EACP deployment Next Steps

29th September

sesar DEPLOYMENT MANAGER

EUROCONTROL

Welcome

- **Hybrid meeting**
  - ❑ How to submit questions: As this is a hybrid meeting with many participants (>70), please submit questions in the chat
- **At the end of the workshop well have a poll, stay tuned**
- **Meeting objective**
  - ❑ Recap of EACP deployment so far
  - ❑ Next EACP deployment steps, based on consulted outcome of the IP
- To avoid misunderstandings, it's also important to clarify **what is not the objective**. We will **not engage into discussions regarding 5.2.1 Local implementation**, as this is a separate topic highly dependent om local infrastructure and organisation. Neither do we intend to enter into **discussions regarding cybersecurity**, although related to **PKI**, as this is regulated by other EU directives and regulations.
- **Agenda**

EACP Workshop proposed agenda

Smooth step from consultation to EACP deployment

10.00-13.00

1. **Welcome**

2. **European Common PKI Mandate – CP1**
   - Why we need an EACP
   - Timeline – Already done (regulatory framework)
   - Project deliverables and consultation
   - Link with local implementations
   - **Q&A**

3. **Introduction of EACP**
   - Scope of EACP
   - Common Procurement
   - Implementing Timeline
   - **Q&A**

4. **Proposed approach and next steps for deployment of EACP and fulfilling family 5.1.1 requirements**
   - **Q&A**

5. **Summary and next actions**
   - Next actions
   - Poll
   - **Q&A**

6. **AOB**

Why we need an EACP

The regulation

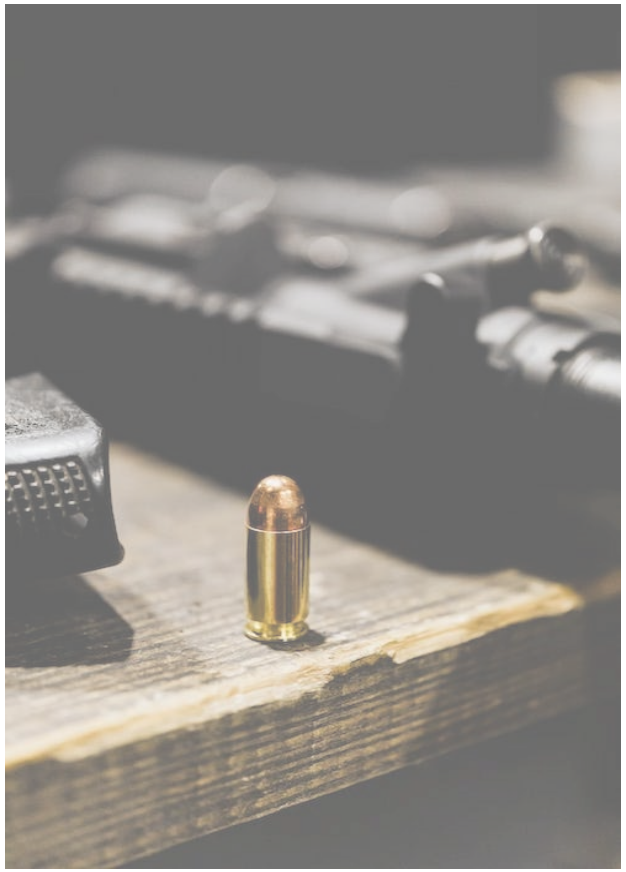
A common public key infrastructure (PKI), which is used in signing, emitting and maintaining certificates and revocation lists used in inter-stakeholder communication for operational purposes.

The SWIM yellow profile technical infrastructure fulfils that communication and interoperability goal by being modular and providing different implementation options based on the web services stack of standards, including commitments to lower layer protocols, taking into account a wide range of needs for information exchanges in an appropriately secured way.

The SWIM yellow profile technical infrastructure can run over any IP based network, such as public internet or new pan-European network services (PENS), based on the stakeholders` needs.

Why we need an EACP
The summary

- SWIM introduces **new way of communication**
  - Public internet
  - NewPENS
- **New and flexible communication paradigms/technologies**
- SWIM may bring **new attack vectors** but most exist already in our existing infrastructure
- Need to **secure the communication** in an appropriately secured way
- PKI will **not solve all information security challenges**, PKI also brings new vulnerabilities by itself



Why we need an EACP
The scope

- 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.
- 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 as required**. 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 will benefit from the project.
- The scope of the project includes the **definition of a dedicated common PKI and its associated trust framework for Europe**. It will ensure the interoperability of digital certificates within Europe and with other regions (FAA).
- The project also aims at **preparing the procurement of the systems needed to operate a PKI** and its associated trust framework in order to produce and manage digital certificates, why the project will prepare the Call For Tenders (CFT).

CP1 Timeline for PKI

Project launch
13 November 2018

Spring 2022
- DM1 Trust Framework Agreed
- DM2 Interop tests completed
- DM3 CFT material available

