SWIM Common PKI and policies&procedures for establishing a Trust Framework

D2.1 – Common PKI specifications

Document information	
Project Title	SWIM Common PKI and policies&procedures for establishing a Trust Framework
Project Number	2017_084_AF5
Project Manager	EUROCONTROL
Deliverable Name	Common PKI specifications
Deliverable ID	D2.1
Edition	1.0
Template Version	01
Task contributors	

Please complete the advanced properties of the document

Abstract

This document contains the Common Public Key Infrastructure (PKI) specifications for the European Aviation Common PKI (EACP).

Note that this document is not subject to review as it is only a container of documents which themselves have been subject to review within the project and by the SESAR Deployment Manager.

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
Patrick MANA EUROCONTROL	Project Manager	21/09/2021

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date

Reviewed By – *e.g. EDA, staff associations, other organisations.*		
Name & Company	Position & Title	Date

Approved for submission to the SDM By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection

Document History

Edition	Date	Status	Author	Justification
1.0	21/09/2021	Released	P.MANA	Final

Table of Contents

Table of Figures

No table of figures entries found.

Table of Tables

No table of figures entries found.

1. Introduction

This document contains the Common Public Key Infrastructure (PKI) specifications for the European Aviation Common PKI (EACP) solution developed by the project so-called "SWIM Common PKI and policies & procedures for establishing a trust framework".

1.1 Content

This Common PKI specifications for the future European Aviation Common PKI is composed of two documents:

- High-level architecture for a common PKI.
- Technical details for a common PKI.

1.2 Objective of this Deliverable

The objective of this Deliverable D2.1 is to define a high-level architecture and a set of technical specifications for a future European Aviation Common PKI.

This deliverable and its two associated documents have been be used as input to produce:

- Interfaces to Common PKI (D3.1 and D3.2).
- The technical part of the Call For Tenders (D5.1 and D5.2).
- Guidance for SWIM service providers (D6.1) and for SWIM service consumers (D6.2).

1.3 Project description

The project aims at developing and deploying a common framework for both integrating local PKI deployments in an interoperable manner as well as providing interoperable digital certificates to the users of SWIM and other services and systems supporting European aviation operations. The resulting PKI and its associated trust framework, which will be part of the cyber security infrastructure of aviation systems, are required to sign, emit and maintain digital certificates and revocation lists including as required in the family 5.1 of Common Project 1 Implementing rule (EC 116/2021). The digital certificates will allow user authentication and encryption/decryption when and where needed in order to ensure that information can be securely transferred. All aviation Stakeholders (ANSPs, Airspace users, MIL, Airport, etc …) will benefit from the project.

1.4 Project scope

The scope of the project includes the definition and development of a dedicated common PKI and its associated trust framework for Europe, its integration and validation with some Stakeholders. It will ensure the interoperability of digital certificates within Europe and with other regions.

The solution will not be restricted to provide certificate only for SWIM purposes. Benefits of developing and deploying this solution have been taken to extend its scope as much as possible to:

- Increase the level of security of the European aviation network by allowing as many stakeholders, applications, services, systems using digital certificates as security enhancement means.
- Increase the cost-efficiency of the solution as the cost of developing and operating a PKI/Bridge is not linearly linked to the number of certificates (e.g. the cost of developing and operating a PKI/Bridge for few or half million certificates is nearly the same).

Therefore, the project will develop the material to prepare the development and the operations for European Aviation Common PKI.

1.5 Project objectives

The project also aims at preparing the development of the systems needed to operate a PKI and its associated trust framework in order to produce and manage digital certificates, e.g. Certification Authorities, validation services such as OCSP (Online Certificate Status Protocol) or CRL (Certificate Revocation List) or SCVP (Server Certificate Validation Protocol), user interfaces, systems supporting the Registration Authority and Policy Management Authority roles. These systems will be developed through procurement, for which the project will prepare a Call For Tenders (CFT).

2. High-level architecture for a Common PKI

The purpose of this document is to describe the architecture of the European Aviation Common Public Key Infrastructure (PKI) as a solution developed under the CEF co-funded "SWIM Common PKI and policies & procedures for establishing a trust framework" project under the SESAR Deployment Management (SDM) portfolio.

After reading this document, the reader should have a clear understanding of the architecture of the European Aviation Common PKI and the rationale behind the necessary decisions made.

The purpose is therefore to both document the architecture from a high-level standpoint, almost down to the specifications of the PKI, and to document the arguments behind the decision-making process.

The governance structure around the trust framework[1] is documented in other products of the project.

It includes the arguments for architectural decisions for the future EACP.

High Level
Architecture for comn

[1] "Trust Framework" includes more than a PKI and evolves a general trust between organisations to cooperate in the Single European Sky.

3. Technical details for a Common PKI

This document describes the procedures necessary to build a trustworthy PKI for European Aviation Common PKI (EACP).

It includes:

1. PKI Operations – Information about the relevant procedures that needs to be in place – The “procedures” and “people” in a functional system.

2. Certificate specifications – What will be the contents of the actual certificates produced by EACP.

3. Technical Specifications – Information about the servers and other parts of the necessary infrastructure to run a PKI. The “Equipment” of a functional system.

The arguments for architectural decisions are in the “High Level Architecture document”.

Technical Details for common PKI v1.0.doc