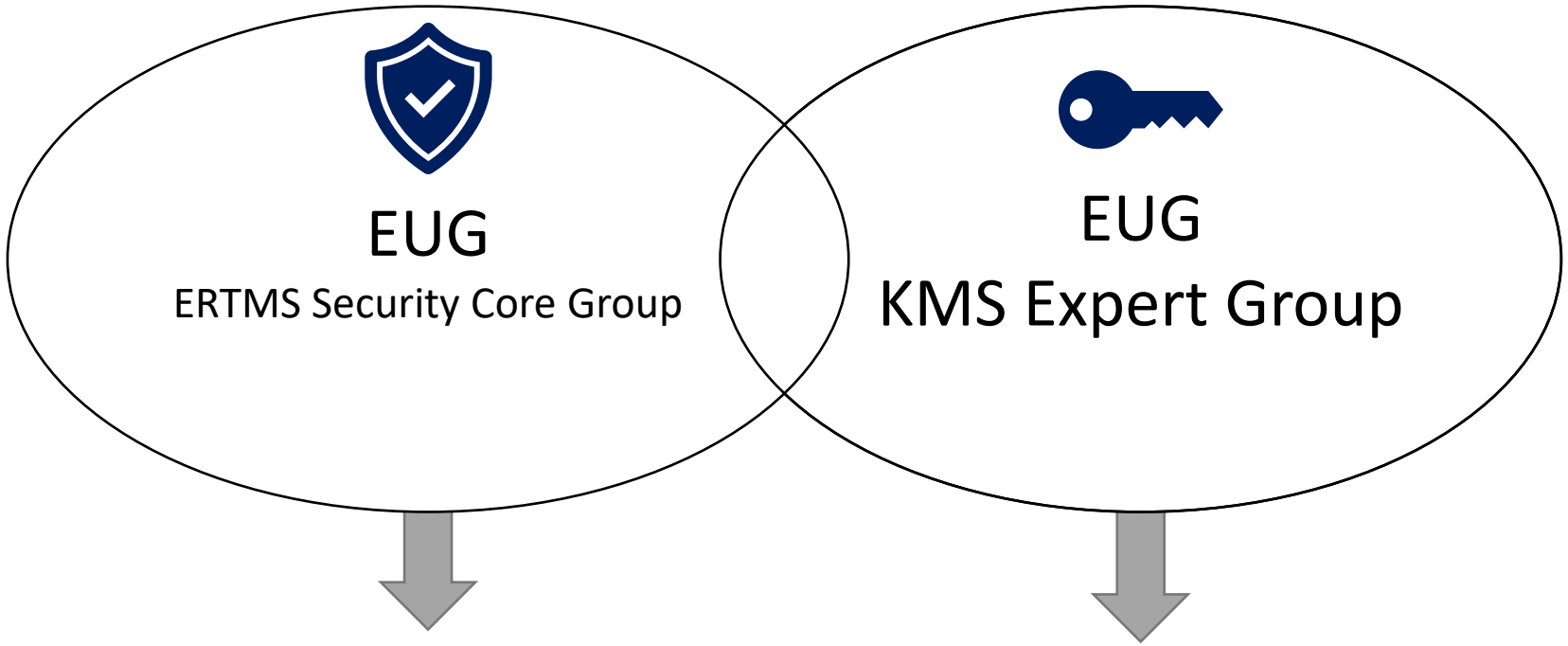
EUG
KMS PKI PoC

3rd ERA ENISA Conference on Cyber Security

08/11/23

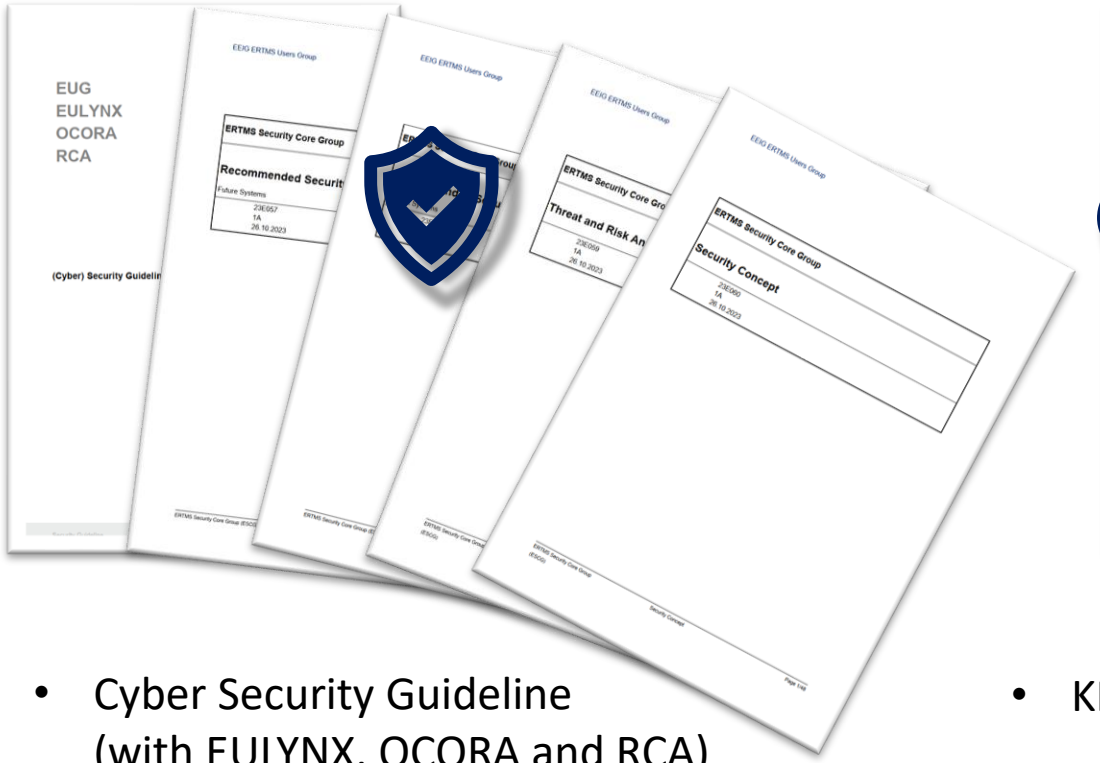
Joint approach for Security in the EUG

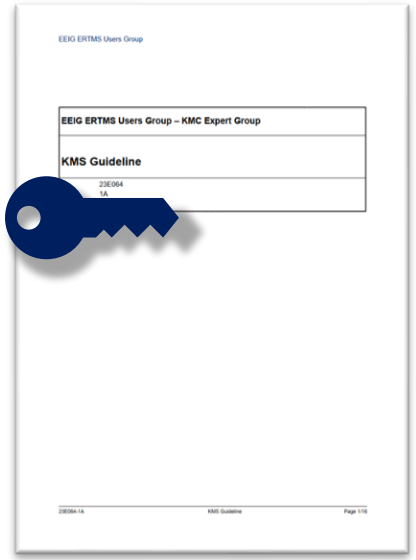


- ERTMS security guidelines for existing and future implementations
- Proposals for Security in future TSIs (Part of EU-Rail Mirror Group)

