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

D1.2 – Final Trust Framework

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	Final Trust Framework
Deliverable ID	D1.2
Edition	1.2
Template Version	01
Task contributors	

Please complete the advanced properties of the document

Abstract

This document is the Trust Framework for the future European Aviation Common PKI (Public Key Infrastructure).

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
Patrick MANA EUROCONTROL	Project Manager	04/06/2021

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
0.1	04/06/2021	Released	P.MANA	Final
0.3	06/07/2021	Draft	N.Gautier	Draft for SDM comments
0.6	29/10/2021	Draft	N.Gautier	Draft summarizing Thread A & B work before project review
0.7	11/11/2021	Draft	N.Gautier	Draft after final review Thread A/B
1.0	06/12/2021	Released Issue	P.Mana	Released Issue taking into account project members comments
1.1	07/03/2022	Released Issue	P.Mana	Released Issue taking into account comments raised during the 1st SDM consultation cycle
1.2	21/04/2022	Released Issue	Abdel Youssouf	Released Issue taking into account comments raised during the 2nd SDM consultation cycle

Table of Contents

1. Introduction 6
1.1 Project description 6
1.2 Project scope 6
1.3 Project objectives 6
1.4 Objective of this Deliverable 7
1.5 Structure 7
2. EACP Technical Trust Framework (Annex A) 8
2.1 Technical Trust Framework Structure 8
Outstanding Issues 9
2.2 9
3. EACP Institutional Framework: MOC and its annexes (AnnexB) 11
3.1 Content 11
3.2 Remaining decisions for the EACP set-up 12
4. EACP Implementation Options (Annex C) 16

Table of Figures

Figure 1: EACP Technical Trust Framework 8
Figure 2: EACP Memorandum of Cooperation 11

Table of Tables

No table of figures entries found.

1. Introduction

This document is the draft Final Trust Framework for the future European Aviation Common PKI (Public Key Infrastructure), deliverable D1.2 of the "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project.

1.1 Project description

The "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project aims at developing and preparing the deployment of 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 Common Project 1 family 5.1 (EC IR 2021/116). 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.

1.2 Project scope

The scope of the "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project includes the definition and development of a dedicated common PKI and its associated trust framework for the European aviation (so-called EACP), its integration and validation with some Stakeholders. It will ensure the interoperability of digital certificates within Europe and with other regions.

The future EACP 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 and 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 a million certificates is nearly the same).

Therefore, the "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project will develop the material to prepare the development and the operations of the future European Aviation Common PKI solution.

1.3 Project objectives

The "SWIM Common PKI and policies&procedures for establishing a Trust Framework" 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).

1.4 Objective of this Deliverable

The objective of this Deliverable D1.2 is to define a set of propositions for the European Aviation Common PKI Trust Framework, covering the institutional, technical as well as business perspectives. Ultimately, these propositions are intended to be approved by the future constituents of the European Aviation Common PKI and serve to operate and use digital certificates and their associated services in the framework of the European Aviation Common PKI.

This document provides an overview of the documentation structure needed to establish EACP. It includes references to a number of other documents that will be necessary to establish or operate the future EACP service.

1.5 Structure

This Trust Framework of the future European Aviation Common PKI is composed of a set of documents providing principles, rules and processes that are intended to govern and describe the operations of the future European Aviation Common PKI. It includes the following parts:

- **D1.2 Annex A – EACP Technical Trust Framework**
- **D1.2 Annex B - EACP Memorandum of Cooperation and its annexes,** which provides the instrument to create EACP and its governance
- **D1.2 Annex C - EACP Implementation Options,** which is a high level business analysis describing the possible options to implement EACP, depending on the number of users and use cases.

2. EACP Technical Trust Framework (Annex A)

2.1 Technical Trust Framework Structure

This section deals with the Technical part of the EACP Trust Framework, and explains how it is shaped to ease the understanding of the documentation structure.
The Technical part of the EACP Trust Framework is made of Annexes that are presented in Figure 1.