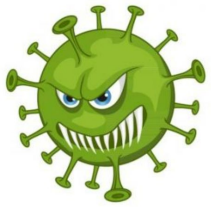
2022/Q4
EACP Initial Solution

December 2024
- DM4 Day-to-Day Operations contract signed
- DM5 Operational use

30 partners:
- 21 ANSPs
- 3 Airspace Users
- 3 Airports
- 2 MIL
- EUROCONTROL

Project deliverables and consultation

The process



Correction

Issues identified

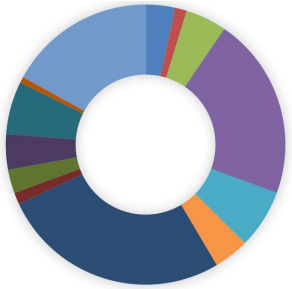
Steering group meetings

Project Deliverables

Final Steering group meeting

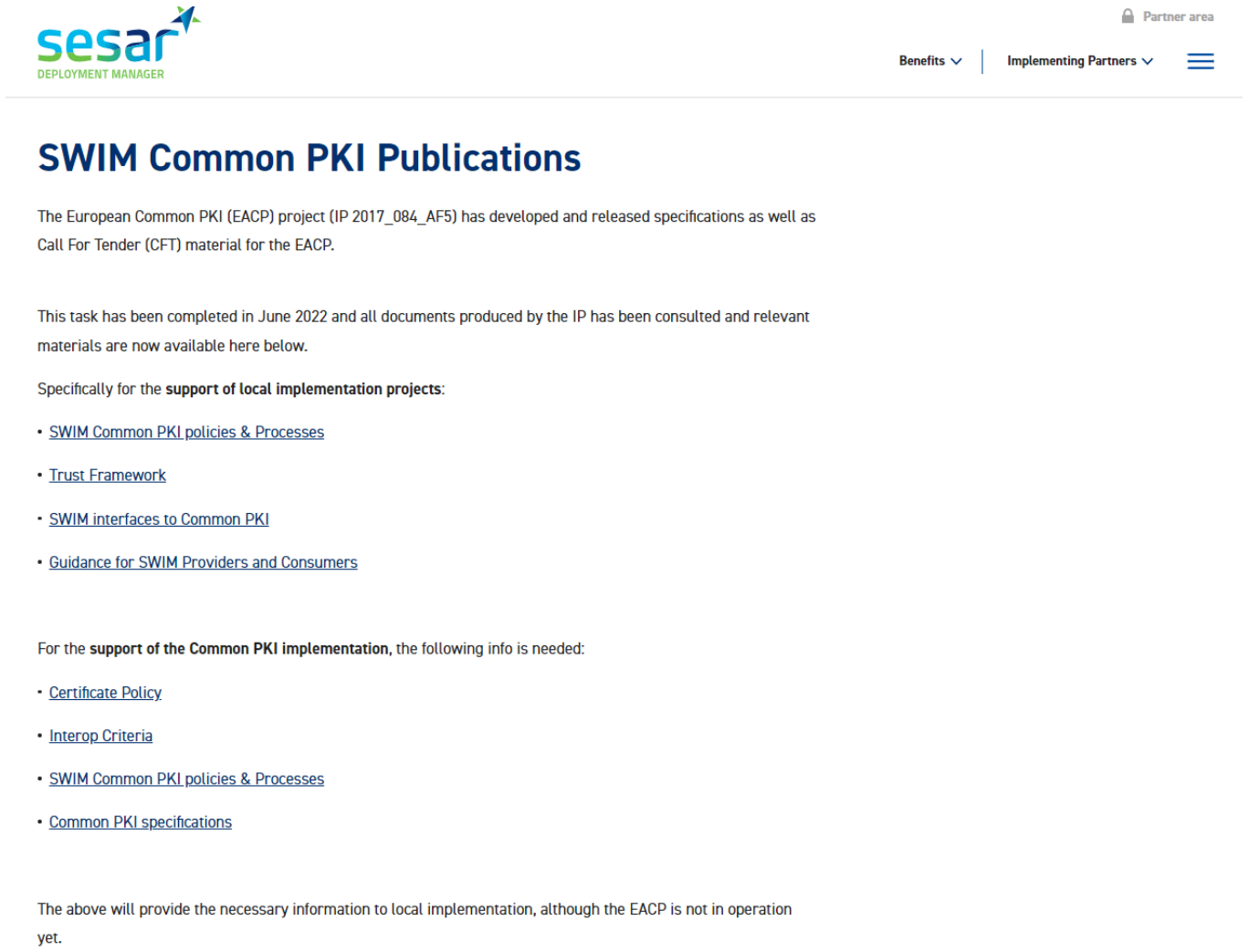
Action agreed

SDM Consultation platform



Project deliverables and consultation

Where to find



sesar DEPLOYMENT MANAGER

Partner area

Benefits | Implementing Partners

SWIM Common PKI Publications

The European Common PKI (EACP) project (IP 2017_084_AF5) has developed and released specifications as well as Call For Tender (CFT) material for the EACP.

This task has been completed in June 2022 and all documents produced by the IP has been consulted and relevant materials are now available here below.

Specifically for the **support of local implementation projects**:

- SWIM Common PKI policies & Processes
- Trust Framework
- SWIM interfaces to Common PKI
- Guidance for SWIM Providers and Consumers

For the **support of the Common PKI implementation**, the following info is needed:

- Certificate Policy
- Interop Criteria
- SWIM Common PKI policies & Processes
- Common PKI specifications

The above will provide the necessary information to local implementation, although the EACP is not in operation yet.

https://www.sesardeploymentmanager.eu/swim-common-pki-publications

Link to local implementation (AF 5.2.1)

Family Deployment Approach			
All stakeholders concerned choosing option A	Option A: Using digital certificates issued by the Common PKI (EACP) on application level	All stakeholders concerned choosing option B	Option B: Using own PKI installation interacting with the Common PKI (EACP)

Several local deployment options:

- Using the EACP solution
- Deploy local PKI
- Combination of the above…
  - Fulfilling the interoperability requirements

