WHITE PAPER

PKI to Secure Data Communication in ERTMS

Authored by:

Selvakumar Kesavan
Technical Architect

Rajasekhara Turlapati
Principal Engineer

ABSTRACT

Communication and data transmission between various components in ERTMS utilizes open transmission systems. To secure data communication over these systems, a Public Key Infrastructure is utilized. Using cryptographic techniques, ERTMS/ETCS applications authenticate the various applications using digital certificates and signatures and authenticates the equipment to enable data transmission.

INTRODUCTION

With the hopes of removing cross-border barriers, the European Rail Traffic Management System (ERTMS) was established to create an interoperable railway network across European countries. The railway industry, faced with a high volume of passengers and freight, is motivated to move towards digital and interoperable systems.

A key feature within ERTMS is communication and data transmission between various components. While ERTMS has improved communication between train networks, the use of open transmission systems for data communication poses significant challenges in terms of security and vulnerability. A Public Key Infrastructure (PKI) is needed to address these vulnerabilities. The PKI is a set of hardware and software required to create, manage, distribute, use, store, and revoke digital certificates and public keys used for interoperability of the train network (RBC, OBU, and KMC systems).

With ERTMS requiring increased electronic interaction and stricter data regulations, PKIs help establish the identity of devices and services, enabling controlled access to systems and resources, protection of data, and accountability in transactions.

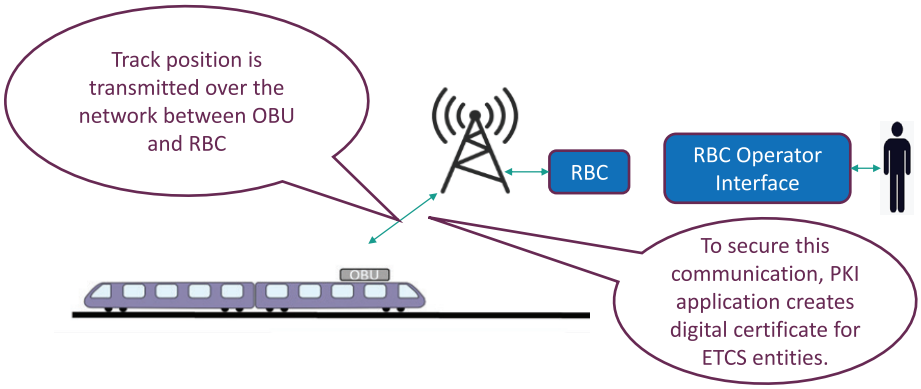
PKI SYSTEMS RESOLVING ERTMS DATA COMMUNICATION CHALLENGES

ERTMS applications use open transmission systems for communication between ERTMS/ETCS equipment. However, data transmission over open transmission systems is not safe or secure. It poses the risk of data being read through unauthorized access, impacting the system's safety. ERTMS/ETCS applications must employ cryptographic techniques to ensure the integrity and authentication of messages sent over open transmission systems.

When ETCS equipment establishes connections, for instance, between an Onboard Unit (OBU) and a Radio Block Center (RBC), both must be able to securely exchange information, authenticate the other equipment, and verify that it is an authorized entity.

PKIs provide a framework that enables cryptographic data security technologies such as digital certificates and signatures to be effectively deployed on a mass scale and authenticates equipment to establish secure communication among the entities.

The information in this document is the property of Quest Global Services Private Limited and may not be disclosed in any manner to a third party nor used for any purpose other than that for which it is supplied without prior written consent.



Where
OBU – On Board Unit
RBC – Radio Block Center
ETCS – European Train Control System

PKI FUNCTIONALITY

PKI is vital in issuing and validating a digital certificate.

