EU-RAIL SYSTEM PILLAR

Migration Guideline

Migration Guideline

Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address:
cybersecurity.review@ertms.be

Review by reviewers

Type of Approval	Document Review

Review by approvers

Type of Approval	✓ Document Approval

1 Table of Contents

2 Preamble

2.1 Scope, Purpose and Intended Audience

🗎**, SP-SEC-MigGuide-2.1-1 -** This guideline supports the usage of the ERJU System Pillar Cybersecurity Specifications together with the application of the CCS TSI 2023. **[**SPPRAMSS-14973 **]**

🗎**, SP-SEC-MigGuide-2.1-2 -** The guideline allows to implement all technical and procedural requirements of the ERJU System Pillar Cybersecurity Specifications in parallel to the compliant application of CCS TSI 2023. **[**SPPRAMSS-14994 **]**

🗎**, SP-SEC-MigGuide-2.1-3 -** For this purpose, the guideline describes the to be applied solutions or chooses variants - where applicable - to allow compliance to both specifications. **[**SPPRAMSS-14993 **]**

2.2 Document Usage

🗎**, SP-SEC-MigGuide-2.2-1 -** This guideline uses identifiers starting with "SP-SEC-MigGuide". **[**SPPRAMSS-14987 **]**

🗎**, SP-SEC-MigGuide-2.2-2 -** Icon types used in this document are defined in [SP-SEC-Tax]. **[**SPPRAMSS-14988 **]**

2.3 References

🗎**, SP-SEC-MigGuide-2.3-1 -** This chapter contains all references of this document. For a complete list including external references see [SP-SEC-Tax] Chapter 3. **[**SPPRAMSS-14985 **]**

[UNISIG SUBSET-147 v4.00]
CCS Consist network communication layer, V4.0

[UNISIG SUBSET-137 v4.00]
ETCS On-line Key Management, v4.0

[UNISIG Subset-26 v4.00]
ETCS System Requirements Specification

[SP-SEC-PrgmReq]
Europe's Rail System Pillar Cybersecurity Domain - Secure Program Requirements, v1.1

[SP-SEC-CompSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.1

[SP-SEC-CommSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Commmunication Specification, v1.1

[SP-SEC-ServSpec]
Europe's Rail System Pillar Cybersecurity Domain - Shared Cybersecurity Services Interface Specification, v1.1

[RFC 9483]
Lightweight Certificate Management Protocol (CMP) Profile

[UNISIG SUBSET-146 v4.00]
ERTMS End-to-End security layer (TLS layer for ETCS and ATO communication), v4.0

2.4 Terms and Definitions

Shared Cybersecurity Services

A collection of standard security interfaces (SSIs) of central security functions accessible for all Secure

Components in the automation solution. The realization of the Shared Cybersecurity Services (SCS) implements the requirements of the Secure Component Specification as they are considered as Secure Components as well.

The interfaces from Secure Components to Shared Cybersecurity Service are identified by SSI-<service name>.

The Shared Cybersecurity Services implementations are identified by SCS-<service name>. **[**SPPRAMSS-1446 **]**

2.5 Modification History

, **SP-SEC-MigGuide-2.5-1 -** First version (V1.0) - October 2025 **[**SPPRAMSS-15674 **]**

3 Guideline

3.1 ERTMS Architecture

3.1.1 Issue description

, **SP-SEC-MigGuide-3.1.1-1 -** With the [SP-SEC-ServSpec] new interfaces are introduced which are not shown in the ERTMS architecture overview in Subset 026-2. That could transfer the impression that the new interfaces are not compatible with the ERTMS subsets. This impression is not correct and shall be solved by the guidance in this chapter. **[**SPPRAMSS-15005 **]**

, **SP-SEC-MigGuide-3.1.1-2 -** In addition, existing services were available in the Subsets already but not shown in the architecture. **[**SPPRAMSS-15009 **]**

