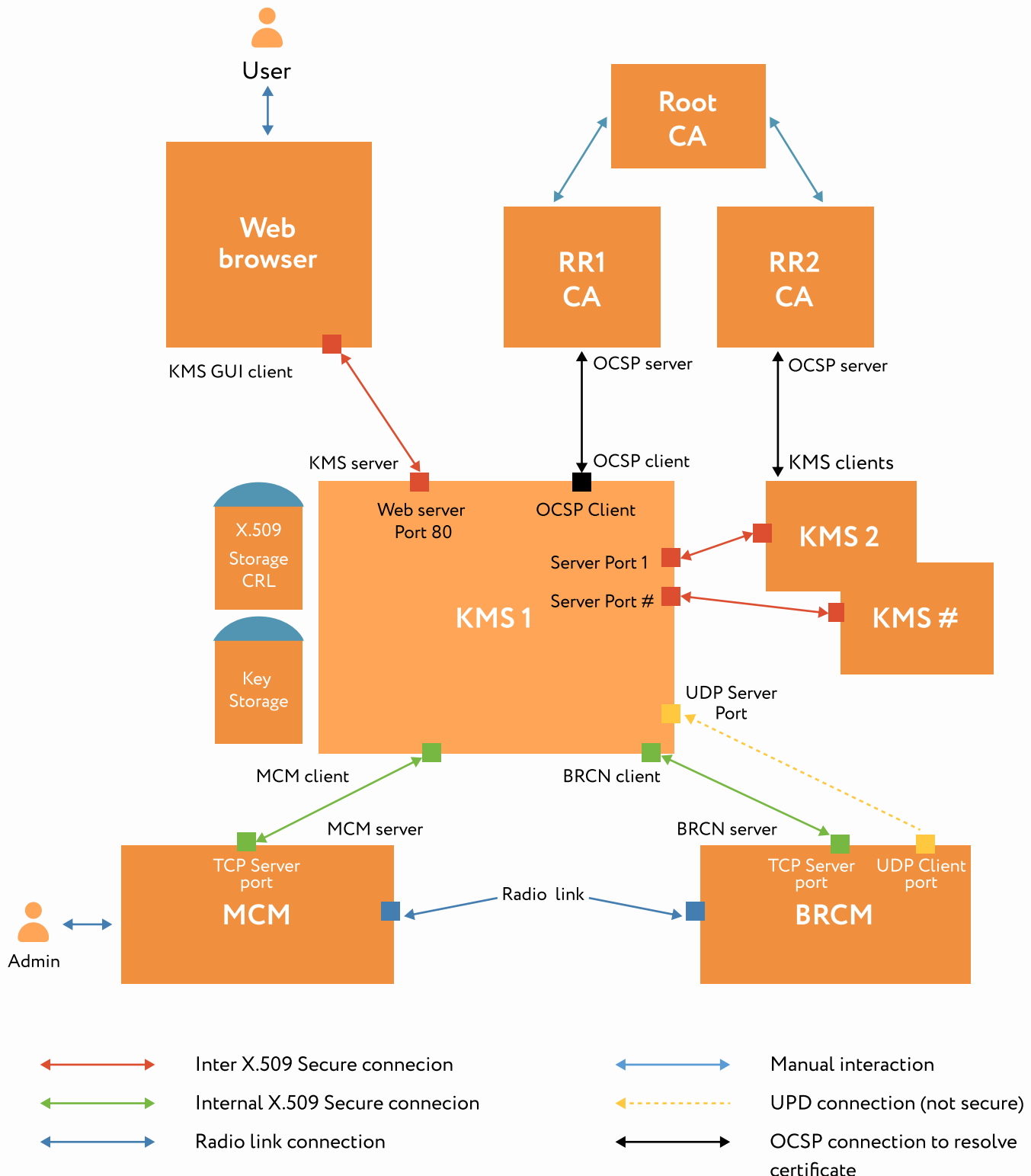# PTC SECURE COMMUNICATION SYSTEM

Datasheet

Project objective

Provide secure communications between railroad vehicles and wayside equipment, including implementing a Key Management System to generate certificates for each component of the system, create encryption keys, and keep them up-to-date.

User

Web browser

KMS GUI client

Root CA

RR1 CA

RR2 CA

OCSP server

OCSP server

KMS server

OCSP client

KMS clients

X.509 Storage CRL

Web server Port 80

OCSP Client

OCSP Client

KMS 2

Server Port 1

Server Port #

KMS 1

KMS #

Key Storage

UDP Server Port

MCM client

BRCN client

MCM server

BRCN server

TCP Server port

TCP Server port

UDP Client port

Admin

MCM

Radio link

BRCM

Inter X.509 Secure connecion

Internal X.509 Secure connecion

Radio link connection

Manual interaction

UPD connection (not secure)

OCSP connection to resolve certificate

Result

The system provides an efficient method for managing and updating secure configurations for the vehicles, trains, and wayside devices, keeping data up-to-date, with a high level of security and protection against unauthorized access.

Scope of work

- Design the architecture of the system providing secure communications between railroad vehicles and wayside equipment

- Implement Key Management System (KMS) to create encryption keys and keep them up-to-date

- Develop Certfication Authority interaction module to confirm encryption keys

- Provide convenient interaction with the system

- Establish secure communication between locomotives and wayside devices using radio link connection and keys provided by KMS

Activities

- Requirements review and analysis

- Initial Internal/External KMS architecture and use cases diagram preparation

- Internal components APIs definition and gaps identification

- Development of CA scripts for Certificate creation

- Installation and support of CA and OCSP servers

- Implementation of KMS-CA API (library or scripts)

- Integration and final delivery onsite

- KMS modules and components implementation

- Database support development

- Web user interface development

- LDAP authentication implementation

- Communication component implementation

- Project documentation development

- VectorCAST-based unit test implementation

About the project

Technologies

- HTML
- CSS
- JavaScript
- C/C++
- Angular JS
- Python
- TCP/IP
- SSH
- XML
- OpenSSL
- GCC
- Git
- VectorCAST

Platform

- Web
- Linux
- Embedded Linux

Project size

- 1 Project Manager
- 4 Software Engineers
- 1 QA Engineer
- 1 Technical Writer
- 1 Graphic Designer

Duration

13

13 months

Jan 2018 – Feb 2019