- Recommendations on KMS setup, inter-KMC arrangements and processes

Joint approach for Security in the EUG

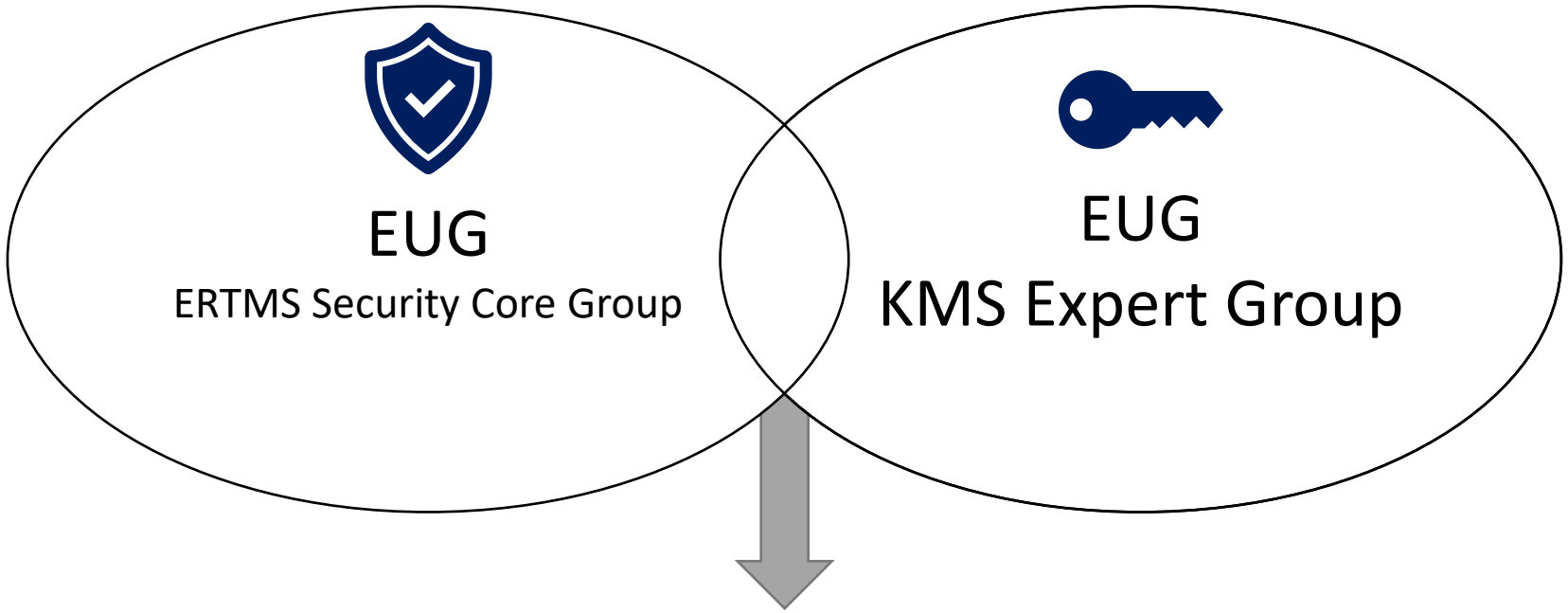




- Cyber Security Guideline (with EULYNX, OCORA and RCA)
- Security Concept
- Threat and Risk Analysis
- Recommended Security Measures Current and Future Systems

