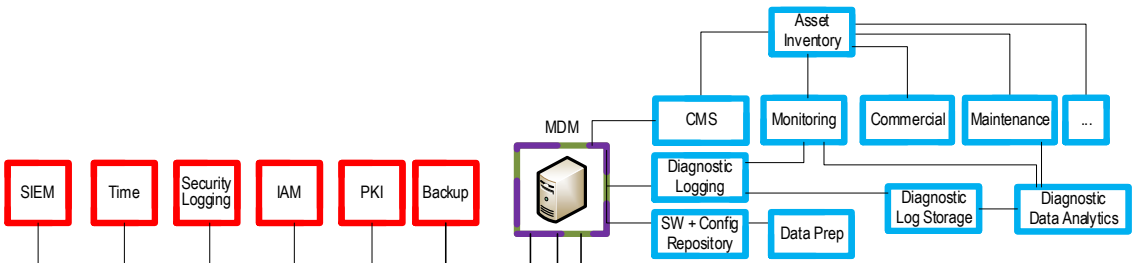

Figure 2: EULYNX Shared Services (Eu.Doc.15 [7], Eu.Sec.362 cropped)

These services are implemented in dedicated technical systems. Which protocols to be used is defined in Eu.Doc.114 [4], Eu.Doc.115 [5] and Eu.Doc.117 [2]. EULYNX documents the Shared Service Platform and the MDM for providing some of these services.

2.1.1 Time (TIME)

The Time service provides a reliable and accurate time to be used by all systems and subsystems. This time is synchronised with national time base and is in UTC. This ensures an independent time base created and maintained at the IM and using UTC avoids any issues related to daylight saving and international coordination.

It ensures accuracy, availability of a system-wide time. With the use of UTC and NTP no further time synchronisation between systems is necessary.

This service is only having interfaces to technical systems and is using no other shared service. This service uses national time services.

2.1.2 Security Logging (SLOG)

The Security Log service is collection and data storage for all security related log and monitoring information. It stores the data and provides data to systems entitled to use them based on information provided by the IAM service. It ensures confidentiality, integrity, availability and non-repudiation of the data received. The service shall be able to fulfil timing requirements required by SIEM services.

This service is only having interfaces to technical systems and is using time, IAM, PKI and backup service.

2.1.3 Backup (BKP)

The Backup service offers services to store and retrieve relevant information, e.g. backup files, in a secure way to ensure confidentiality, integrity, and availability. All tasks to secure the information at rest is done by the centralized part of the backup service.

The backup service orchestrates the backups; hence it triggers backup processes at the target and monitors the success of this backup. The backup service on the centralized part of the backup service processes only data files provided by the device using the backup service and doing the backup. The service does not ensure that the backup's content is usable for restoring. The format of the file is depending on implementation of the backup generating system.

This service is only having interfaces to technical systems and is using time, IAM and PKI service.

2.1.4 Identity and Access Management (IAM)

The Identity and Access Management provides two functions:

- Identity Management: managing the digital identity
- Access Management: managing and providing information to grant/reject access

The Identity and Access Management service provides identity management for machines and personnel interacting with machines. The accuracy and reliability of identifying an entity is of paramount importance. This identification procedure must be secure.

Based on roles assigned to these identities, access management information is generated and provided to subsystems. The roles define the rights granted. The rights include for example granting communication setup or use of a functionality or capability of a subsystem/device. The IAM provides the access grant information to RCA subsystems, based on identity of the requesting subsystem.

The IAM service is having interfaces to technical systems and requires additional non-technical procedures/processes and time, PKI and backup services. For identity management there must be an interface to the supportive service "Asset Management".

Note: The digital identity is provided by PKI service.

2.1.5 Public Key Infrastructure (PKI)

The Public Key Infrastructure service provides the digital representation of the identity of an entity in the form of certificates used for public-key cryptography (encryption and integrity protection). It provides technical services to handle request, renew, revoke and validate certificates. To fulfil its purpose, it requires the identity management part of the IAM. This can be provided by the IAM service or by non-technical procedures/processes ensuring the management of the identify.