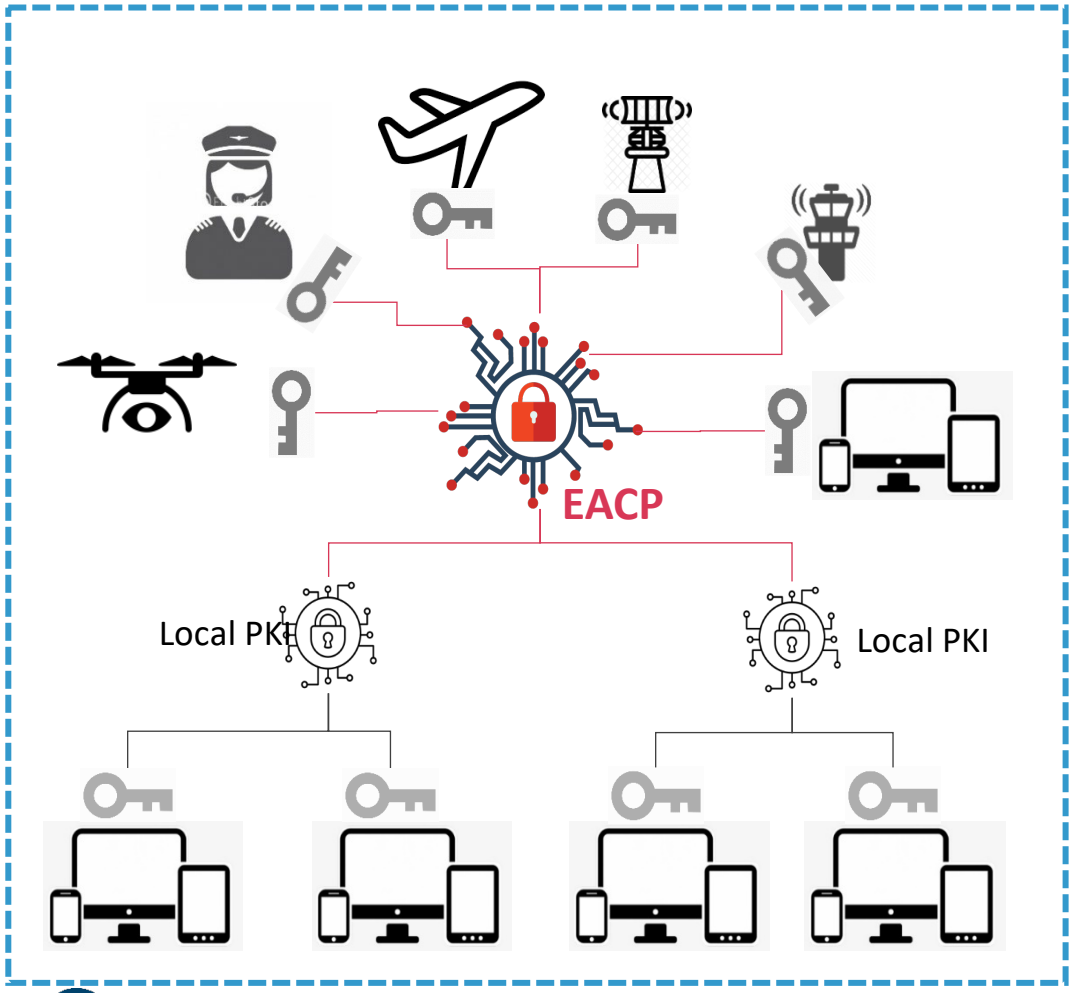
Specifically for the **support of local implementation projects**:

- SWIM Common PKI policies & Processes
- Trust Framework
- SWIM interfaces to Common PKI
- Guidance for SWIM Providers and Consumers

3.Introduction of EACP (European Aviation Common PKI)

European Aviation Common PKI (EACP)

A Building Block for the European Aviation Digital Infrastructure



Improve security throughout aviation value chain

Trust Framework (governance, policies, procedures)

Common service reducing costs & providing:

- Certificates
- Interoperability between existing PKI

EACP Target Solution

Main + Optional Services

EACP Main Services

commonly procured, technical services to be dimensioned according to the needs (number of certificates, CAs, …)

CP1 services

- Interop with Local PKI (SWIM)
- Certificates (SWIM)
- Interop with Local PKI (others)
- Certificates (others)

Mandatory EACP scope: SWIM

Extended scope: other certificates

Extended Use Cases: UC that can be covered by the same requirements / technical solution => No additional costs

Extended Technical Scope: UC that require additional requirements (e.g. potentially compliance to new standard, new CAs, etc.) => Potential additional costs

Optional services

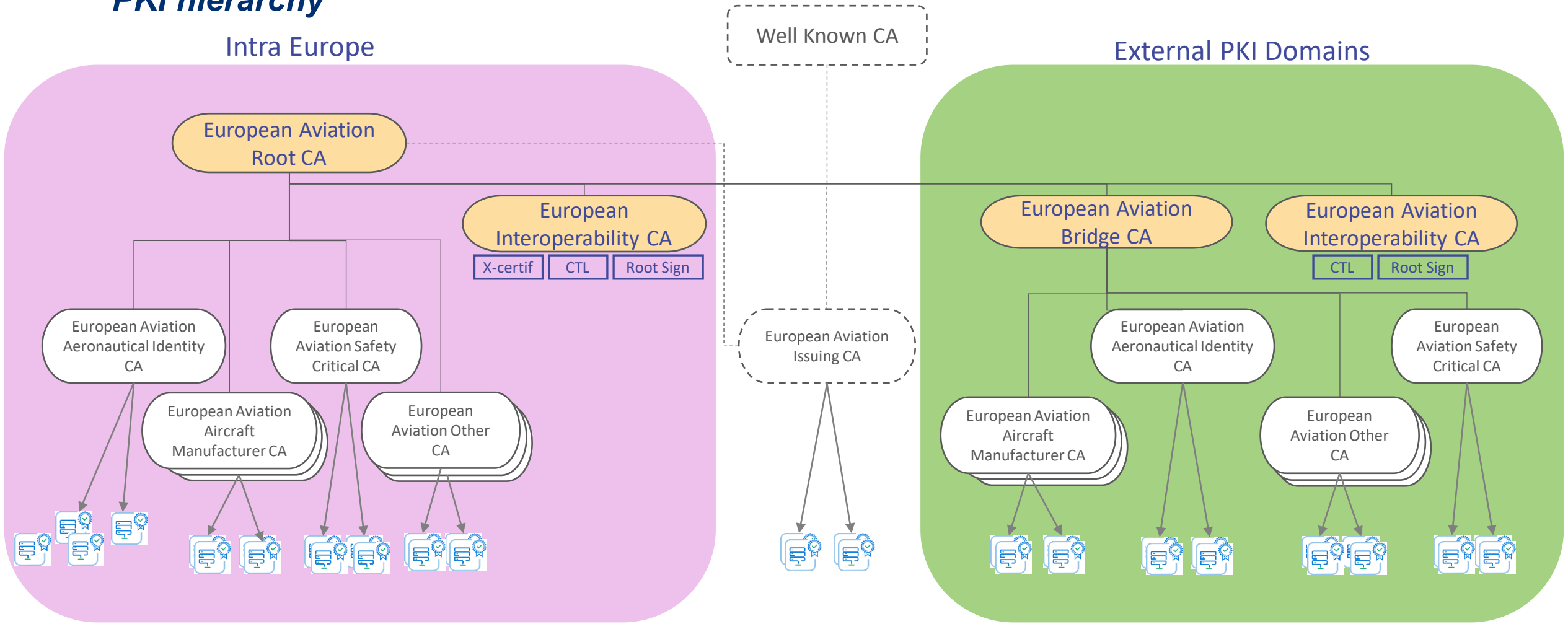
commonly procured for cost efficiency and paid by those needing them