Figure 1: EACP Technical Trust Framework

Annex A gives an overview of the Technical part of the EACP Trust Framework. It is made of the following sub-annexes:

- Annex A1 details the EACP membership and Users Agreements. This document describes the different possibilities to participate in EACP (either as a Governing Member, as a User, or as a Relying party) and the related membership agreements. It presents also other subsequent agreements related to EACP services.
- Annex A2 provides the EACP Technical Solution. Annex A2 presents the EACP catalogue of Products and Services, and presents the EACP Hierarchy of Certification, altogether with the different Identity Assurance Levels that will be supported by the EACP solution should EACP adopt it Certificate Policy document for its solution implementation.
- Annex A3 describes EACP Policies and Processes. It is made of:
  - Annex A3.a: EACP Certificate Policy document. This document describes a set of rules that indicates the applicability of EACP digital certificates with security requirements. It is drafted according to the RFC3647.
  - Annex A3.c EACP Processes and Procedures. This document details processes and procedures for the different EACP services, including the advanced ones, surrounding the EACP certificate lifecycle management.
  - Annex A3.d: Criteria and Methodology for Interoperability. This document presents the eligibility criteria for European Aviation stakeholders as well as for external PKI domain partners to join the EACP network of Trust by the Interoperability Scheme.

2.2 Outstanding Issues

The outstanding issues identified in this section will be addressed either at the time of initiating EACP by founding members (e.g. those listed in 2.2.1, 2.2.2 or 2.2.3) or at the time there is a need for (e.g. those listed in 2.2.4).

2.2.1 EACP Identity Assurance Levels

In the case of EACP custom solution, the project member could not reach a common consensus whether EACP will adopt:

I. the classical three Identity Assurance Levels as per NIST Publication SP 800-63a (Low, Medium, High).
II. the Identity Assurance Level as set forth in Spec 42: 13 Assurance levels. (Low with 4 sub-levels, Medium with 4 sub-levels, High (PIV AV) with 3 sub-levels, + Short-Life Low Assurance-256 Level and Short-Life Med Assurance-256 Level)
III. The 11 Identity Assurance levels as proposed in International Aviation Trust Framework (IATF) Common Certificate Policy document (Low with 3 sub-levels, Medium with 5 sub-levels and High with 3 sub-levels).

Remark: The EACP Certificate Policy document is drafted based on the IATF's 11 Identity Assurance Levels, and need to be reviewed once a common agreement has been achieved.

2.2.2 Intra Interoperability Assessment Report

In the deliverable D1.2, the Annex A3.d.1 introduces a framework for the assessment of a candidate Local PKI to be conducted in the case of EACP intra-Europe interoperability.
Building upon this framework, the formal detailed assessment document with its associated security controls will be developed later as it depends upon the actual use cases which are not known at this stage. This to-be-developed document, that will include details and level of rigor of the security controls, will be submitted to the EACP PMA for approval.

2.2.3 Outstanding procedures:

The following procedures need to be developed at a later stage.

- Swimlane figure for initial registration process
- Procedure for PKI Operators
- Procedures for Time Stamping
- Procedures for Publication
- Procedures for Certificate Transparency

2.2.4 Outstanding Agreements / Terms of Use in Annex A

- "Validation As Service" Terms of Use
- "Signing As Service" Terms of Use

- "Time Stamping" Terms of Use

3. EACP Institutional Framework: MOC and its annexes (Annex B)

3.1 Content

The European Aviation Common PKI service will be established through a multi stakeholder agreement, defining the legal basis on which EACP will operate. The content of this legal document is available in a draft form as an appendix to this document, and it is expected that it will be finalised by the signatory parties at the moment of the actual establishment.

It is expected that this agreement will at least include the following annexes:

- The EACP Trust Framework, itself made of a set of documents that defines rules, processes, and procedures applicable to the parties involved in the EACP service;
- The EACP Governance ToRs; and
- The EACP Charging Policy.

