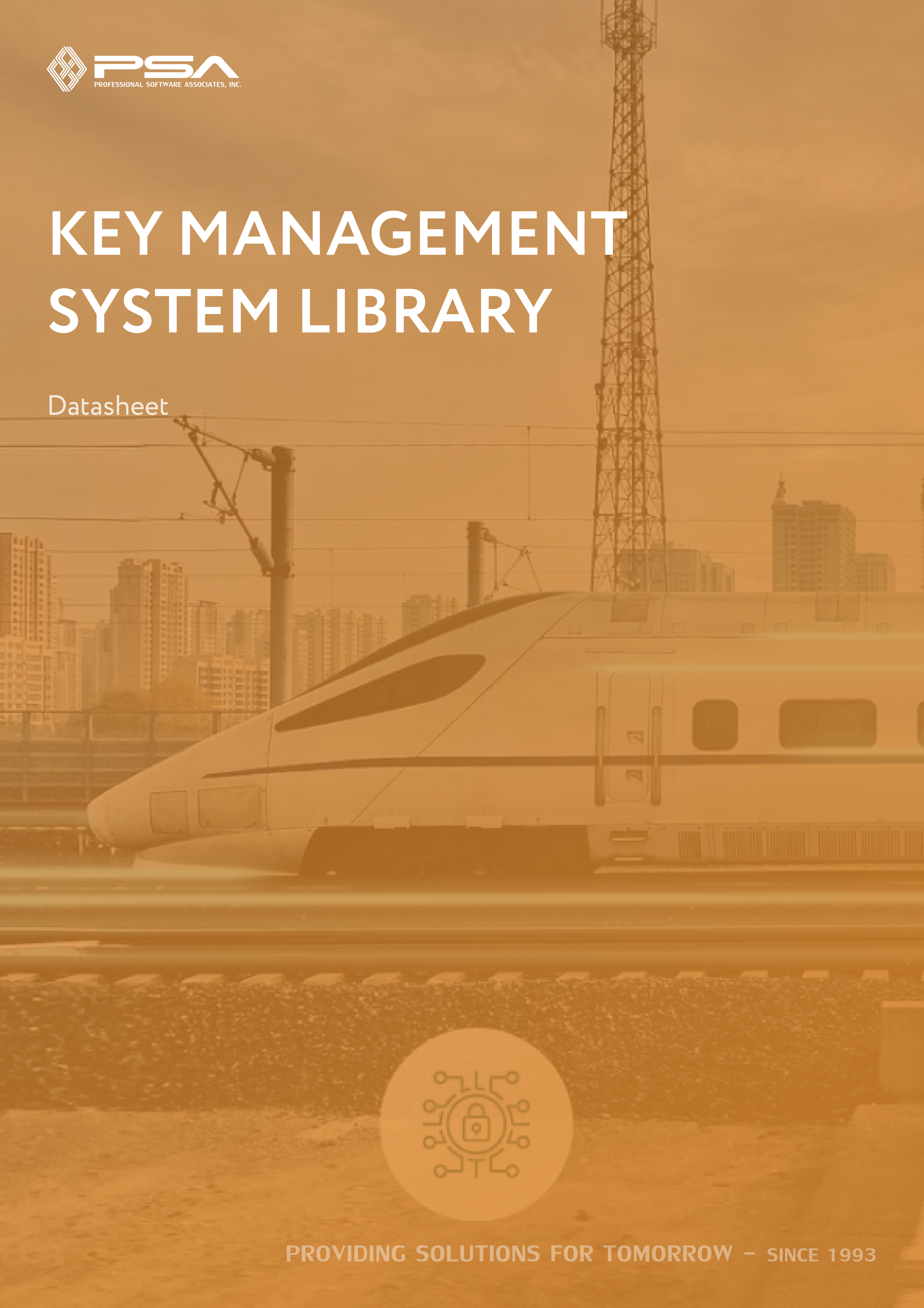
PSA
PROFESSIONAL SOFTWARE ASSOCIATES, INC.