This service is only having interfaces to technical systems if the IAM service is present. If the IAM service is not present, this service must implement the identity management part of the IAM service or rely on external identity management.

This service is using time service.

Note: This service is a certificate authority and shall therefore be secured with respect for business continuity/disaster recovery. This combined with the security protection requirements for this data, the backup service of the Shared Services might not be suitable.

The architecture of the public key infrastructure is not specified yet and under discussion. Different set-ups are possible.

2.1.6 Security Incident and Event Management (SIEM)

The SIEM service provides security related monitoring of the system and supports the management of security incidents. The SIEM provides analytical functionality to detect security anomalies.

The basis for the SIEM analytics can be the information of an Intrusion Detection System (IDS), Security Logging and all information available from the diagnostic logging. Furthermore, the SIEM can be connected, amongst others, to the Asset Management, the IAM and further services that can support the correlation process for analytics.

If a potential anomaly is detected, an alarm is issued to a predefined organization that manages security incidents. Network Intrusion Detection (IDS) is one element amongst others within the SIEM service. The network intrusion detection uses log and monitoring information provided by network related components, e.g., network access, NAC logs, network events, network component logs, and traffic pattern over time or event related.

The SIEM service is a mainly technical service, however heavily interconnected to different data sources and may include additional non-technical procedures to enhance or verify anomaly detection. These non-technical procedures have interfaces to units operating Command Control Signalling system, units operating the network and units controlling and operating the railway service itself.

The basis for the SIEM set-up and its connected (on-boarded) systems are use-cases that need to be specified in advance.

This service is expected to change constantly over time to keep up with threat intelligence. Due to this nature, this service is not further documented in this document.

2.1.7 Diagnostic Data Analytics (DDA)

The Diagnostic Data Analytics service analyses diagnostic and monitoring data to either create alarms or support maintenance and fixing malfunctions. It applies simple concepts as well as sophisticated approaches using big data or AI. The service has a human interface.

2.1.8 Asset Management (AM, AM-INV, AM-CFG)

The Asset Management is used to track the life cycle of all hardware and software assets. The assets managed include all assets relevant within the RCA/EULYNX architecture and not only the security related assets. It tracks the data of assets beginning with the interface from the procurement management, ending with the decommissioning.

The Asset Management service is a non-technical service using available technical systems of an IM and is interconnected with commercial processes, including supply chain and procurement processes.

The asset management contains amongst others:

- Configuration Management System (CMS)
- Maintenance aspects
- Commercial aspects

For use within RCA, the CMS is a mainly technical service. The CMS manages the software and configuration of the assets in the context of a desired, certified, overall state. The CMS must provide a versioning system which records and provides the configuration used by the assets, their functional relationship and the regulatory application conditions. The CMS does not store software or configurations. The software and configuration is stored in the SW+Config Repository.

The CMS orchestrates configuration updates using the SW+Config Repository service to deploy software files and configuration.

The RCA subsystem DCM is supporting CMS by performing a lookup for the software and configuration version defined in and requested by the CMS. The DCM is requesting the corresponding software and configuration from the SW+Config Repository. The retrieved software and configuration are then deployed to the asset using SMI.