📄, **SP-SEC-MigGuide-3.1.1-3 -**

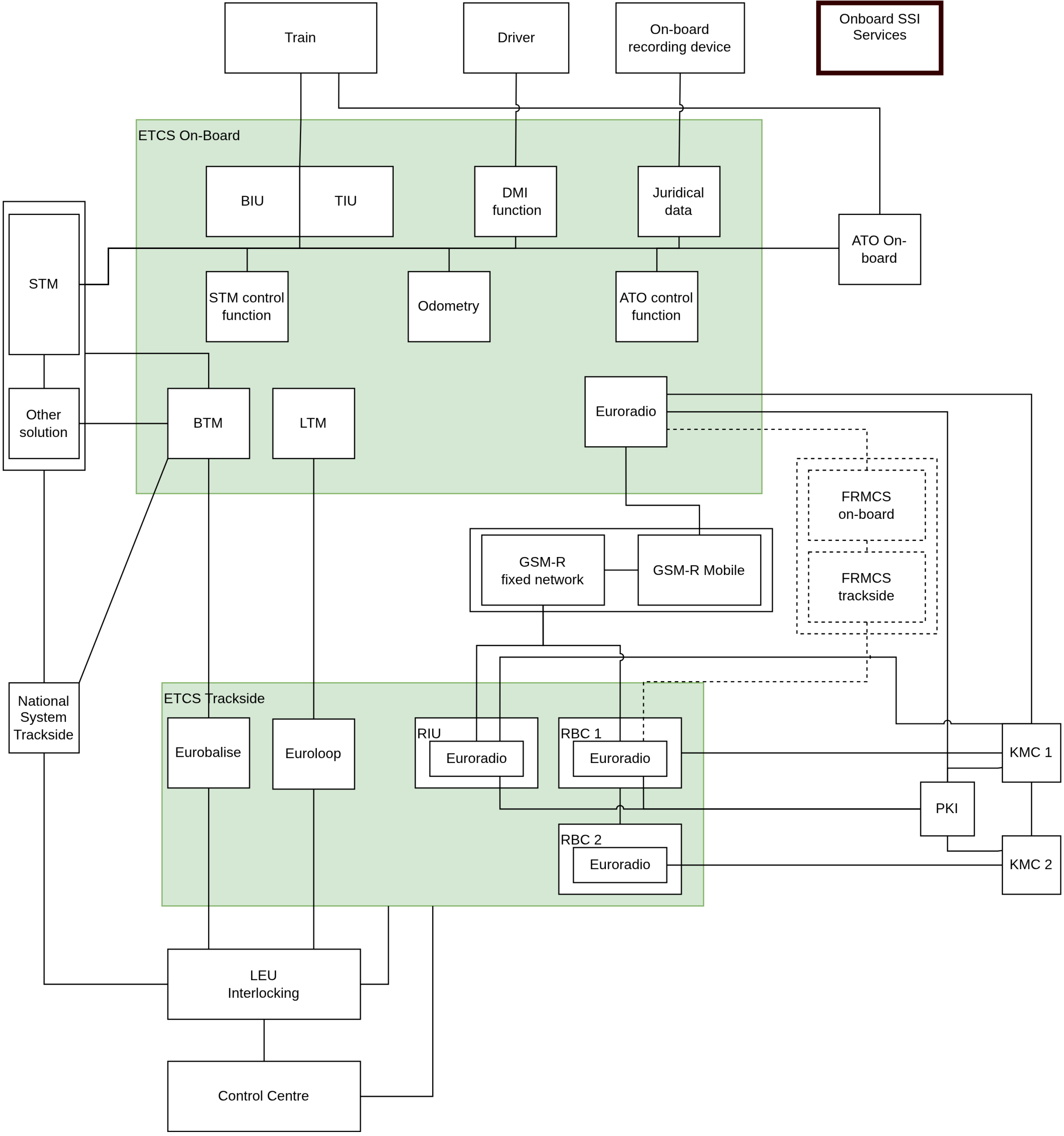

Figure 1 ERTMS architecture without SCS

[SPPRAMSS-15021 **]**

3.1.2 Affected System, components or interfaces

📄, **SP-SEC-MigGuide-3.1.2-1 -** The whole ERTMS architecture is affected. **[**SPPRAMSS-15004 **]**

3.1.3 Guidance

📄, **SP-SEC-MigGuide-3.1.3-1 -** The architecture shows the existing and improved interfaces in light green. **[**SPPRAMSS-15008 **]**

, SP-SEC-MigGuide-3.1.3-2 - The architecture shows the new interfaces by the [SP-SEC-ServSpec] in dark green. **[**SPPRAMSS-15010 **]**