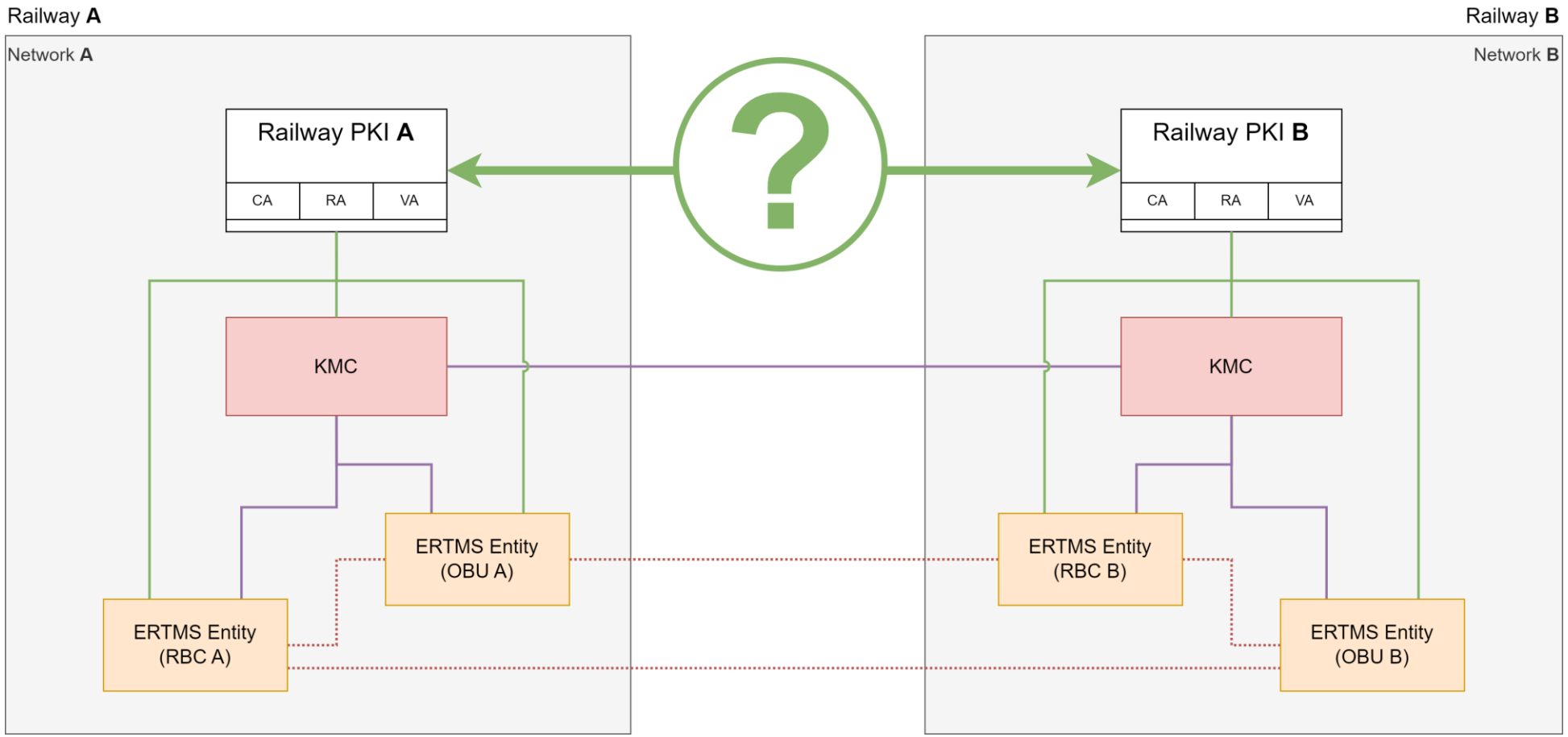
- KMS Guideline

Joint approach for Security in the EUG



- Proposals for future TSIs regarding Key Management
- Cross-Border/Cross-Organisation Key Management
- Inter-PKI structures and arrangements

How do we establish Inter-KMC connections?



KMS and PKI – Proof of Concept

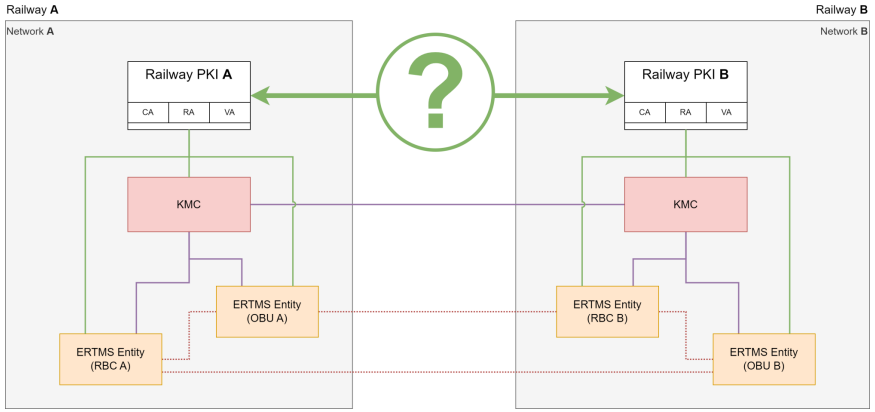
Goals

Core Target:

Which organisational and technical structures and procedures are needed for efficient, interoperable ERTMS cross-border operation?

Proof of Concept - Objectives:

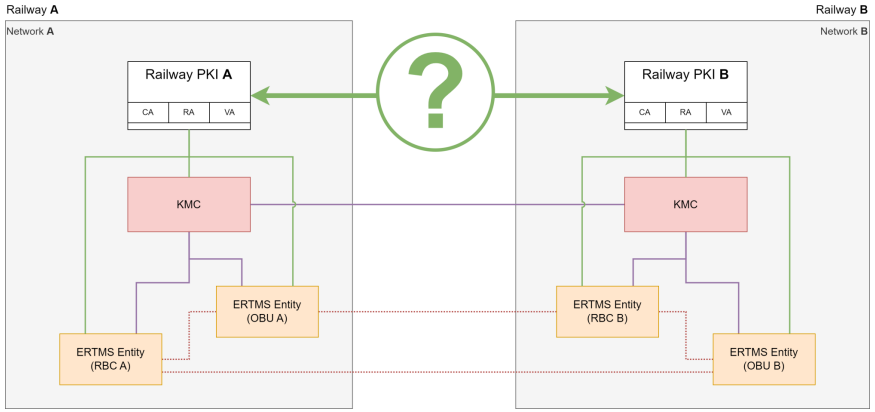
- Practical evaluation of PKI structures and certificate management (including revocation)
- Practical evaluation of inter-PKI communication
- Simplified demonstration of On-Line Key Exchange
- Simulate procedures (e.g. degraded mode) and technologies for cross-border traffic