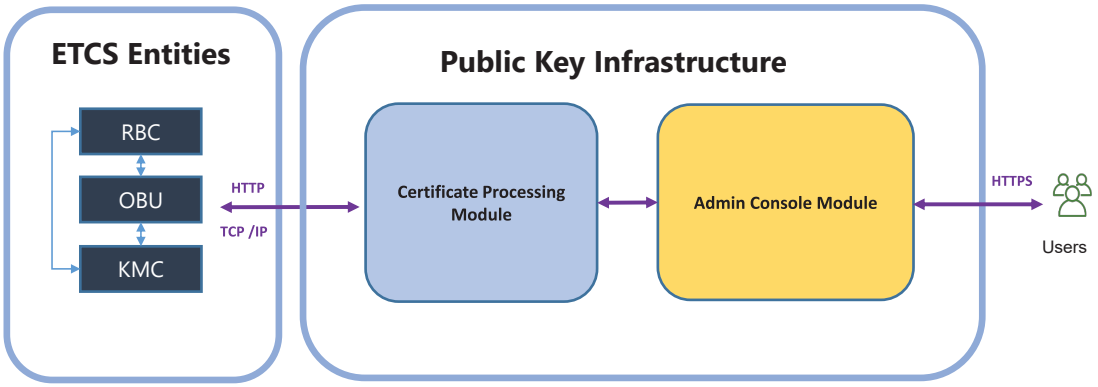
When two entities like the OBU and RBC need to exchange data, the OBU extracts and validates the digital certificate of the RBC by sending an online certificate status protocol (OCSP) request to the PKI application.

The PKI application checks and validates the status of the certificate and responds to the OCSP request. The OBU encrypts the data using the RBC's public key and transmits it via an open transmission system, which is decrypted and consumed by the RBC using its private key.

PKI MODULES

The PKI typically has two main components, a backend component called a Certificate Processing Module and a front-end UI module called an Admin Console Module. The Certificate Processing Module processes the request from an entity for certificate creation and validation. The Admin Console Module for a PKI user interacts with the PKI application for creating and issuing a Root CA. It is also used for creating and updating entities, user management, and monitoring CMP and OCSP requests.

The below sections provide an insight into how these modules work and interact.



The information in this document is the property of Quest Global Services Private Limited and may not be disclosed in any manner to a third party nor used for any purpose other than that for which it is supplied without prior written consent.

CERTIFICATE PROCESSING MODULE

Key operations of the Certificate Processing Module are the Certificate Management Protocol operation and the Online Certificate Status Protocol (OCSP) operation.

When the PKI system receives a First Certificate request, it validates the request, generates the digital certificate, and sends it as a response to the ETCS entity.

PKI functions on asymmetric key methodology: private and public keys. The private key can only be accessed by the owner of a digital certificate. After getting the digital certificate from PKI, if the private key of an ETCS entity is compromised and the ETCS entity wants to use the same digital certificate with a different key, it can send a Re-Key request to the PKI to get a new key for the same digital certificate.

When the ETCS entity wants to verify the authenticity and validity of the digital certificate, it sends the certificate details as an OCSP request to PKI for verification.

When the PKI receives an OCSP request, it validates the request, verifies the certificate status, and sends the response with the certificate status. The certificate status could be valid, revoked, or unknown.

ADMIN CONSOLE MODULE

The Admin Console Module in PKI has eight components. These are

1. Certificate Authority - For the ETCS entity to start communicating with the PKI, it should have a Root and Issuing CA generated from the PKI. The PKI will use the certificate to validate and authenticate the request from the ETCS entity for Digital Certificate generation. This component enables users to create a Root and Issuing CA for the ETCS entity. Once created, the certificates can be downloaded and shared with the ETCS entity through a secured channel.
2. Entity Management – This component handles the addition and modification of the ETCS entity. When the ETCS entity receives the Root and Issuing CA, the entity can send a First Certificate request to receive the digital certificate.
3. User Management - This component handles user creation, modification, and password reset. Users are created with respective roles, such as Admin or Operator, to operate the PKI application.
4. Certificate Management Protocol (CMP) - Monitors the CMP request received from various ETCS entities.
5. Online Certificate Status Protocol (OCSP) - Monitors the OCSP request received from various ETCS entities
6. Database View – Displays the details of the entity along with the certificate details.
7. Application Log - To troubleshoot, this component provides application logs for each type of

The information in this document is the property of Quest Global Services Private Limited and may not be disclosed in any manner to a third party nor used for any purpose other than that for which it is supplied without prior written consent.

communication TCP (Transmission Control Protocol) and HTTP (Hyper Text Transfer Protocol) and also to clear the logs on demand basis.