, SP-SEC-MigGuide-3.1.3-3 -

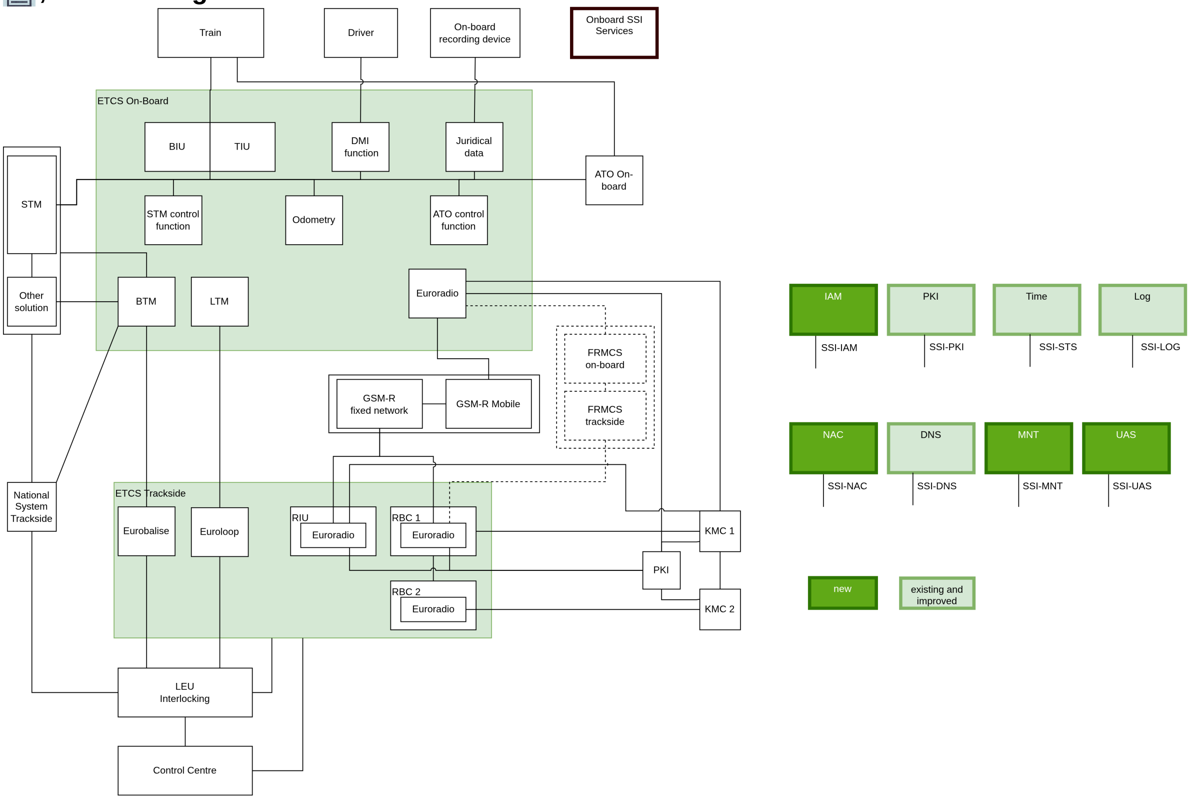

Figure 2 ERTMS architecture with SCS

[SPPRAMSS-15011 **]**

, SP-SEC-MigGuide-3.1.3-4 - The Shared Cybersecurity Services (SCS) can be made available in the system by installing them and making them reachable in the communication network. **[**SPPRAMSS-15006 **]**

, SP-SEC-MigGuide-3.1.3-5 - Each element of the ERTMS (including FRMCS) system may have access to these services by connecting to the SCS using the defined interfaces SSI-xx. **[**SPPRAMSS-15007 **]**

, SP-SEC-MigGuide-3.1.3-6 - No incompatibilities are driven by the integration of the new interfaces of SCS. **[**SPPRAMSS-15022 **]**

3.2 CRL vs OCSP certificate handling

3.2.1 Issue description

, SP-SEC-MigGuide-3.2.1-1 - The [SP-SEC-ServSpec] requires the usage of CRL only for certificate handling at server and client side. **[**SPPRAMSS-15088 **]**

, SP-SEC-MigGuide-3.2.1-2 - In contrast, the [UNISIG SUBSET-137 v4.00] and [UNISIG SUBSET-146 v4.00] require OCSP for Certificate handling for the Online Key Management. **[**SPPRAMSS-15097 **]**

📄**, SP-SEC-MigGuide-3.2.1-3 -** In addition [SP-SEC-ServSpec] on one hand, and [UNISIG SUBSET-137 v4.00] and [UNISIG SUBSET-146 v4.00] on the other hand, require slightly different certificate profiles. **[**SPPRAMSS-15100 **]**

📄**, SP-SEC-MigGuide-3.2.1-4 -** Strict implementation of the [SP-SEC-ServSpec] would cause incompatibility. **[**SPPRAMSS-15096 **]**

3.2.2 Affected System, components or interfaces

📄**, SP-SEC-MigGuide-3.2.2-1 -** The described incompatibility affects the Online Key Management between RBC, EVC and KMC. **[**SPPRAMSS-15094 **]**

3.2.3 Guidance

📄**, SP-SEC-MigGuide-3.2.3-1 -** The PKI shall offer the OCSP responder as long as there is Online Key Management (including BL4R1), which requests an OCSP responder. **[**SPPRAMSS-15092 **]**

📄**, SP-SEC-MigGuide-3.2.3-2 -** To solve the conflict of different certificate profiles, different solutions are possible. For this reason, the KMS guideline (EUG document 23E064) will be updated to provide best practices. The flexibility is provided through the PKI services. **[**SPPRAMSS-15099 **]**

📄**, SP-SEC-MigGuide-3.2.3-3 -** The solution does not hinder going to tender with the combination of the TSI subsets and the ERJU System Pillar Cybersecurity Specifications. As the flexibility considering the certificate profiles is provided by PKI service, the Subset definitions are not affected. **[**SPPRAMSS-15101 **]**

📄**, SP-SEC-MigGuide-3.2.3-4 -** The PKI shall be capable of managing different certificate profiles
Note: This is a standard capability of PKI services. **[**SPPRAMSS-15102 **]**

3.3 Responsibility of Railways considering Shared Cybersecurity Services

3.3.1 Issue description

📄**, SP-SEC-MigGuide-3.3.1-1 -** The [SP-SEC-ServSpec] does not specify who is responsible to provide the Shared Cybersecurity Services. **[**SPPRAMSS-15103 **]**

📄**, SP-SEC-MigGuide-3.3.1-2 -** Where railway infrastructure managers usually take it automatically as their responsibility, railway undertakings, especially smaller ones, are often unaware of this challenge. **[**SPPRAMSS-15114 **]**

📄**, SP-SEC-MigGuide-3.3.1-3 -** To avoid uncertainty, a definition shall be provided. **[**SPPRAMSS-15112 **]**

3.3.2 Affected System, components or interfaces

📄**, SP-SEC-MigGuide-3.3.2-1 -** All Shared Cybersecurity Services are affected. **[**SPPRAMSS-15109 **]**

3.3.3 Guidance

📄**, SP-SEC-MigGuide-3.3.3-1 -** The railway is responsible in providing the Shared Cybersecurity Services in their network to allow the operation of the secure components developed and delivered based on the ERJU System Pillar Cybersecurity Specifications.
Hint: Additional services, like Vulnerability management, Asset management, Config Management need to be available to efficiently

manage the secure components over the life-cycle. All the relevant services are required through the European legislation (NIS2) already. **[**SPPRAMSS-15111 **]**

📄**, SP-SEC-MigGuide-3.3.3-2 -** The Shared Cybersecurity Services may be operated by third party. The strategic decision lays with the railways. **[**SPPRAMSS-15113 **]**