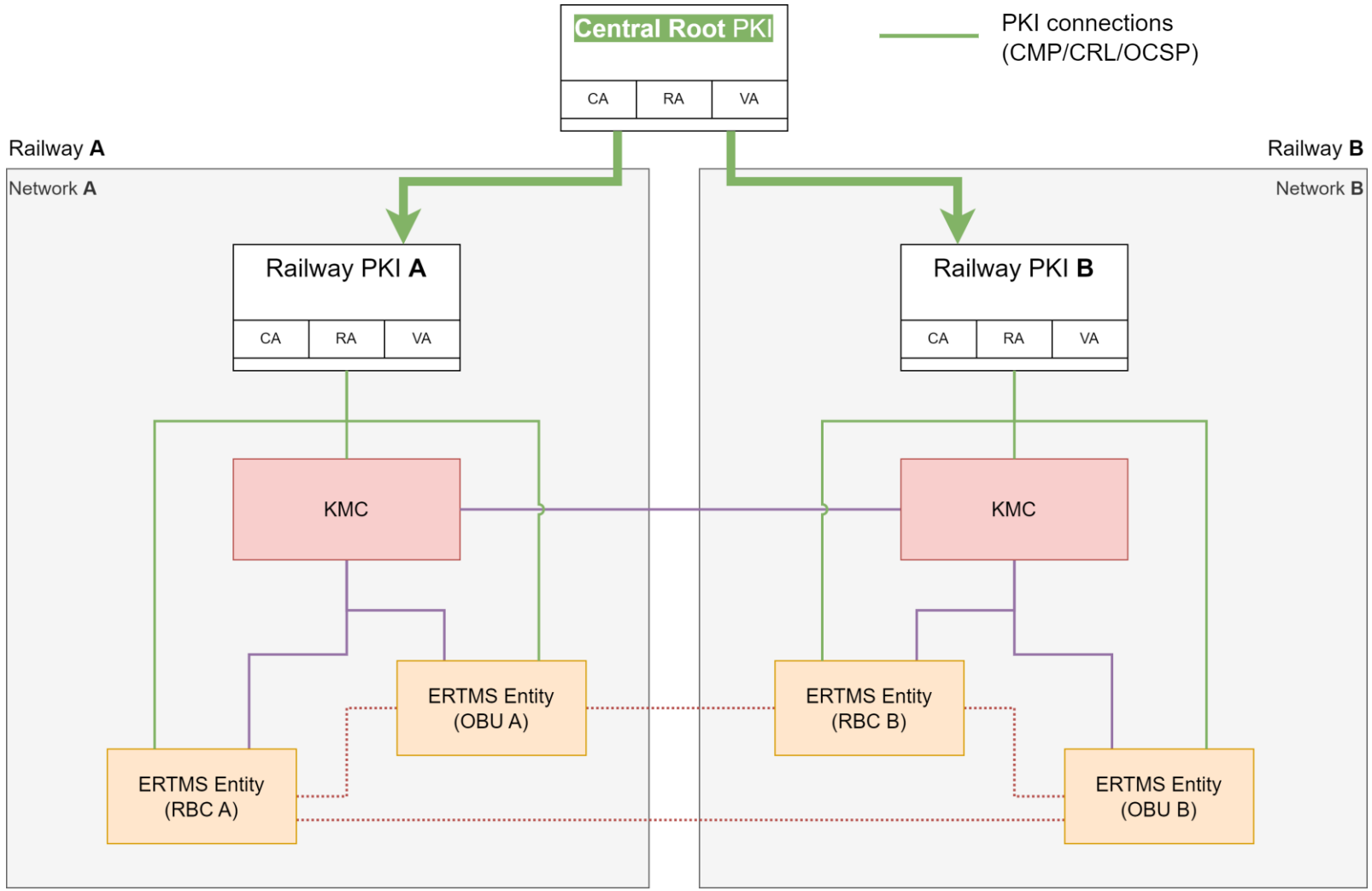
KMS and PKI – Proof of Concept

High Level Planning

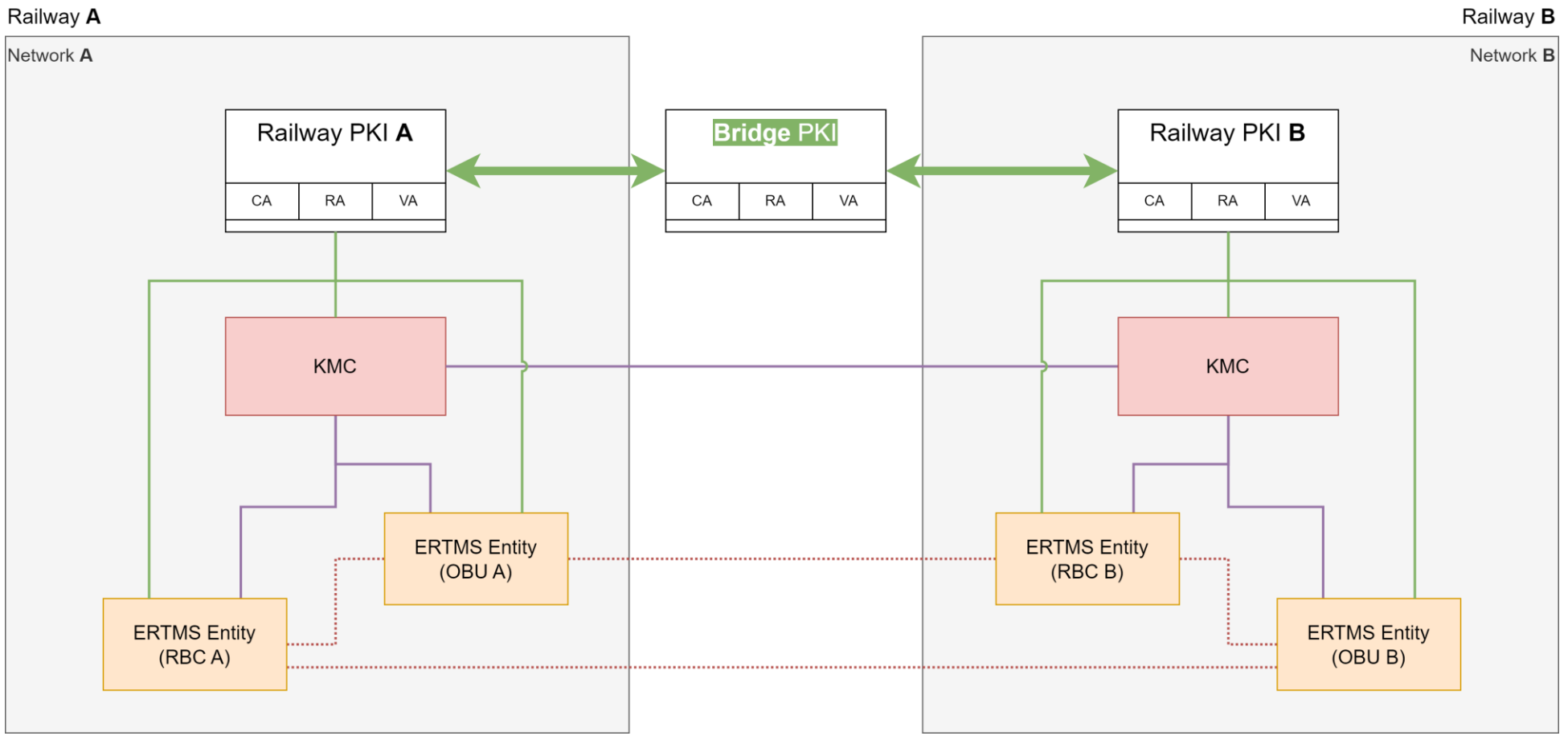
- **Provide (expandable) virtualized environment** for tests regarding
  - different PKI structures
  - inter KMC exchange
- **Deliverables:**
  - Report on results derived by EUG (+ additional involved parties)
  - Details regarding technical implementations
  - Identify necessary changes to the EUG/ESCG and the upcoming Subsets of EU-Rail