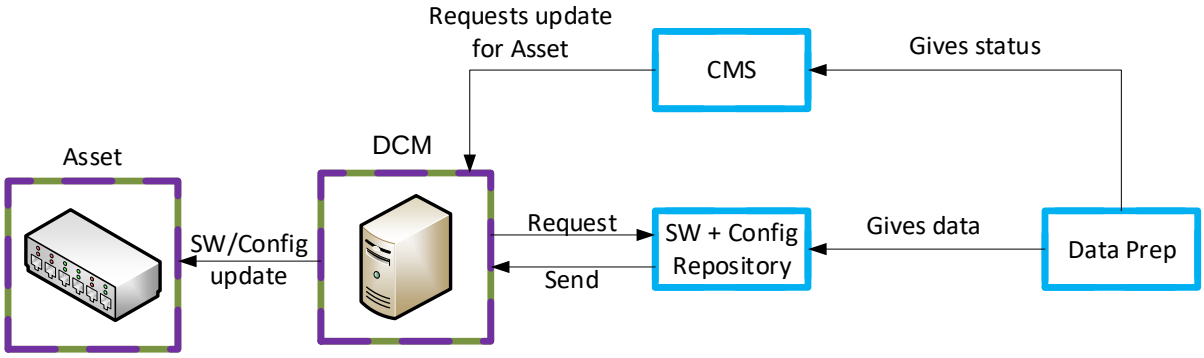

Figure 3: Asset and Configuration Management (Eu.Doc.15 [7], Eu.Sec.411 adapted)

Note: From a safety point of view, the "black channel" is starting at Data Prep and ending at the Asset (e.g. assets on the device control layer). As a result, the DCM, CMS and SW+Config Repository are not safety related, hence non-safe.

2.1.9 Software & Config Repository (REPO)

The SW+Config Repository service is an authenticated and authorised point to provide software and configuration/parameters.

This service is used by the Configuration Management Service configuration provisioning service and to other services requesting a dedicated software for a specific device. The service protects the confidentiality, integrity and non-repudiation of the software and config files in the repository. The data (software, configuration/parameters,..) are provided either by "Data Prep" or by the suppliers in another way. The files can be accessed based on access rights provided by the IAM service.

The service is only having interfaces to technical systems and is using time, IAM, PKI, SLOG, backup and Data Prep service

2.1.10 Diagnostic logging (DLOG)

The Diagnostic Logging service gathers all safety, non-safety and non-security-specific information distributed by the connected components related to diagnostic, monitoring and logging. This set of information can be used to investigate malfunctions and perform troubleshooting. Main user of this data is the monitoring service and maintenance.

This information can be provided to the SIEM to be a basis for a more profound investigation of security incidents, e.g., used by security forensics.

This service is only having interfaces to technical systems and is using time, IAM, PKI, DLOGS, SLOG and backup service.

2.1.11 Monitoring (MON)

Monitoring is part of technical operation of the overall system. It uses diagnostic/status data to create a consistent view on the operating status of all devices/subsystems/services of the overall systems.

2.1.12 Data Prep

Data Prep is the data interface between system integrator/operator/buyer and the suppliers. EULYNX specifies DataPrep as a data model based on UIC's RSM 1.2. With BL4R1 it focuses on the path buyer to supplier, aiming at improving efficiency and accuracy for planning purposes. Data Prep is a procedural service using technical services for handling of the defined data, transferred using the specified XML files.

RCA shall follow a similar but extended approach (e.g., support supplier to operator data transfer).

2.2 Modes of operation of Shared Services

Shared Security Services have the following operation states:

- service available
- service in degraded mode
- service not available

Shared Supportive Services have the following operational states:

- service available
- service not available

The following Shared Security Services have direct negative impacts in case of unavailability to the CCS operational mission:

- Time: logging (security and diagnostic) and log analysing functionality requiring exact timing may not work as expected. This might affect SIEM and therefore monitoring of security status
- IAM: communication channels may not be established, functionality may not be permitted
- PKI: Authentication may fail, authorisation may fail, and communication channels may not be established due to missing or out-dated certificate
- SIEM Timely response to events by the Security Operations Center based on the SIEM may be hindered and thus attacks might be performed successfully.

Shared Supportive Services have no direct impact on CCS operational mission as long as the unavailability does not occur within a transition e.g., configuration update.

3 Functional Overview

The following chapters give an overview of the used protocols and specifications where they can be applied.

The basis for the definitions is the EULYNX Shared Services and Platform Specification ([2], [3]).

3.1 Time (TIME) (details in Eu.Doc.117 [2])

Time synchronisation is relevant to synchronise event-based analysis and functionality.