3.4 DMI

3.4.1 Issue description

📄**, SP-SEC-MigGuide-3.4.1-1 -** Some railway suppliers are uncertain whether DMIs need to fulfill the ERJU System Pillar Cybersecurity Specifications. **[**SPPRAMSS-15115 **]**

📄**, SP-SEC-MigGuide-3.4.1-2 -** To allow common interpretation a clear definition shall apply. **[**SPPRAMSS-15123 **]**

3.4.2 Affected System, components or interfaces

📄**, SP-SEC-MigGuide-3.4.2-1 -** The onboard DMI is affected. **[**SPPRAMSS-15121 **]**

3.4.3 Guidance

📄**, SP-SEC-MigGuide-3.4.3-1 -** If the DMI is connected to any train-borne network, the [SP-SEC-CompSpec] applies to the DMI. **[**SPPRAMSS-15018 **]**

📄**, SP-SEC-MigGuide-3.4.3-2 -** If the DMI is connected directly to a Secure Component without own connection to any train-borne network, the [SP-SEC-CompSpec] does not apply to the DMI. **[**SPPRAMSS-15124 **]**

📄**, SP-SEC-MigGuide-3.4.3-3 -** If the DMI is connected directly to a Secure Component without own connection to any train-borne network, the Secure Component the DMI is connected to shall be treated as "Component with HMI" according to SP-SEC-Comp Chapter 7.2 - Components with HMIs. **[**SPPRAMSS-15125 **]**

, SP-SEC-MigGuide-3.4.3-4 - The following figure shows the two different variants.

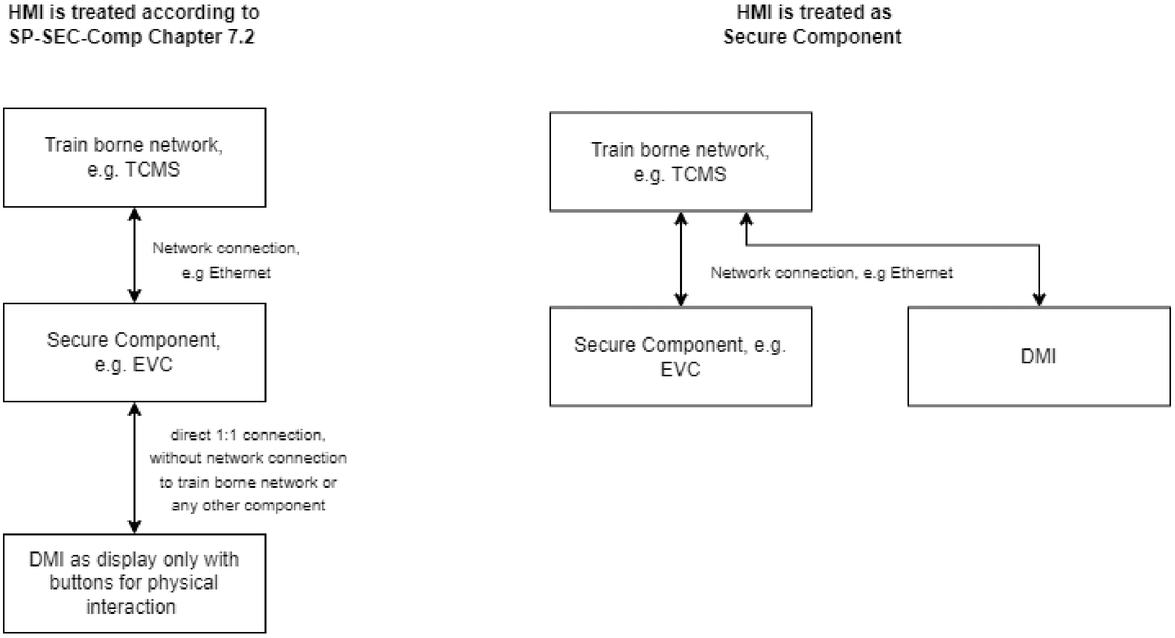
HMI is treated according to SP-SEC-Comp Chapter 7.2
HMI is treated as Secure Component
Train borne network, e.g. TCMS
Network connection, e.g Ethernet
Secure Component, e.g. EVC
direct 1:1 connection, without network connection to train borne network or any other component
DMI as display only with buttons for physical interaction
Train borne network, e.g. TCMS
Network connection, e.g Ethernet
Secure Component, e.g. EVC
DMI

Figure 3 DMI implementation variants

[SPPRAMSS-16034 **]**

3.5 Train driver identification and authentication

3.5.1 Issue description

, SP-SEC-MigGuide-3.5.1-1 - The [SP-SEC-CompSpec] and [SP-SEC-PrgmReq] require a user identification and authentication for every HMI. **[**SPPRAMSS-15126 **]**

, SP-SEC-MigGuide-3.5.1-2 - Currently, no driver identification and authentication is defined or available to identify the train driver. This leaves identified cybersecurity risks unmitigated. **[**SPPRAMSS-15141 **]**

, SP-SEC-MigGuide-3.5.1-3 - The main challenge is to agree on an overall procedure that does not hinder daily train operation. **[**SPPRAMSS-15140 **]**

, SP-SEC-MigGuide-3.5.1-4 - References in [SP-SEC-PrgmReq] :
SPPRAMSS-12209 - If systems and components implement a Human Machine interface, the railway shall...
SPPRAMSS-13041 - The railway shall ensure that every user (human users, software processes or dev...
SPPRAMSS-12240 - If a human access is available, multi factor authentication for the human users...
[SPPRAMSS-15139 **]**