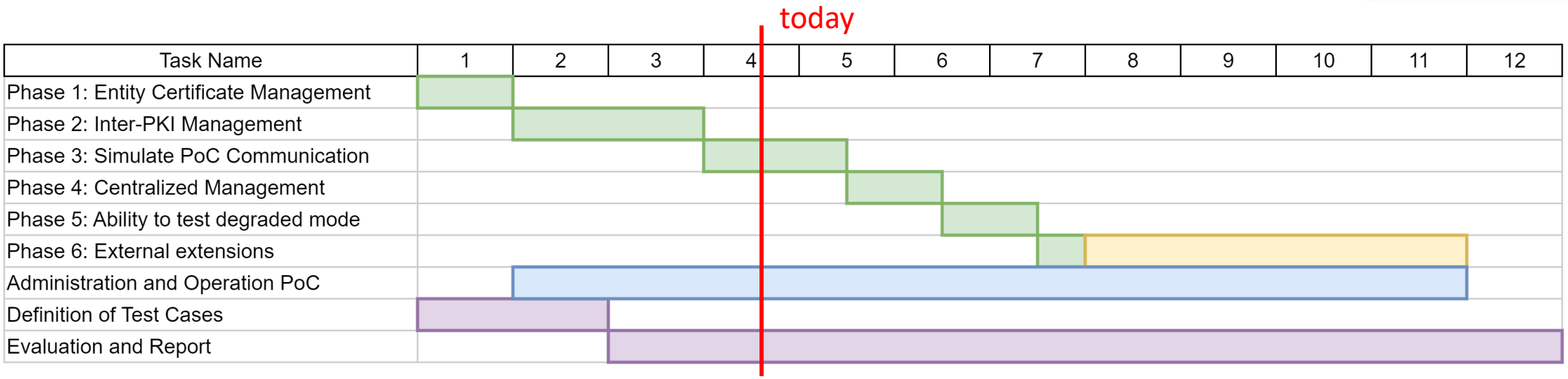
Example for PoC Setup



Example for PoC Setup



Schedule PoC - Phases



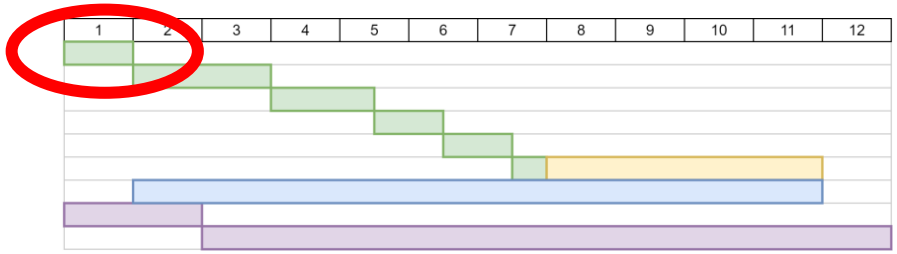
Setup

Support External Extension

Operation

Coordination of Evaluation

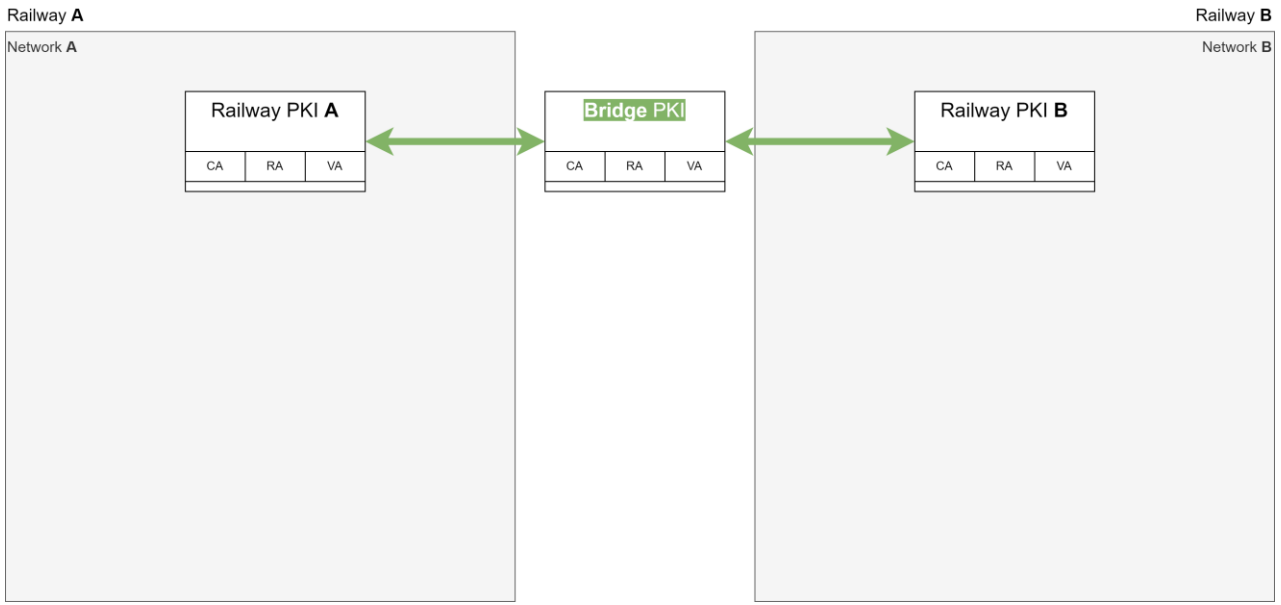
Schedule PoC - Phases

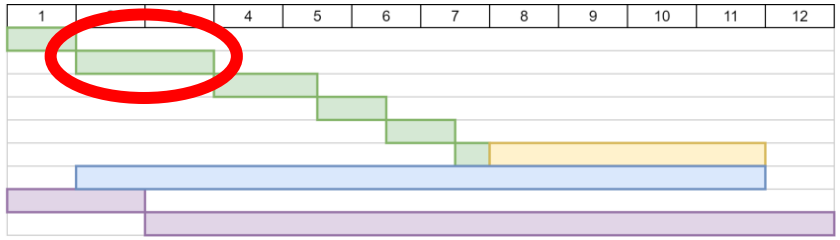


Phase 1:

After phase 1 a basic PKI with standard functionality is accessible and can be used to issue standardized certificates.

Schedule PoC - Phases

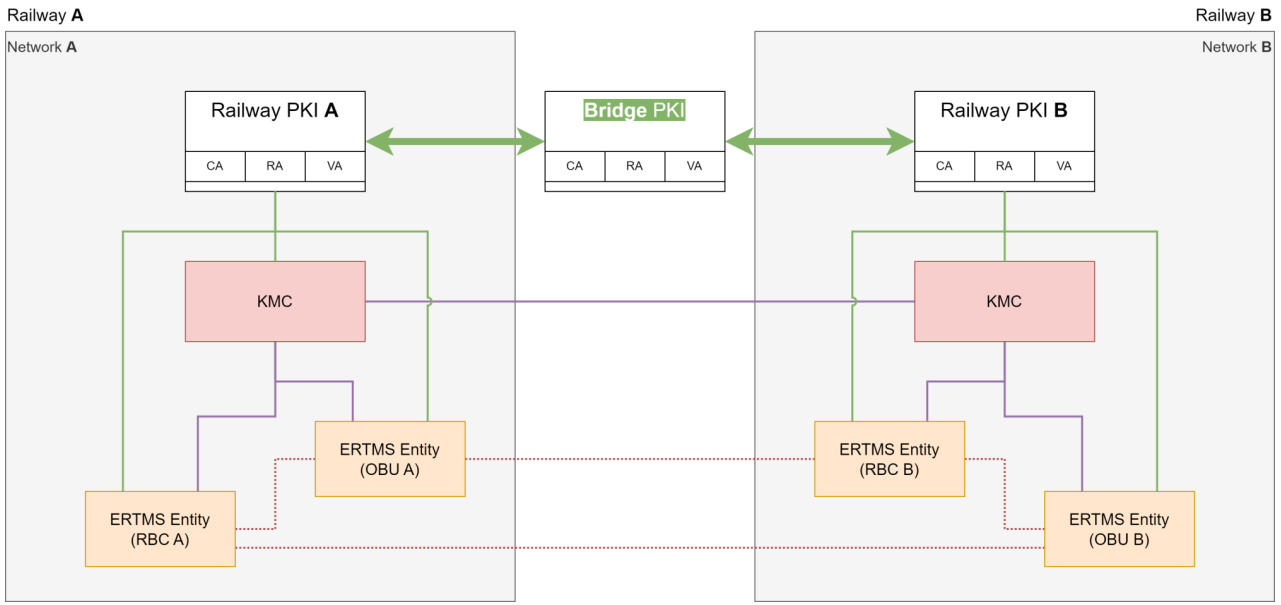


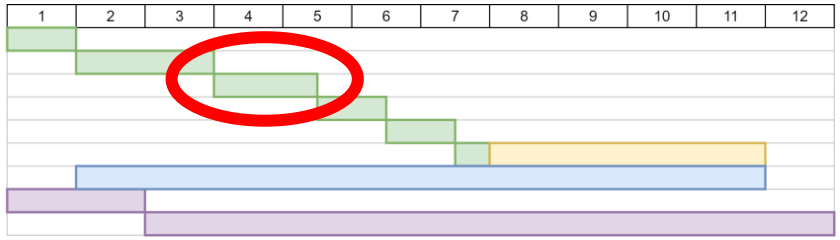


Phase 2:

Multiple PKIs are working next to each other in a dedicated sandbox environment. The set-up is designed modularly and prepared for easy extension for quick set-up.