- Public Trust Certificates
- Signing
- TimeStamping
- Validation

Local Registration Authority

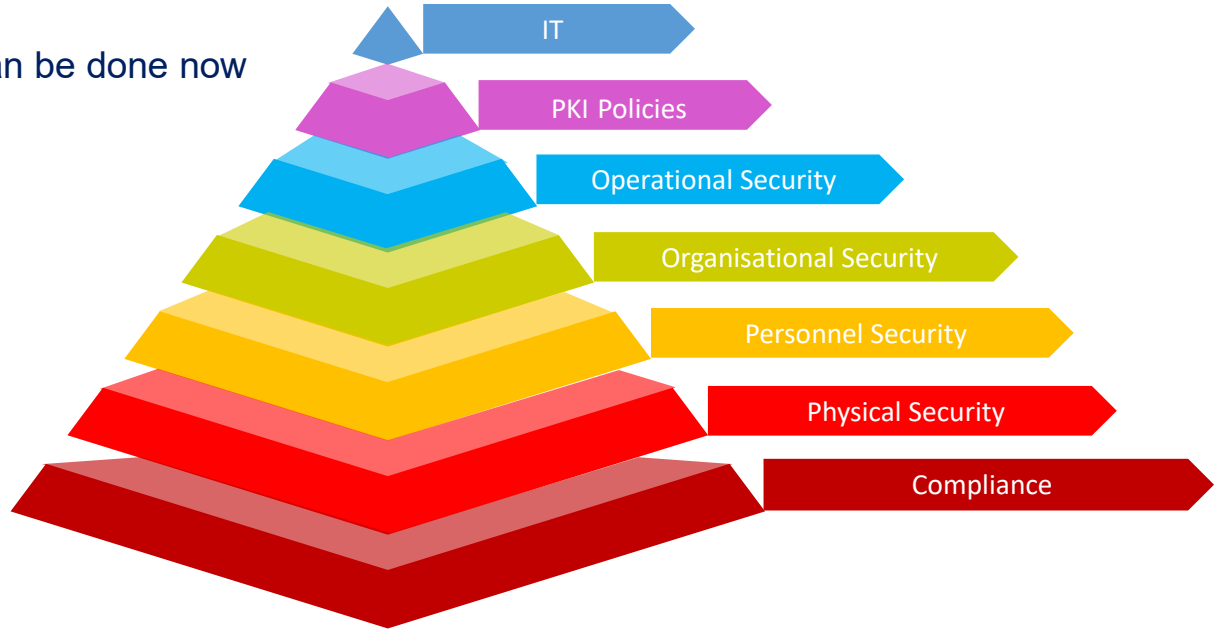
EACP Target Solution

PKI hierarchy



EACP Target Solution
Interop with Local PKI

- Identifies criteria for Local PKI interop:
  - D1.2 Annex A3.d
  - Assessment framework & procedures
  - Acceptable proof of compliance – to be refined
  - If Local PKIs already exist, an initial “pre-assessment” can be done now



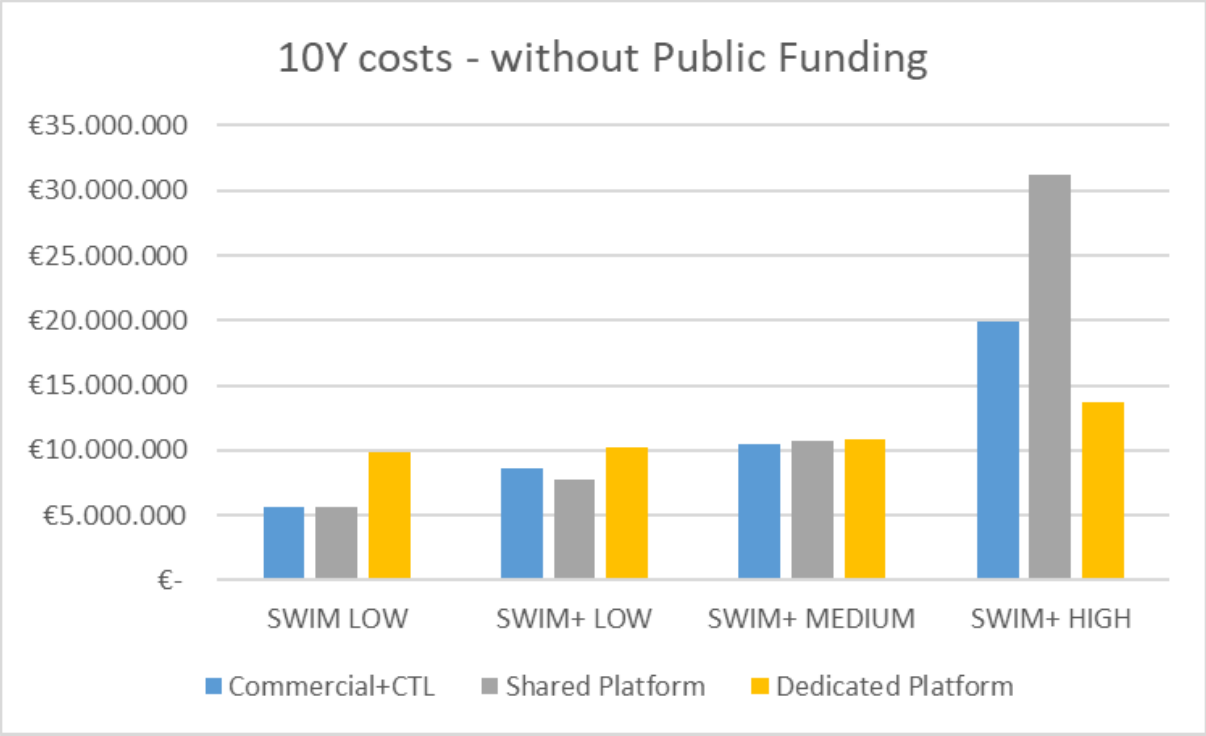
** The scope of this workshop is not to discuss local implementation*

EACP Target Solution
Implementation Options

	Mandatory Scope + Extended Use cases	Extended Technical Scope
Commercial PKI with CTL COTS certificate, certificate policy of the provider CTL signed by end entity certificate	Y	N
Shared PKI EACP on PKI provider platform used for CERTSuite and IOPSuite EACP Certificate Policy IOP supports Cross-certification and Bridge CA	Y	Y
Dedicated PKI EACP on dedicated platform used for CERTSuite and IOPSuite EACP Certificate Policy and Bridge CA	Y	Y