Figure 2 provides an overview of the structure of the Memorandum of Cooperation

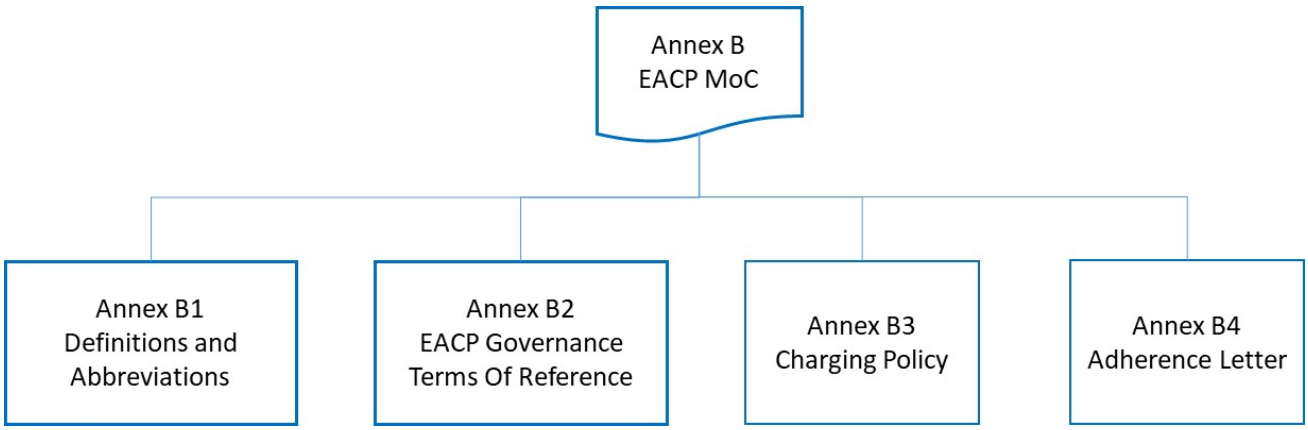

Figure 2: Structure of the EACP Memorandum of Cooperation

Annex B1 – Definitions and Abbreviations.

Annex B2 – EACP Governance ToRs aim at defining the Governance arrangements for the European Aviation Common PKI Trust Framework: the different bodies, their scope and responsibilities, their membership and working practices.

Annex B3 – EACP Charging Policy for the users of the service.

As Annex B4 – Adherence Letter.

3.2 Remaining decisions for the EACP set-up

The project developed the required material to enter into the EACP implementation phase. Some remaining decisions of a political nature remain to be taken by the future members of the governance when establishing EACP. These decisions are listed in the two following sections, concerning first the Memorandum of Cooperation, and second the Terms of Reference of the future Governance.

3.2.1 Remaining decisions for MoC

3.2.1.1 EACP service provision model

An outstanding decision is how the EACP service provision will be made (by whom, and which legal document will define it). Three possibilities exist in the MoC:

1. Not addressing it in the MoC: in such case, the MoC just defines the governance; the service provision model will need to be defined in a separate agreement to be negotiated at a later stage by the governance members.
2. Service procured and provided by EUROCONTROL
3. Common Procurement Agreement (à la NewPENS)

The following figure depicts the service provision options (2 – on the left) and (3 – on the right).

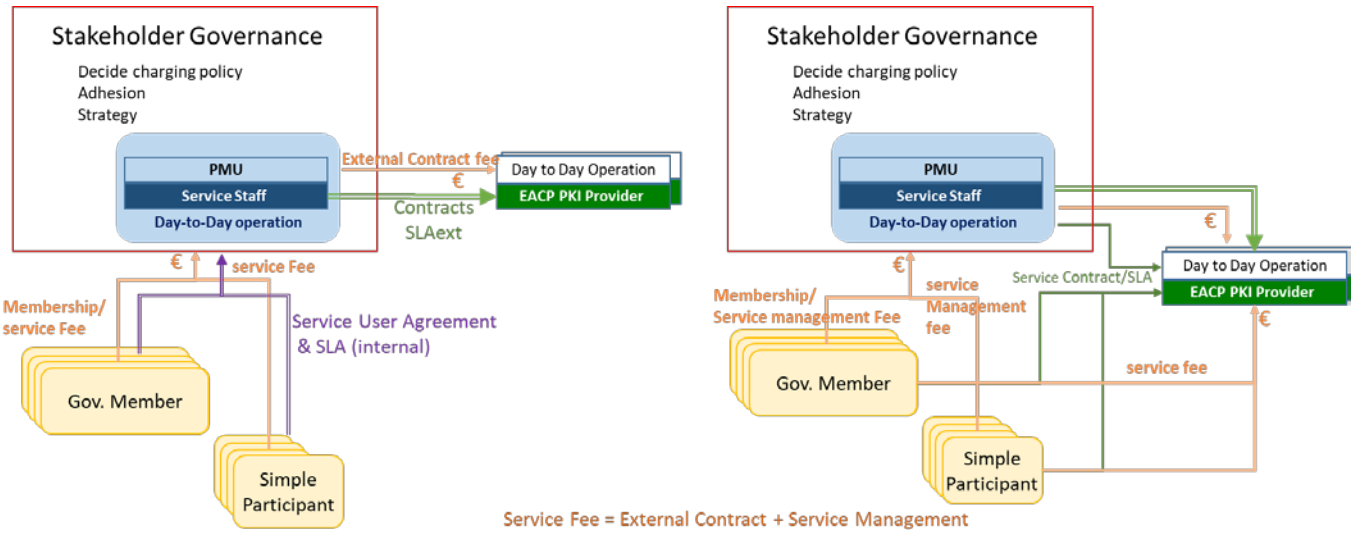

Figure 3: EACP service provision models

In case of a service provided by EUROCONTROL (2), a contractual arrangement will be concluded between EUROCONTROL and the PKI provider, under the steering of the common governance. EUROCONTROL, as a legal entity, could become the EACP trusted provider on behalf of the EACP governance. All users will benefit from the services provided by the PKI provider.