Schedule PoC - Phases

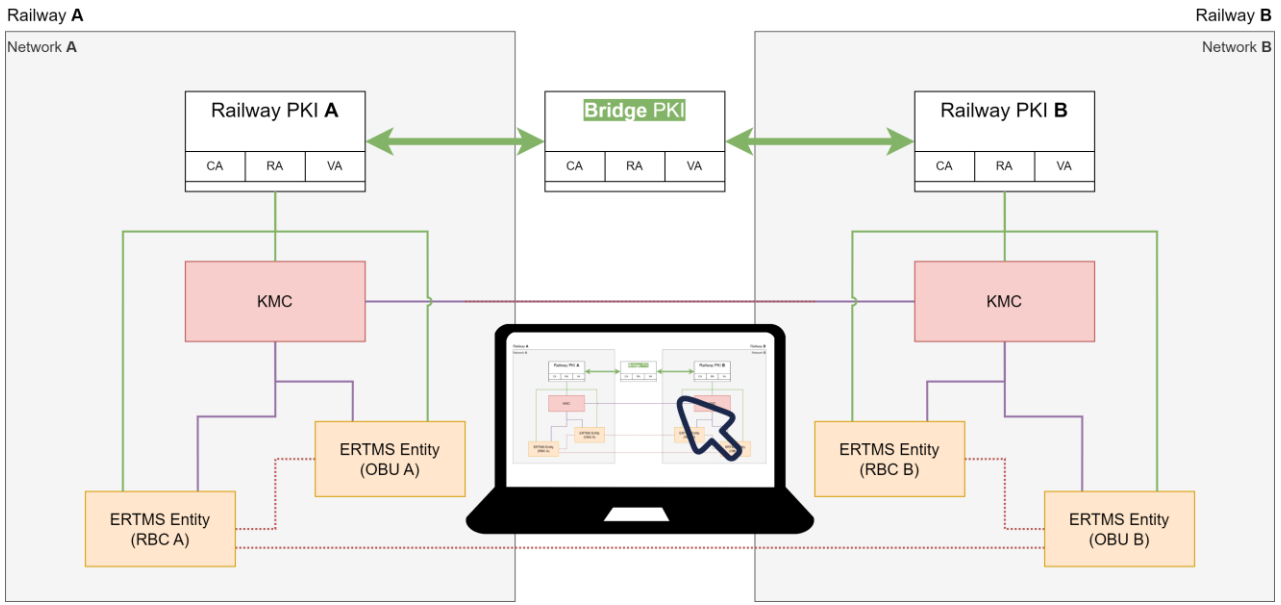


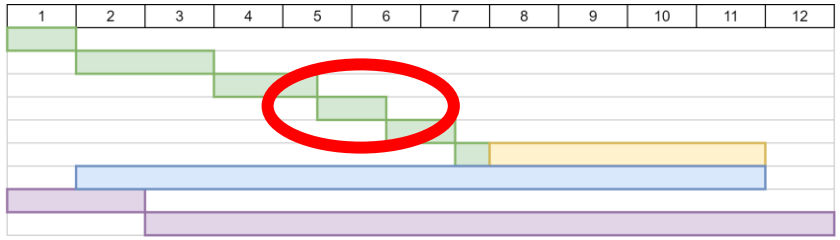


Phase 3:

A complete simulation environment will be available. The system will be able to establish mock connections using certificates issued by different PKIs in complex environments.

Schedule PoC - Phases

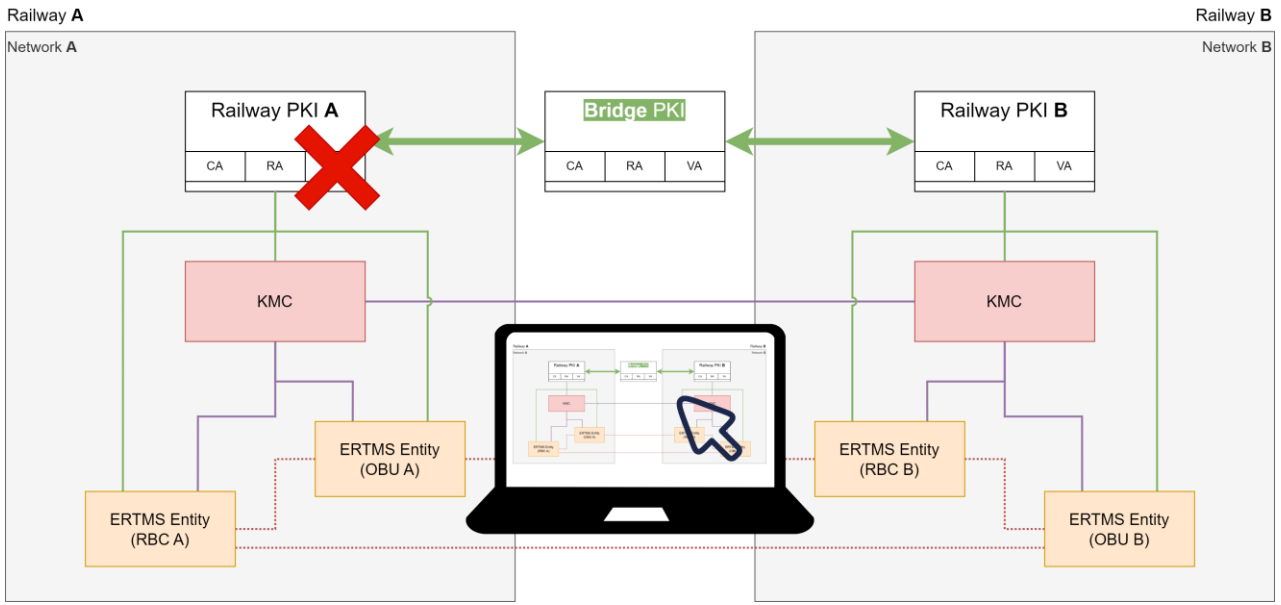


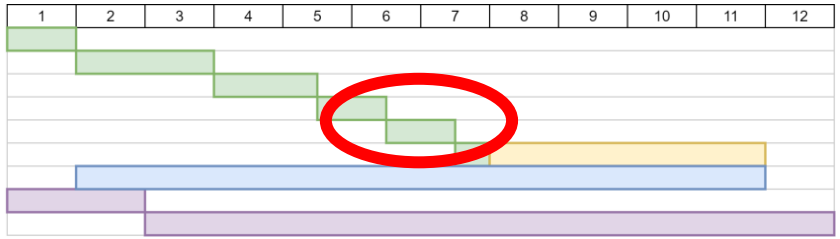


Phase 4:

A graphical user interface (GUI) will be implemented that allows to capture log data, start simulation, and manage the PKI servers in a simulation environment.

Schedule PoC - Phases

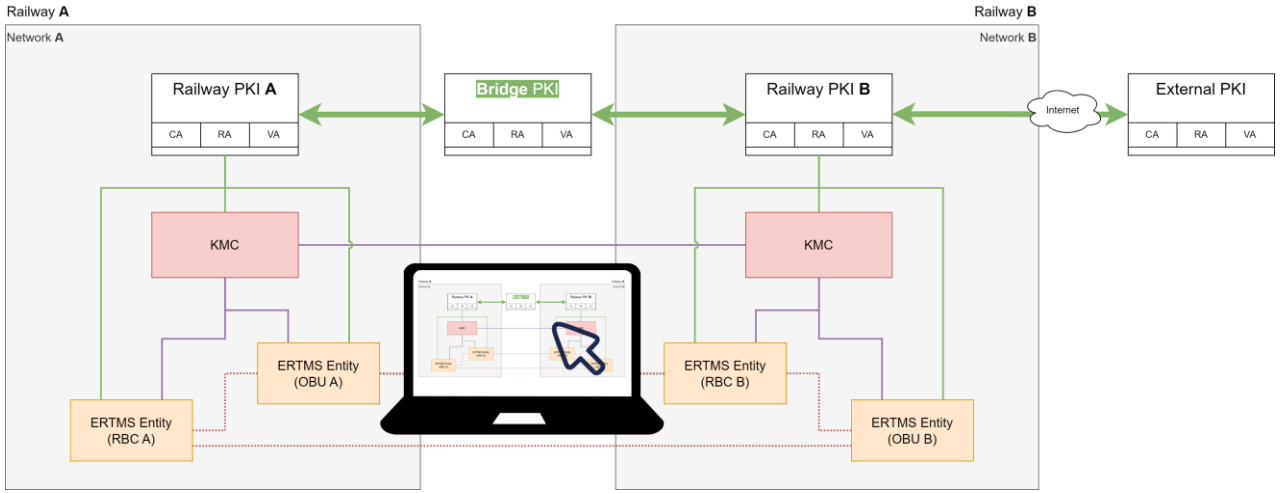


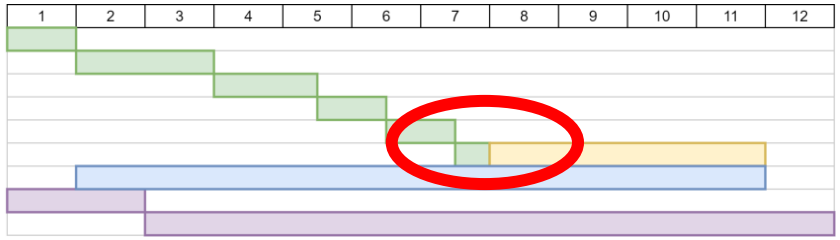


Phase 5:

Degraded mode for entities can be tested in the simulation environment. This includes using invalid certificates, simulating communication breakdown and other scenarios.

Schedule PoC - Phases





Phase 6:

The environment is prepared for external extensions. Hence e.g., external PKIs or mock-ups can be connected to the PoC environment.

Technical Details

- Virtualized on AWS using Docker
- Automatic deployment of the PKI architecture
- Using EJBCA Community version
- Code and Configuration is available on GitHub for all project members

Do you like to join the project?

Contact / Further Information

Richard Poschinger

richard.poschinger@incyde.com

Results of the project will be available at

https://**ertms.be**/activities/ertms-security-core-group

An overview of the work of the ESCG is provided in the article **"Cyber security measures for ERTMS from the rail operators' perspective"** in issue 09/23 of **Signal+Draht**.

Cyber-Security-Maßnahmen für ERTMS aus Sicht der Bahnbetreiber

Cyber security measures for ERTMS from the rail operators' perspective

Richard Poschinger | Christof Jungo | Ernst Kleine | Martin Espenschied

Durch eine steigende digitale Gefährdungslage rückt die Cyber Security im Bahnbereich verstärkt in den Vordergrund. Die Anzahl der mit dem europäischen digitalen Zugbeeinflussungssystem ETCS betriebenen Strecken steigt. Der damit einhergehende Bedarf zur securityspezifischen Absicherung von ETCS resultierte innerhalb der ERTMS Users Group (EUG) in der Gründung der ERTMS Security Core Group (ESCG). Die Arbeit der ESCG resultierte in umfangreichen, praktisch anwendbaren Security-Maßnahmen und Vorschlägen für die zukünftige Entwicklung von ETCS.

The growing digital threat means that cyber security is assuming an increasingly prominent role in the railway sector. More lines are being operated with ETCS, the European digital train control system. The consequent need to provide ETCS with specific security protection was the impetus for establishing the ERTMS Security Core Group (ESCG) within the ERTMS Users Group (EUG). The work undertaken by the ESCG has resulted in comprehensive security measures with practical applications and proposals for the future development of ETCS.