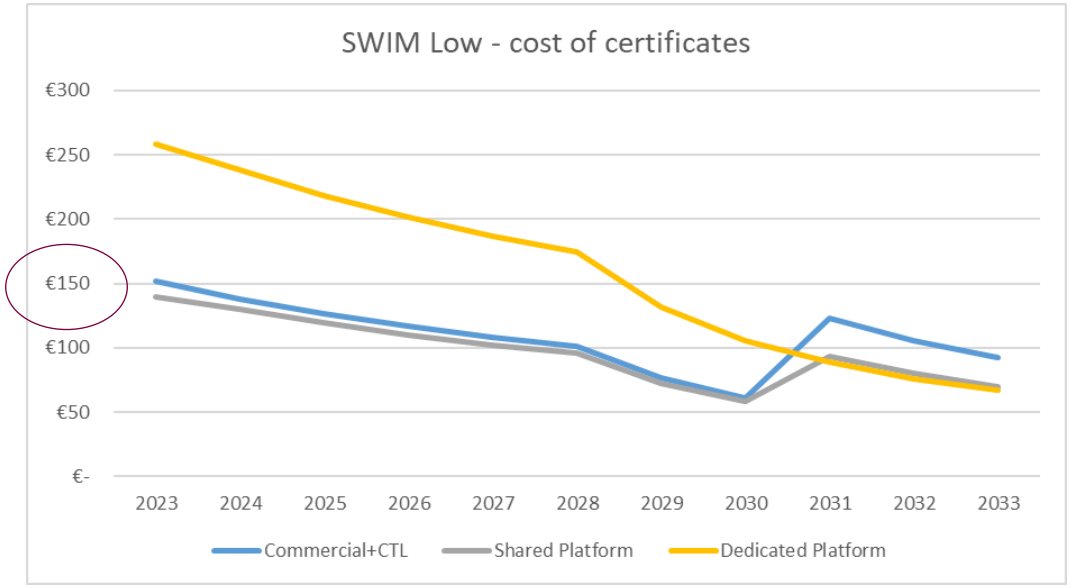
Different technical solutions, with different associated costs

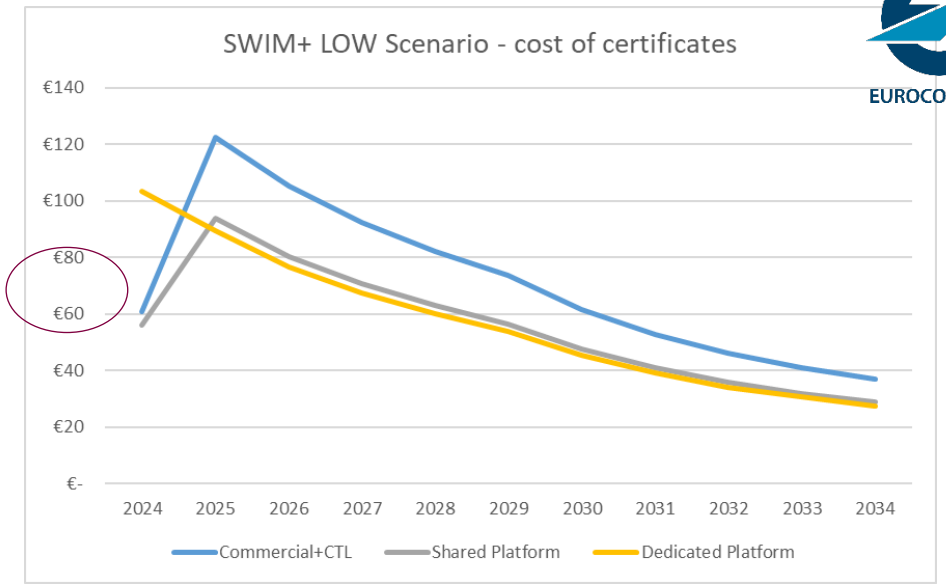
EACP Target Solution
Implementation options



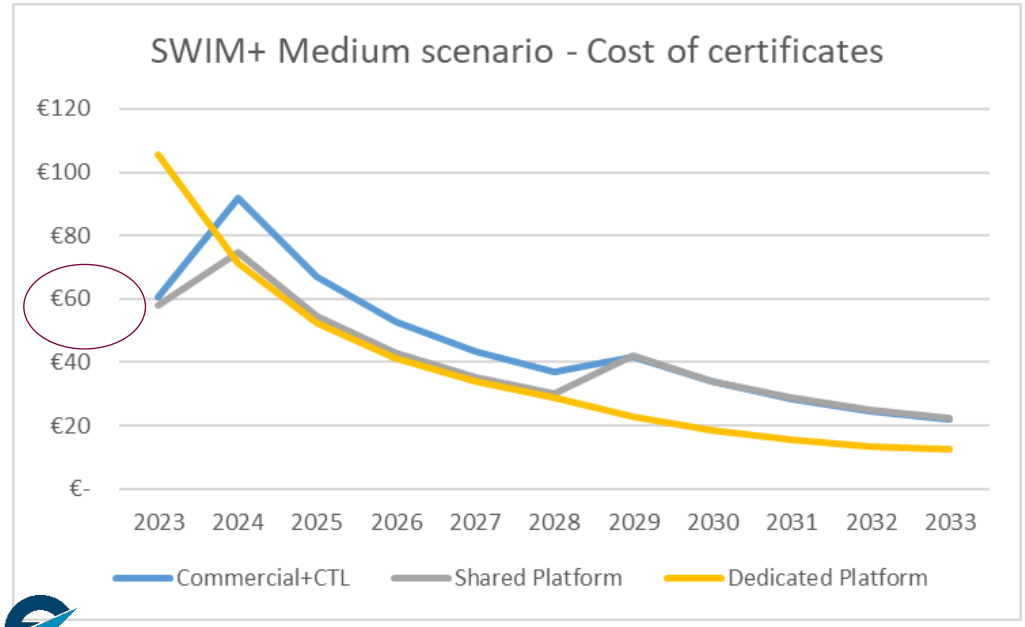
4 scenarios for volume of certificates needed:

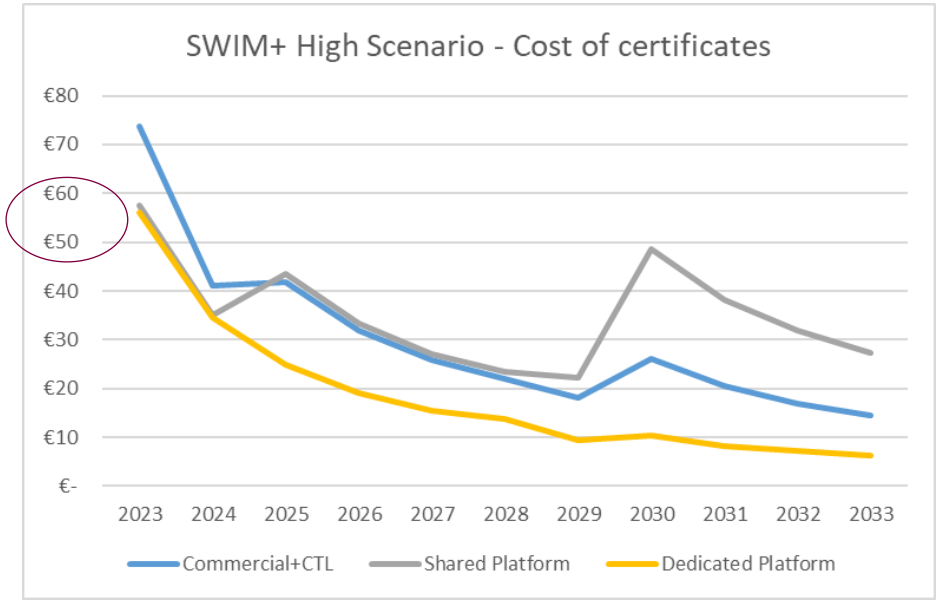
- SWIM LOW: SWIM only - from 2.000 to 8.000 certs
- SWIM+ LOW: SWIM and other use cases – from 5.000 to 20.000 certs
- SWIM+ MEDIUM: SWIM and other use cases – from 5.000 to 50.000 certs
- SWIM+ HIGH: SWIM and other use cases – from 10.000 to 200.000 certs



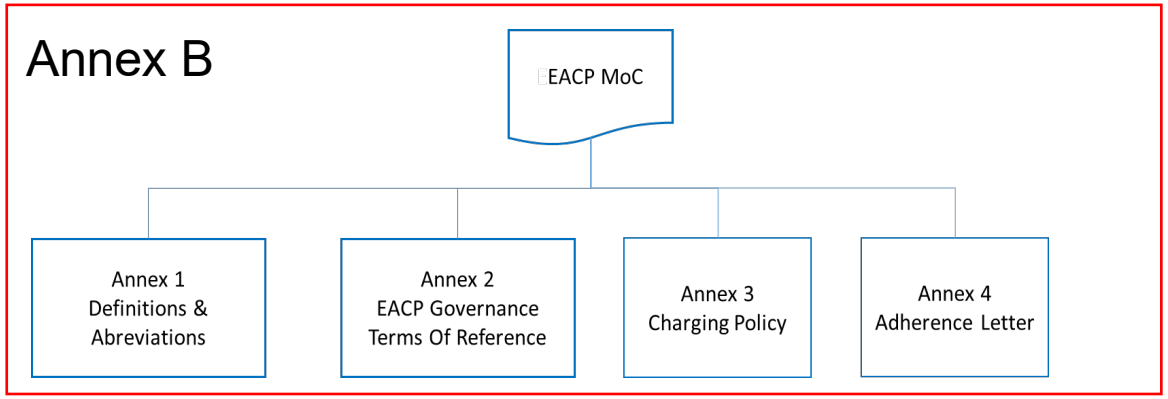


Evolution of the costs of private trusts certificates in the different scenarios





D1.2 – Final Trust Framework



Annex C – Implementation options

Annex A
EACP Technical Trust Framework

Annex A1 - EACP Membership & Users Agreements

Annex A2 – EACP Solution Description

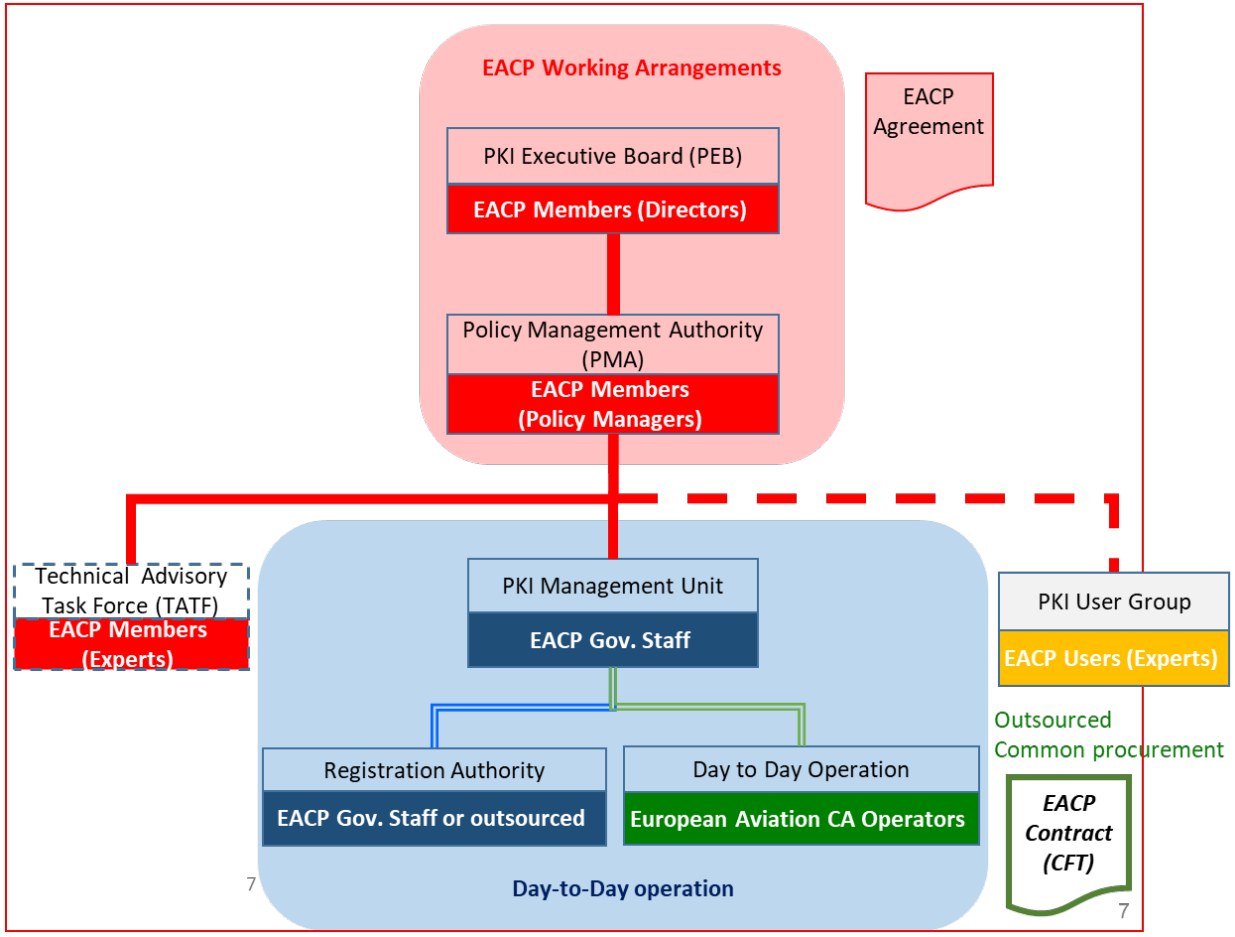
PKI Hierarchy
Catalogue Of Product & Services
Identity Assurance Levels
Guidance & Training Material