3.5.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.5.2-1 - The affected systems onboard the train are at minimum:

- ETCS-DMI (CCD)
- GSM-R Display
- Electronic Time Display

- Diagnostic Display (TDD)

[SPPRAMSS-15131 **]**

, SP-SEC-MigGuide-3.5.2-2 - Potential affected systems are the doors to access the driver cabin. **[**SPPRAMSS-15142 **]**

3.5.3 Guidance

, SP-SEC-MigGuide-3.5.3-1 - To allow "Single sign on" onboard the train for the train driver the technical solution shall make use of the user authentication service (SCS-UAS) to manage the access rights. **[**SPPRAMSS-15130 **]**

, SP-SEC-MigGuide-3.5.3-2 - The SCS-UAS shall be installed as a service onboard the train and connected to the relevant HMIs. **[**SPPRAMSS-15143 **]**

, SP-SEC-MigGuide-3.5.3-3 -

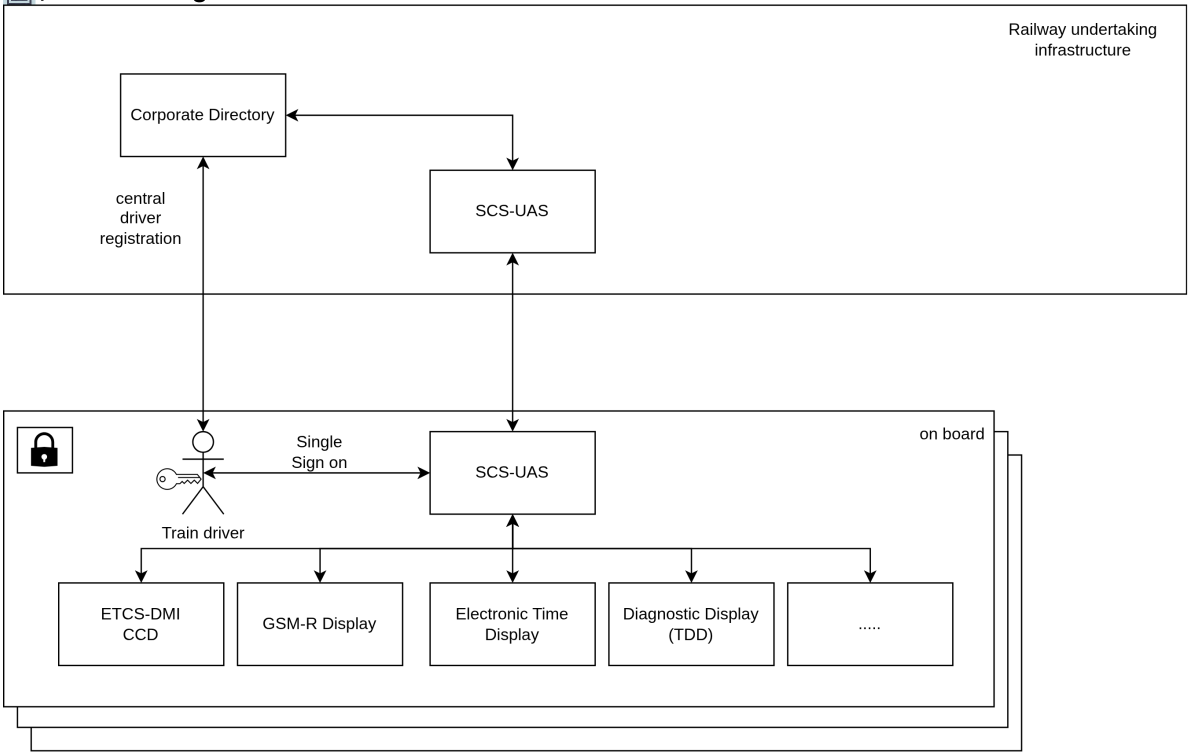

Figure 4 Train driver authentication

[SPPRAMSS-15135 **]**

, SP-SEC-MigGuide-3.5.3-4 - The train driver shall have a physical device, e.g. a key card, with his personal credentials. **[**SPPRAMSS-15136 **]**

, SP-SEC-MigGuide-3.5.3-5 - The SCS-UAS locally on the train shall have a copy of the access rights downloaded, so it can authenticate without network connection. **[**SPPRAMSS-15133 **]**

, SP-SEC-MigGuide-3.5.3-6 - For the authentication the main criteria is "train driver". So if the card holder has a card for a train driver, he/she can access basically every train. **[**SPPRAMSS-15134 **]**

, SP-SEC-MigGuide-3.5.3-7 - As a second check, the allowed train category, train owner and personal rights can be checked. In case of no updated offline list, the fall-back always is "train driver". **[**SPPRAMSS-15137 **]**

, SP-SEC-MigGuide-3.5.3-8 - The driver authentication shall also apply to access the driver cabinet. **[**SPPRAMSS-15138 **]**

, SP-SEC-MigGuide-3.5.3-9 - To proceed and standardise an alignment with Train CS is required. In this context, the following definitions need to be described at minimum:
- Degraded mode, e.g. via mobile phone.
- Standardisation of the physical device, e.g. rfid chip/card, mobile phone, nfc, etc.
- The operational process to allow company internal and with external participation the handling of the access **[**SPPRAMSS-15269 **]**