8. User Audit - This component maintains a record of all changes made to the database by the user.

HIGH AVAILABILITY FEATURE

The PKI application must always be available for the ETCS entity to acquire and validate the digital certificate.

The Quest Global team has designed and developed a solution wherein the PKI application is deployed in multiple nodes with a load-balancing capability that always ensures availability. Quest Global has built the application to handle automatic failover in case of failures in the primary system. Databases are replicated to ensure the availability of data at all times.

PKI USAGE IN REAL-WORLD APPLICATIONS

Our PKI product can be customized to meet the customer's needs and secure online communications. PKI is widely used to establish HTTPS (Hyper Text Transfer Protocol Secure) communication between the browser and web server. HTTPS combines HTTP and SSL (Secure Socket Layer)/TLS (Transfer Layer Protocol) and provides encrypted data communication.

PKI can also be used for email encryption, signing documents, and software, secure communication with database servers, securing access to IoT devices, etc.

SUMMARY

PKI helps organizations establish trusted signatures, encryptions, and identities. However, PKI is different from other technologies present in the IT stack. You need highly skilled in-house IT teams to run it effectively. With the PKI product, we offer cost-effective, customized solutions to meet the unique requirements of our customers. By leveraging cryptographic techniques and digital certificates, we ensure the integrity and authentication of data transmitted over open transmission systems.

At Quest Global, we strive to be the most trusted partner for the world’s hardest engineering problems. Our strength lies in our highly experienced local-global execution team, which is aligned with our vision of being your "Trusted thinking partner of choice."

We deliver world-class, end-to-end engineering solutions by leveraging our deep industry knowledge and digital expertise. Our PKI product, designed and developed with the utmost care, plays a crucial role in enhancing the security of data transmission within the European Rail Traffic Management System

The information in this document is the property of Quest Global Services Private Limited and may not be disclosed in any manner to a third party nor used for any purpose other than that for which it is supplied without prior written consent.

(ERTMS) application.

ABOUT THE AUTHORS

Rajasekhar and Selvakumar penned this article. The authors have worked on various projects across numerous domains including rail transportation. With a combined experience of 3 decades, they have experience working with a wide range of cutting-edge tools and languages.

Rajasekhar leads a team of engineers at Quest Global and is currently working on signaling projects for customers globally. He has extensive experience in transportation, wireless technologies, industrial electronic products and consumer and networking projects/products. He has executed embedded projects, from inception to production, across multiple domains.

Selvakumar, a seasoned Technical Architect, brings over two decades of expertise across Banking, Utility, Direct Tax, and Railway. Among his many notable achievements, he analyzed legacy PKI software for a customer and spearheaded the design of a modern architecture aligning seamlessly with the HTTP layer, adhering to the industry-standard RFC 6712 and 2616. This architectural transformation significantly enhanced the efficacy of digital certificate creation and verification processes.

The information in this document is the property of Quest Global Services Private Limited and may not be disclosed in any manner to a third party nor used for any purpose other than that for which it is supplied without prior written consent.

https://www.linkedin.com/company/quest-global

https://www.facebook.com/QuESTGlobal

https://twitter.com/QuEST_Global

https://www.youtube.com/user/questglobal10

About Quest Global

We are Quest Global. We're in the business of engineering, but what we're really building is a brighter future. It's not just what we do, but why we do it that makes us different. We believe engineering has the unique opportunity to solve the problems of today that stand in the way of tomorrow. For 25 years, we have strived to be the most trusted partner for the world's hardest engineering problems. As a global organization headquartered in Singapore, we live and work in 17 countries, with 56 global delivery centers & offices, driven by 17,000+ extraordinary employees who make the impossible possible every day.

Quest Global brings deep industry knowledge and digital expertise to deliver end-to-end global product engineering services. We bring together technologies and industries alongside the contributions of diverse individuals and their areas of expertise to solve problems better, and faster. This multi-dimensional approach enables us to solve the most important and large-scale challenges across the Aerospace & Defense, Automotive, Energy, Hi-Tech, Healthcare, Medical Devices, Rail, and Semiconductor industries.

The information in this document is the property of Quest Global Services Private Limited and may not be disclosed in any manner to a third party nor used for any purpose other than that for which it is supplied without prior written consent.