Annex A3 – EACP Policies & Processes

Annex A3.a – Certificate Policy
Annex A3.b – Certification Practices Statement
Annex A3.c – Processes and Procedures
Annex A3.d – Criteria & Methodology for Interoperability

Parts to be finalised by the EACP governance

EACP Target Solution
Internal governance



Memorandum of cooperation

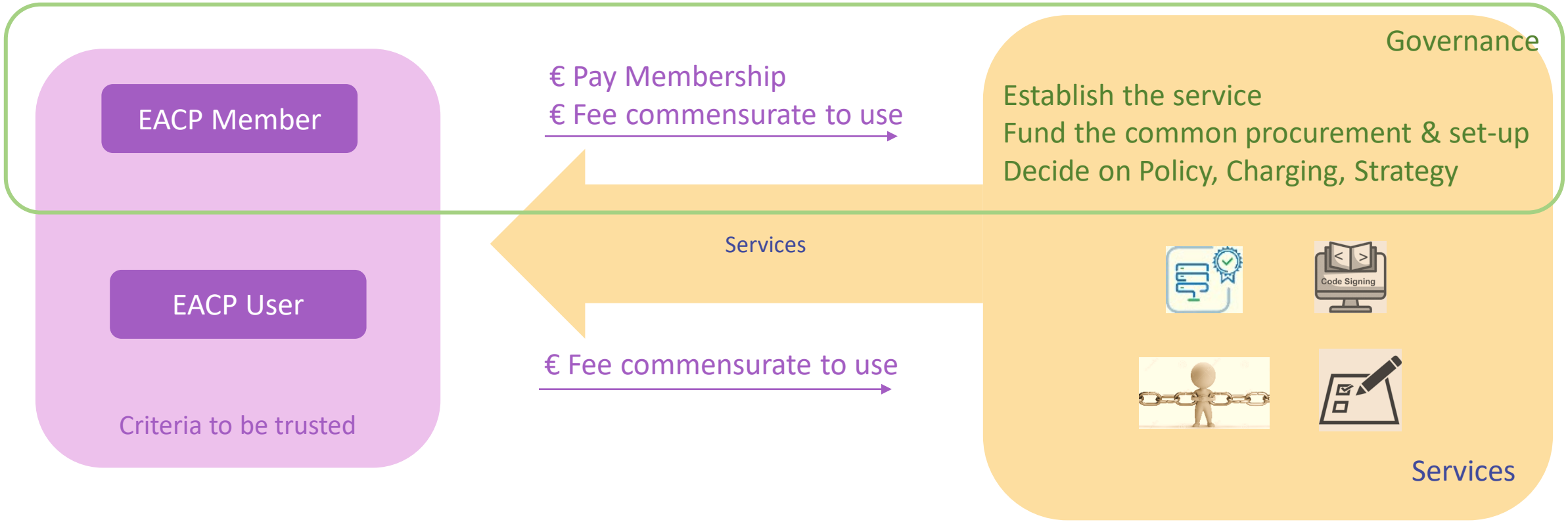
- Defines the purpose, objective, principles of EACP
- Establishes the governance
- Defines the model for service procurement
- Defines the legal provisions for EACP: confidentiality, liability, ethics, resolutions of disputes etc.

EACP Target Solution
EACP Participation

Governing Member 	**Following entities of EUROCONTROL Member States** • ANSP, AIM, MET • Airport • Airspace User • Military • CAA as a user (not as oversight) • Aviation manufacturer • Entity which main business is aviation

User    	**All the Above**
	+ on approval of EACP Governance
	• Entities of other States
	  • ANSP, AIM, MET
	  • Airport
	  • Airspace User
	  • Military
	  • CAA as a user (not as oversight)
	  • Entity which main business is aviation
	  • Aviation manufacturer
	• Supply chain to EACP Members