- To synchronise time NTP is used
- The time base is UTC
- Time sources are IM stratum servers synchronised with national NTP stratum 1 servers

3.2 Security Logging (SLOG) (details in Eu.Doc.117 [2])

The Storage of log information is relevant for security

- Relevant log information can be defined by each sub system specification and IM individually as an extension to the minimum requirements.
- Central security logging service receive logging data from subsystems via:
    - OPC UA, client mode, similar to EULYNX SDI
    - Syslog
- Security logging services on subsystems shall provide logging data via:
    - OPC UA, server mode, similar to EULYNX SDI providing security logging information specified in Eu.Doc.114 [4]
    - syslog for additional logging
- Access to information on central security logging service is provided using
    - OPC UA, server mode (only data received by OPC UA), subscription of log data points based on available log level (debug, info, warning, …) or log data point (Eu.Doc.114 [4])
    - syslog: includes data received by syslog and OPC UA
- Users shall be able to request filtered data. The filtering will be done by the central security logging service.
- Authenticated and authorised access to the data based on information provided by the IAM service for the respective user (default filters).

3.3 Diagnostic Data Analytic (DDA)

Diagnostic Data Analytic (DDA) generates alarms and reports based on rule and trend analysis.

- Generate reports based on analytics, targeted at predictive maintenance
- Offers a human interface for data analytics
- Users shall be able to request filtered data. The filtering will be done by the central log storage service.
- Authenticated and authorised access to the data based on information provided by the IAM service for the respective user (default filters).

Example solutions, amongst others and without recommendation are: Splunk, Elasticsearch or Solr.

3.4 Backup (BKP) (details in Eu.Doc.117 [2])

Backup functionality provides the basis for recovering after failure or attack. Backup requirements differ from system to system. The following requirements apply generally.

- Data storage with confidentiality, integrity, and availability protection (data at rest) shall be used
- Data provided to and from the service shall be files
- Backup functionality manages full, differential, and incremental backup: initiating, storing, keep their relation, create file set for restore, …
- Back up services provides orchestrating and triggering of backup procedures according to backup plan and providing all required information to perform the backup, especially for incremental/differential backups
- Back up services provides monitoring of backup process, alarm in case of failure
- Back up services shall be able to cancel an already initiated or running backup
- Back up services shall only allow authenticated and authorised access using IAM service
- Back up services shall provide a backup file/package for restore or retention/archival for a defined backup (system, time, …). This includes all files required especially for incremental backups.
- Back up services shall provide mechanisms to ensure confidentiality and integrity protection for data in transit, e.g., during transfer of the file to the centralized backup service
- Backups shall be removed automatically according to the backup plan
- Back up services provides functionality to manage backup plans
- Back up services provides functionality to manage backup service (e.g., define systems to be processed, backup service parameters and procedures for these systems, …

3.5 Identity and Access Management (IAM) (details in Eu.Doc.117 [2])

The IAM is consolidating multiple sources of information to support access management functionality.

- Asset Management process provides information on assets (ID, functional role/capability, supplier…) either using technical interface (e.g., SAP) or manual entry (e.g., bill of material after delivery)
- Human Resource Management process provides information on people (person, role within organisation…) either using technical interface (e.g., LDAP) or procedural (e.g., manual entry)
- Ensures management of the digital identity (proof of identity, create identity, grant & revoke permission to an identity, archive identity) incl. history/audit-trail
- Management of profiles for roles/permissions/capabilities Reporting / monitoring to detect non-met profile Provides authorisation service:
    - Provides authorisation tokens (OAuth2-Tokens)
- Supports authentication using
    - OpenID Connect
    - Supports multi-factor authentication schemas for authenticating humans

3.6 Public Key Infrastructure (PKI) (details in Eu.Doc.117 [2])

A Public Key Infrastructure (PKI) provides digital identity for each relevant entity (e.g., all identities of IAM)