In the case of a common procurement (3), a common contract will be concluded by EUROCONTROL on behalf of all parties, which would sign a Common Procurement Agreement. All parties will be able t accede to the common contract and benefit from the services of the PKI provider. It is however not clear in this case what will be the legal entity that will be declared trusted service provider (as commercial providers may refuse to be the trusted service provider for a Certificate Policy which is not their own)

Common service steered and driven by users through a dedicated working arrangement established (strategic evolution, prioritisation, etc.)	
Common specifications developed by the governing members. Possibility for governing members to take part in the procurement, according to EURCONTROL procurement rules	
Common SLA ensuring same quality of service for all users	
Financed by users (set-up costs by governing members)	
Procured by EUROCONTROL; service provided to all users by the PKI provider	Common procurement with EUROCONTROL as common procurement agent
SLA between ECTL and users	SLA between PKI provider and users
ECTL Trusted Service provider under EACP governance	Unclear what legal entity would be the Trusted Service Provider

	Common Service (option 2)	Common Procurement (option 3)
Pro	Contractually simpler (1 external contract, change management easier) User SLA / contract independent from External Operator (no change in case of change of supplier) For users, 1 SLA with PMU One Oversight by EASA for the Pan European Service	Clear and direct liabilities No additional charges on PMU More acceptable politically? Adapted for buying commercial certificates, less for a private trust network
Cons	PMU liability, crossed liabilities Additional Administrative charges on PMU	Complexity of changing a framework for a high number of users & T&Cs different according to local legislation Change of External Supplier = change of x contracts (heavy)

		Extra Cost on Participants for contract management Regulatory Oversight to be implemented by each Participant

CPH also requested to consider another option – creation of a new legal entity for the purpose of EACP. Two comments were made by EUROCONTROL on this option:

- This would require other legal instruments than an MoC.
- EUROCONTROL cannot legally participate to the establishment of a legal entity (cf. NewPartnership).

Resolution: by implementing partners (recommendation from project team)

3.2.1.2 Set-up costs financing (applicable to MoC and charging scheme)

A comment was raised that set-up costs evenly borne by Governing Members could be an issue for some stakeholders. The Annex C (Implementation Options) provides a view of possible set-up costs to be born in different implementation scenarios. No alternatives was however found to the financing of the set-up costs by the Governing Members. The financing of set-up costs could however be linked to the type of services that will be used in the future by Governing Members.

3.2.2 Remaining decisions for the governance ToRs

3.2.2.1 Coordination with external bodies

Two different views were expressed with regards to external coordination and relation to NDTECH (see section 1.2 of the EACP Governance ToRs).

One proposal is to establish a strategic coordination with NDTECH for matters relevant to the overall network interests. The other proposal is not to identify such link but to refer in general to coordination with ICAO, ACI, IATA, etc.

Resolution: by implementing partners

3.2.2.2 PMU Composition

Two different views were expressed with regards to the PMU composition (see 3.2).

The first is the same model as in NewPENS: EUROCONTROL supports the PMU and provides a head of PMU, while contribution to the PMU is also possible from other MoC participants.

The second consist of PEB/PMA assigning a contract for running the PMU to a member for a period of minimum three (3) year and maximum (6) years.

This second option would have implication on the model for the service provision (see issue MOC#3):

- In case of common procurement, the Common Procurement agreement will need to define the respective responsibilities of the Head of PMU and common procurement agent.
- In case of EUROCONTROL procured service, the second solution might be impossible to implement as some liability in the service provision would lie with EUROCONTROL.

Resolution: by implementing partners

4. EACP Implementation Options (Annex C)

This document develops the different implementation option elements to facilitate the decision making process for the deployment of the EACP service. It identifies key scenarios that will allow the future founding members to understand how EACP would be financed and to decide what will be the most appropriate options for EACP deployment.