# KEY MANAGEMENT SYSTEM LIBRARY

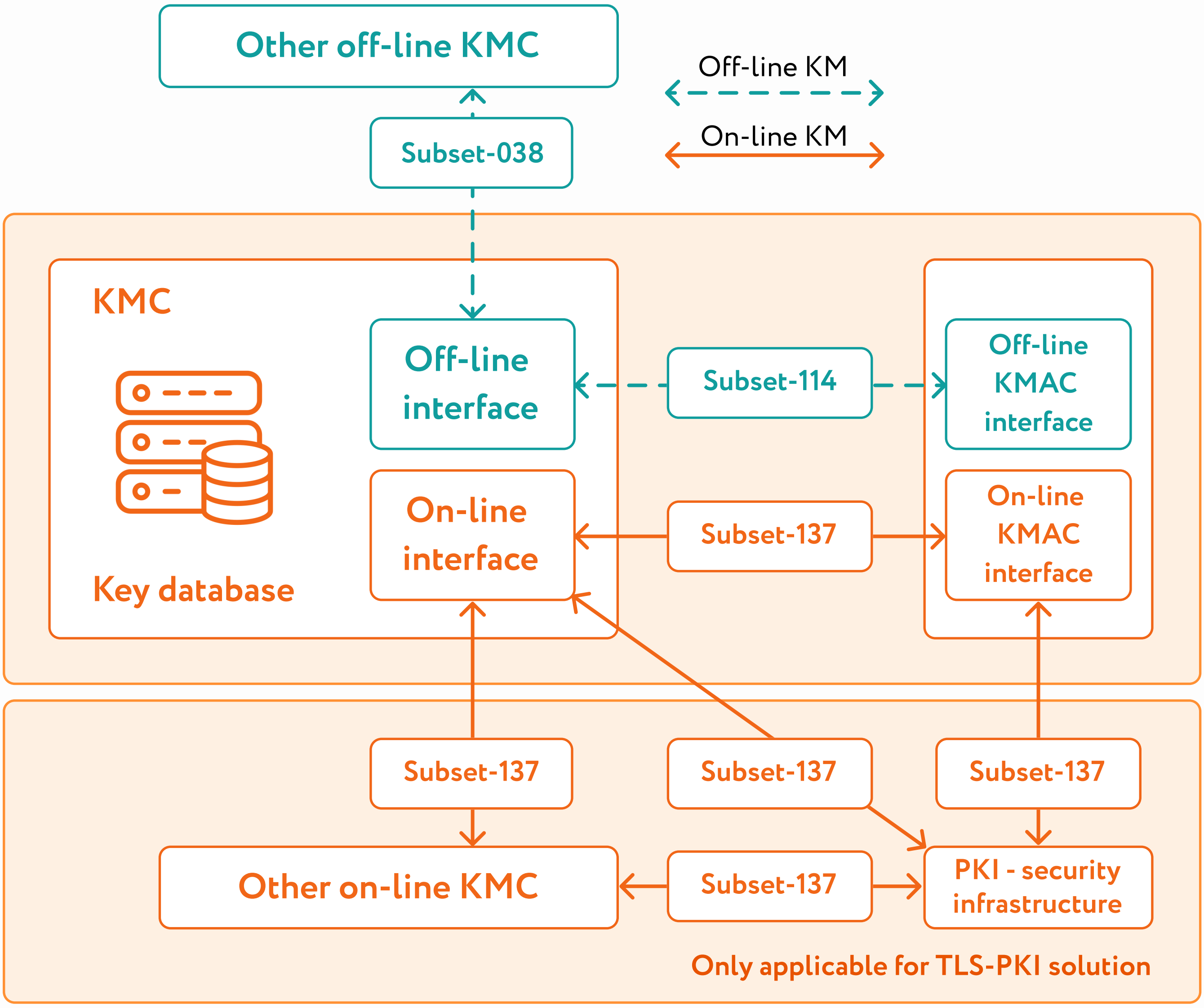
Datasheet



PROVIDING SOLUTIONS FOR TOMORROW – SINCE 1993

# Project objective

Complete the Key Management System Library for the client's product to fulfill 100% secure real-time communication between wayside and onboard equipment. Provide the realization of the protocol described in "ERTMS/ECTS: On-line Key Management FFFIS" UNISIG SUBSET-137.



# Result

The provided Key Management System library allows rail system developers to seamlessly build rail security applications. This component allowed the client to finalize their product, a software tool designed for rail system developers. The solution is accompanied with all the necessary documentation on how to utilize the library to build your own railway safety-critical application.

## Scope of work

- Analysis of the architecture and the code structure of the existing version of the KMS library. Gaps identification, and bug fixing
- Certificate Authority (CA) interaction implementation. CA scripts development, CRL, and building a certificate chain
- Advanced encryption through elliptic curves X.509 certificate
- Public Key Infrastructure (PKI) platform configuration
- KSM library client functions. Checksum function, X.509 authentication, TLS-PSK, OCSP, and CMP functions
- Software Architecture Specification (SAS) and Software User Manual (SUM) documents
- Unit test cases to verify correct message structure generation for command and notification messages. They include test execution results, traceability matrix, bug reports, and coverage statistics
- Demo application creation to verify the secure connection between server and client applications organized using OpenSSL

## Activities

- Requirements definition
- Software architecture review
- Software development
- Unit test cases creation and execution
- Documentation creation

# About the project

## Technologies

- C/C++
- OpenSSL library
- VectorCAST
- Redmine
- Confluence
- Git

REDMINE
flexible project management

Confluence

## Project size

- 1.5 people

## Duration

22
months

May 2021 – March 2023

## Platform

Linux
Embedded