, SP-SEC-MigGuide-3.5.3-10 - Note: So far, the following companies/organisation are supporting this approach:
- EUG
- SNCF (using it already for latest train generations)
- NS **[**SPPRAMSS-15270 **]**

3.6 TLS version management

3.6.1 Issue description

, SP-SEC-MigGuide-3.6.1-1 - The [SP-SEC-CommSpec] requires the use of TLS 1.3. Older versions are not allowed. **[**SPPRAMSS-15012 **]**

, SP-SEC-MigGuide-3.6.1-2 - The CCS TSI 2016, 2019 and 2023, through their Subsets 137 and 146, use non-TLS, TLS 1.2 and TLS 1.3 connections. **[**SPPRAMSS-15155 **]**

, SP-SEC-MigGuide-3.6.1-3 - In addition, the related ciphers differ through the different versions of the TSIs. **[**SPPRAMSS-15157 **]**

, SP-SEC-MigGuide-3.6.1-4 - As the different TLS versions are not compatible with each other, it needs to be defined how the systems shall interact with each other. **[**SPPRAMSS-15158 **]**

3.6.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.6.2-1 - The affected systems are:

- Euroradio (RBC-EVC)
- ATO (ATO TS - ATO OB)
- Online Key Management (KMC-RBC, KMC-EVC)

[SPPRAMSS-15020 **]**

3.6.3 Guidance

, SP-SEC-MigGuide-3.6.3-1 - For ETCS, no backwards incompatibility issues exist, because TLS usage depends on radio bearer (5G or GSM). Only with 5G TLS is used. In this case [UNISIG SUBSET-146 v4.00] defines the usage of TLS 1.3.
So, as long as 5G is not used, no security layer is used.
The moment 5G is used, TLS 1.3 is used to protect the communication. **[**SPPRAMSS-15154 **]**

, SP-SEC-MigGuide-3.6.3-2 - For ATO, no backwards incompatibility issues exist, as ATO shall use only TLS 1.3 from TSI 2023 onwards.
Information: TLS 1.2 is only allowed for backwards compatibility. As no "old" TSI specifications for ATO exist, no backwards compatibility is required or used. **[**SPPRAMSS-15152 **]**

, SP-SEC-MigGuide-3.6.3-3 - For online key management (KMC-RBC, KMC-EVC), no backwards incompatibility issue exists, as online key management shall support TLS 1.2 and 1.3 from TSI 2023 onwards. **[**SPPRAMSS-15153 **]**

, SP-SEC-MigGuide-3.6.3-4 - For KMC-KMC connection, no backwards incompatibility issue exists, as online key management shall support TLS 1.2 and 1.3 from TSI 2023 onwards. So, every "new" (TSI 2023) KMC supports connection to "old" (TSI 2019) KMC. **[**SPPRAMSS-15335 **]**

3.7 Use of pre-shared keys with certificates

3.7.1 Issue description

, SP-SEC-MigGuide-3.7.1-1 - KMC-EVC and KMC-RBC connections using preshared keys for the TLS connection instead of certificates may exist based on TSI 2019 and older. **[**SPPRAMSS-15166 **]**

, SP-SEC-MigGuide-3.7.1-2 - The [SP-SEC-CommSpec] and TSI 2023 only allow the application of certificate based TLS for new systems. **[**SPPRAMSS-15168 **]**

, SP-SEC-MigGuide-3.7.1-3 - In TSI 2023, [UNISIG SUBSET-146 v4.00] allows the usage of pre-shared key inside one KM-domain for backwards compatibility only. **[**SPPRAMSS-15169 **]**

, SP-SEC-MigGuide-3.7.1-4 - To avoid misinterpretation and allow compatibility between different versions, a clear definitions is required. **[**SPPRAMSS-15167 **]**

, SP-SEC-MigGuide-3.7.1-5 - Reference in [SP-SEC-CommSpec]: SPPRAMSS-2030 - The TLS endpoint shall perform authentication using certificates in accordance w... **[**SPPRAMSS-15170 **]**

3.7.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.7.2-1 - The following systems are affected:

- EVC
- RBC
- KMC

[SPPRAMSS-15160 **]**

3.7.3 Guidance

, SP-SEC-MigGuide-3.7.3-1 - For Online Key Management, [UNISIG SUBSET-146 v4.00] allows the usage of pre-shared keys inside one KM-domain for backwards compatibility to Subset 137 only. So, if a railway has already implemented pre-shared key based TLS connections in its KM-domain, the new installations are allowed to support this for backwards compatibility. **[**SPPRAMSS-15165 **]**

, SP-SEC-MigGuide-3.7.3-2 - For new implementations and for KMS-KMS communications, the use of pre-shared keys is prohibited.