- The PKI and the using entities shall implement Certificate Management Protocol (CMP) according to RFC 4210 and RFC 4211, on HTTP (RFC 6712)
- The PKI and the using entities shall implement the X.509 protocol and CRL in accordance with RFC 5280.
- The PKI and the using entities shall implement Implements ACME protocol (RFC 8555) using an automated challenge integrating IAM service on HTTPS.
- The following processes shall be available and used:
    - Request a certificate
        - without another certificate (e.g., blank first-time setup) (initialisation request & response)
        - with another certificate (supplier, operator, …) (certification request & response)
    - Renew a certificate
        - with a valid certificate from the PKI service (certification request & response)
    - Revoke a certificate
    - Validate a certificate
- The PKI shall interact with Identity and Access Management (IAM):
    - IAM ensures the correct relation of the real entity to its digital identity.
    - IAM interacts with ACME service.
    - IAM is updated on new and revoked certificates. This shall be possible using CMP (certification announcement) or certificate transparency.
- The PKI shall interact with Certificate Management System:
    - Certificate Authority
    - Registration Authority
- The PKI shall interact with Validation Authority
    - Certificate Revocation List (CRL) Server (RFC 5280)
        - as HTTP download
        - as HTTPS download
- OCSP Responder (RFC 6960)

3.7 Security Incident and Event Management (SIEM)

Security Incident and Event Management (SIEM) provides analytical functionality to detect potential security incidents. It is usually integrated in a Security Operations Centre (SOC) environment.

- The SIEM shall provide alarming functionality to trigger human action
- The SIEM shall provide auto-react functionality to trigger other technical systems
- The SIEM shall not automatically react on OT systems directly to avoid attack vectors that address decrease of availability or restart functionalities of any entities.
- The SIEM shall provide a ticket system to manage incidents and events
- The SIEM service uses time, security logging, diagnostic logging, IAM, PKI and backup services

3.8 Asset Management (AM)

3.8.1 Asset Management - Asset Inventory (AM-INV)

- Interacts with Life-Cycle Managers
- Interacts with maintenance personnel (maintenance, replacement)
- Interacts with build projects (import/create assets to be managed)
- Interacts with IAM (basic data for identity, decommissioning of asset)
- Supports maintenance activities
- Provides technical, commercial and supply chain data based on authentication and authorisation based on IAM service
- Documents physical (e.g., location) and high-level logical (e.g., EIL area) context of asset
- Provide Configuration Management System (CMS)

3.8.2 Asset Management - Configuration Management System (AM-CFG)

- Orchestrating MDM for software and configuration changes, ensuring compliance with safety regulation/certificates (Configuration Management System (CMS)
- Interacts with processes/systems supporting change (systems to support service management)
- Interacts with the MDM
- Uses the Software & Configuration Repository service (REPO)
- Implements Configuration Management Data Base (CMDB)
- Implements or interacts with service for valid configuration combinations with respect to safety regulation/certificates and operator specific homologation.

3.9 Software & Configuration Repository (REPO)

- Data storage with confidentiality, integrity, and non-repudiation protection
- Authenticated and authorised access to the data using IAM service
- Interacts with supply chain security process for software and configuration data
- Interacts with “Data Prep” / ”Data Prep service” to process new or changed configuration data

Note: Signing software or configuration data is performed outside this service. Validating signatures is done outside this service.

3.10 Diagnostic logging (DLOG)

- Collecting data from different sources, e.g., MDM diagnostic data store, in a timely manner
- Authenticated and authorised access to the data using IAM service
- Diagnostic logging uses time, IAM and backup service

3.11 Monitoring (MON)

- Collecting data from different sources, e.g., diagnostic service or MDM monitoring data store, in a timely manner provides user interface for operation management / monitoring of technical services
- Authenticated and authorised access to the data using IAM service
- Diagnostic logging uses time and IAM service

3.12 Data Prep

- Provide data interface to suppliers
- Imports data using the data prep format into IMs asset management systems/services and into the software & configuration repository