Explanation: This is the resulting combination of "not recommended" of Subset 146 4.3.1.11 and the clear requirement to only use certificates from the ERJU System Pillar Cybersecurity Specifications. [SPPRAMSS-15172]

, **SP-SEC-MigGuide-3.7.3-3 -** This means that, for every new implementation, certificate-based authentication is foreseen, so there is no incompatibility between [UNISIG SUBSET-146 v4.00] and the ERJU System Pillar Cybersecurity Specifications. **[**SPPRAMSS-15171 **]**

3.8 Euroradio and Chapter 6 of SP-SEC-Comm

3.8.1 Issue description

, **SP-SEC-MigGuide-3.8.1-1 -** The SP-SEC-CommSpec Chapter 6 - Securing other Communicating Interfaces defines the security for other interfaces than specified in the respective specification. **[**SPPRAMSS-15174 **]**

, **SP-SEC-MigGuide-3.8.1-2 -** Euroradio would fall on these "other" interfaces. But Euroradio cannot apply these requirements. **[**SPPRAMSS-15182 **]**

3.8.2 Affected System, components or interfaces

, **SP-SEC-MigGuide-3.8.2-1 -** The affected system is the Euroradio interface between RBC and EVC. **[**SPPRAMSS-15181 **]**

3.8.3 Guidance

, **SP-SEC-MigGuide-3.8.3-1 -** For Euroradio, the SP-SEC-CommSpec Chapter 6 - Securing other Communicating Interfaces shall not be applied. **[**SPPRAMSS-15179 **]**

3.9 Use of NTS and NTP

3.9.1 Issue description

, **SP-SEC-MigGuide-3.9.1-1 -** The [SP-SEC-ServSpec] requires the use of NTS for time synchronisation. The CCS TSI 2023 and earlier require the use of NTP for time synchronisation. **[**SPPRAMSS-15271 **]**

, **SP-SEC-MigGuide-3.9.1-2 -** It needs to be defined, how this inconsistency shall be managed. **[**SPPRAMSS-15279 **]**

3.9.2 Affected System, components or interfaces

, **SP-SEC-MigGuide-3.9.2-1 -** All CCS systems are affected. **[**SPPRAMSS-15276 **]**

3.9.3 Guidance

, **SP-SEC-MigGuide-3.9.3-1 -** NTS and NTP can be operated in parallel. NTS servers by default provide the simple NTP data on a different port. The railway only need to ensure that clients are configured to use the applicable port. No conflict or additional security risk for NTS clients arises from this parallel operation.
Reference in [SP-SEC-ServSpec]: SPPRAMSS-6707 - NTS is backwards compatible to NTP. That means an NTP client can synchronize wit... **[**SPPRAMSS-15278 **]**

, SP-SEC-MigGuide-3.9.3-2 - The railway shall ensure that NTP client requests without NTS extension are accepted and answered by the NTS server. **[**SPPRAMSS-15281 **]**

, SP-SEC-MigGuide-3.9.3-3 - The railway shall ensure that a NTS server is available with the first installation based on [SP-SEC-ServSpec]. **[**SPPRAMSS-15280 **]**

3.10 Certificate profiles with different ETCS baselines

3.10.1 Issue description

, SP-SEC-MigGuide-3.10.1-1 - The [SP-SEC-ServSpec] requires the use of elliptic curves for certificates. **[**SPPRAMSS-15285 **]**

, SP-SEC-MigGuide-3.10.1-2 - Some ETCS baselines do not support the use of elliptic curves. **[**SPPRAMSS-15296 **]**

, SP-SEC-MigGuide-3.10.1-3 - Clarification is needed where this issue occurs and how it can be resolved. **[**SPPRAMSS-15298 **]**

, SP-SEC-MigGuide-3.10.1-4 - References in [SP-SEC-ServSpec]:
SPPRAMSS-10177 - All certificates in the PKI hierarchy shall be based on Elliptic Curve Cryptogra...
SPPRAMSS-7494 - The PKI RA/CA shall support the following protection algorithms for creating sig...
SPPRAMSS-7496 - The SSI-PKI client shall sign CMP requests by using ecdsa-with-sha256 as protect...
SPPRAMSS-7495 - The PKI client shall support the following protection algorithms for creating si...
[SPPRAMSS-15299 **]**

3.10.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.10.2-1 - The following interfaces may be affected:

- Euroradio (RBC-EVC)
- ATO
- Online Key Management (RBC-KMS and EVC-KMS)

[SPPRAMSS-15283 **]**

3.10.3 Guidance

, SP-SEC-MigGuide-3.10.3-1 - For Euroradio (RBC-EVC) TLS 1.3 is mandatory according to Subset 146 in combination with FRMCS. As Subset 146 is introduced with B4R1 and B4R1 is only compatible with B4R1 no incompatibility concerning elliptic curves and TLS version may arise on this interface. **[**SPPRAMSS-15293 **]**

, SP-SEC-MigGuide-3.10.3-2 - For ATO TLS 1.3 is mandatory according to Subset 146. As Subset 146 is introduced with B4R1 and B4R1 3.0 is only compatible with B4R1 no incompatibility concerning elliptic curves and TLS version may arise on this interface. **[**SPPRAMSS-15291 **]**

, SP-SEC-MigGuide-3.10.3-3 - For the RBC-KMS and EVC-KMS interface, the incompatibility between TLS 1.2 and TLS 1.3 may occur. This can be solved by providing backwards compatibility on the KMS side. **[**SPPRAMSS-15292 **]**

, SP-SEC-MigGuide-3.10.3-4 - Note: The update of the KMS is required before the implementation of RBC or EVC if an existing KMS (supporting BL 3) shall be used with new RBC or EVC of BL 4. **[**SPPRAMSS-16036 **]**

, SP-SEC-MigGuide-3.10.3-5 - The KMS shall implement TLS 1.3 and in parallel TLS 1.2 for backwards compatibility. **[**SPPRAMSS-15289 **]**

, SP-SEC-MigGuide-3.10.3-6 - The KMS shall implement RSA for the use within TLS 1.2 for backwards compatibility only. **[**SPPRAMSS-15290 **]**

, SP-SEC-MigGuide-3.10.3-7 - The EVC shall implement TLS 1.3 for the EVC-KMS connection. **[**SPPRAMSS-15294 **]**

, SP-SEC-MigGuide-3.10.3-8 - The RBC shall implement TLS 1.3 for the RBC-KMS connection. **[**SPPRAMSS-15295 **]**

3.11 Use of NAC

3.11.1 Issue description

, SP-SEC-MigGuide-3.11.1-1 - NAC is required by the ERJU System Pillar Cybersecurity Specifications. It is not allowed to be turned off. **[**SPPRAMSS-15303 **]**

, SP-SEC-MigGuide-3.11.1-2 - NAC is not required for most of the systems following the existing CCS TSI subsets, except [UNISIG SUBSET-147 v4.00]. **[**SPPRAMSS-15331 **]**

, SP-SEC-MigGuide-3.11.1-3 - A component that does not support NAC cannot access a network that requires NAC. **[**SPPRAMSS-15333 **]**

, SP-SEC-MigGuide-3.11.1-4 - A components that enforces to use NAC can only connect to networks that support NAC. **[**SPPRAMSS-15332 **]**

3.11.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.11.2-1 - All components of CCS TSI. **[**SPPRAMSS-15330 **]**

3.11.3 Guidance

, SP-SEC-MigGuide-3.11.3-1 - NAC is not used for ETCS baselines. The only exception is [UNISIG SUBSET-147 v4.00] for onboard communication. **[**SPPRAMSS-15306 **]**

, SP-SEC-MigGuide-3.11.3-2 - Thus there is no incompatibility between onboard and trackside by requiring the NAC capability. **[**SPPRAMSS-15324 **]**

, SP-SEC-MigGuide-3.11.3-3 - For onboard, no incompatibility exists because it already requires the use of NAC of all participants. **[**SPPRAMSS-15325 **]**

, SP-SEC-MigGuide-3.11.3-4 - IF a network is already using NAC, the railway shall ensure that NAC is deactivated for ports where ETCS components not supporting NAC need to communicate. **[**SPPRAMSS-15322 **]**

, SP-SEC-MigGuide-3.11.3-5 -
For secure components, the railway shall ensure that the access switch supports NAC.
Note: An unsecure configuration, like turning off NAC, is prohibited for secure components.
[SPPRAMSS-15323 **]**

3.12 Syslog message formats

3.12.1 Issue description

, SP-SEC-MigGuide-3.12.1-1 - [UNISIG SUBSET-146 v4.00] has defined different syslog messages than the ERJU System Pillar Cybersecurity Specifications. **[**SPPRAMSS-15319 **]**

3.12.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.12.2-1 - All components of CCS TSI. **[**SPPRAMSS-15329 **]**

3.12.3 Guidance

, SP-SEC-MigGuide-3.12.3-1 - If differences between syslog message formats occur, the railway shall adapt the rule sets in the SIEM (server side) so they can be managed. **[**SPPRAMSS-15326 **]**

3.13 Use of DNS

3.13.1 Issue description

, SP-SEC-MigGuide-3.13.1-1 - The CCS TSI for ETCS define the use of DNS for IP based communication. **[**SPPRAMSS-15309 **]**

, SP-SEC-MigGuide-3.13.1-2 - In the ERJU System Pillar Cybersecurity Specifications, DNS over TLS is required by the [SP-SEC-ServSpec].
[SPPRAMSS-15327 **]**

3.13.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.13.2-1 - All components of CCS TSI. **[**SPPRAMSS-15311 **]**

3.13.3 Guidance

, SP-SEC-MigGuide-3.13.3-1 - To allow compatibility between older versions (based on [UNISIG SUBSET-146 v4.00]) and new systems (based on ERJU System Pillar Cybersecurity Specifications), the DNS servers shall offer DNS and DNS over TLS. **[**SPPRAMSS-15308 **]**

, SP-SEC-MigGuide-3.13.3-2 - If systems requiring DNS (without TLS) are operated, the railway shall provide DNS servers that provide DNS and DNS over TLS. **[**SPPRAMSS-15328 **]**

3.14 Use of pre-shared keys with certificates

3.14.1 Issue description

, SP-SEC-MigGuide-3.14.1-1 - [UNISIG SUBSET-146 v4.00] allows for Certificate Request (CMP) the use of passphrase for the commissioning process: "5.5.2.3.10 For the first certificate request, the PKI client shall authenticate itself by using shared secret information (a ‘passphrase’) to create the “protection” field contained in the “Certificate Request” message or by using a valid certificate (e.g., a manufacturer device certificate)." This is in conflict with the Shared Cybersecurity Specification definition SPPRAMSS-2030 - The TLS endpoint shall perform authentication using certificates in accordance w... . **[**SPPRAMSS-16342 **]**

3.14.2 Affected System, components or interfaces

, SP-SEC-MigGuide-3.14.2-1 - The following systems are affected:

- KMC
- EVC
- RBC
- ATO-OB
- ATO-TS

[SPPRAMSS-16335 **]**

3.14.3 Guidance

, SP-SEC-MigGuide-3.14.3-1 - To allow compatibility, the central PKI shall provide passphrases (MAC-based protection according to RFC 9483 section 4.1.5) according to [UNISIG SUBSET-146 v4.00] as long as the client implements and uses this implementation. This solution is applicable to all affected systems. **[**SPPRAMSS-16337 **]**