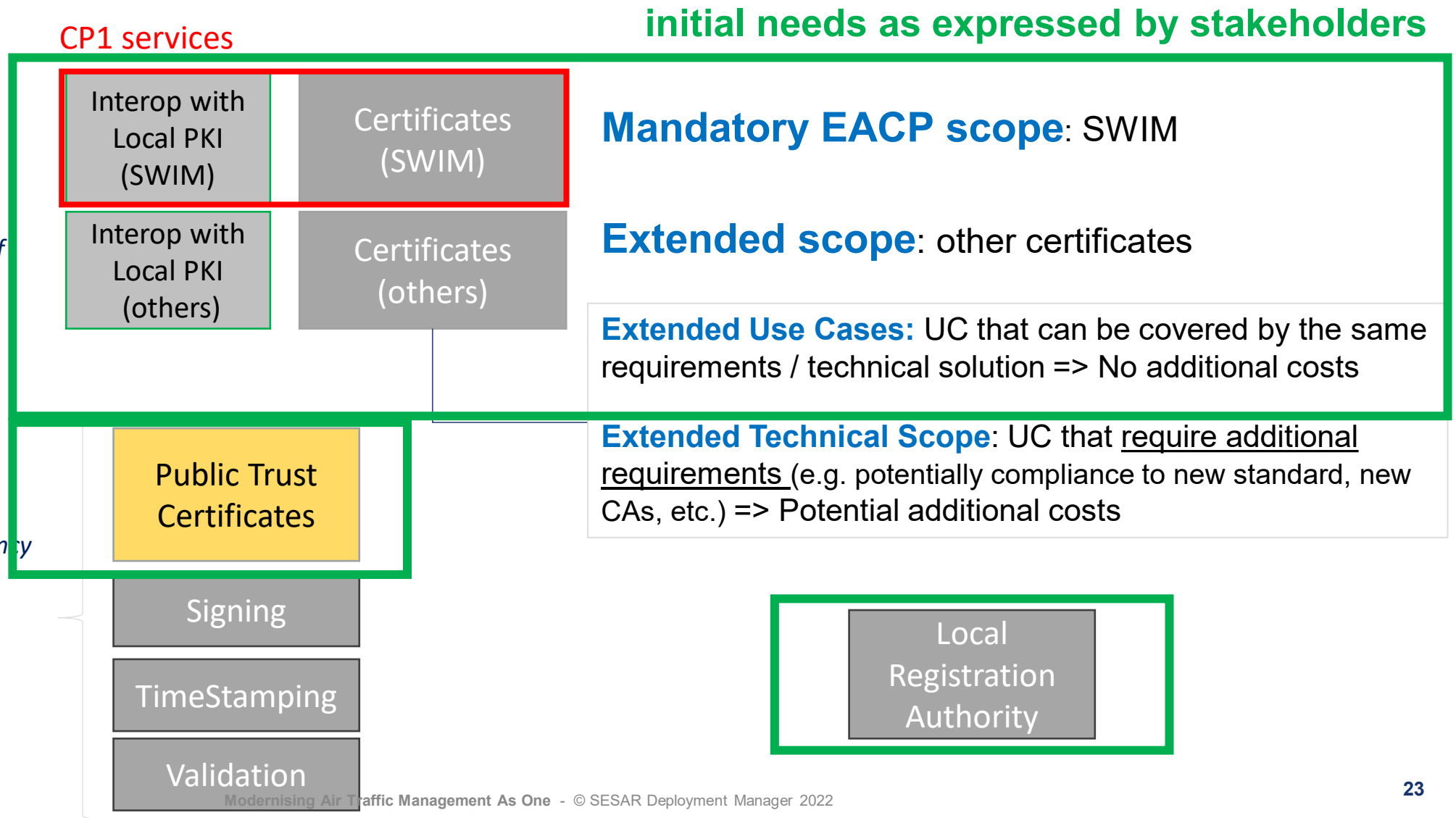
EACP Target Solution
Membership and charging



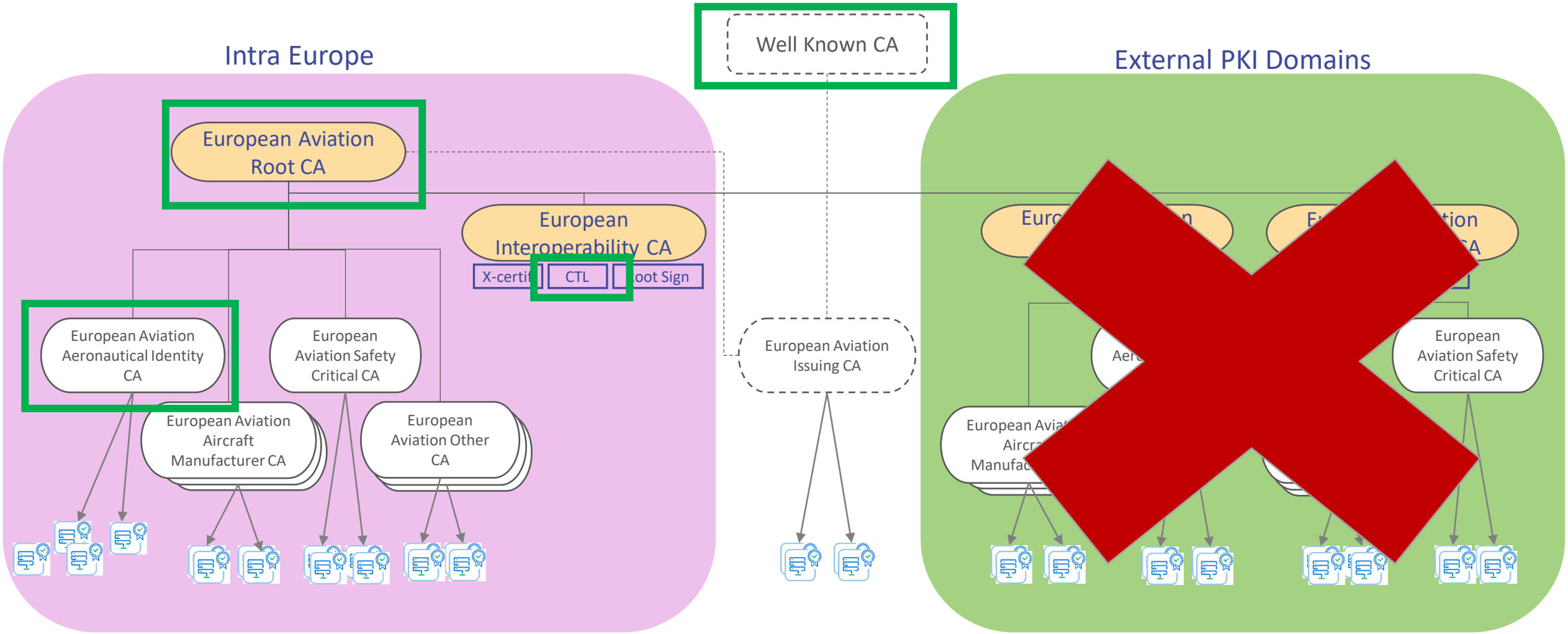
EACP Initial Solution Scope

EACP Main Services
commonly procured, technical services to be dimensioned according to the needs (number of certificates, CAs, …)

Optional services
commonly procured for cost efficiency and paid by those needing them



PKI Architecture – Initial step



EACP Initial Solution
Initial Implementation Option

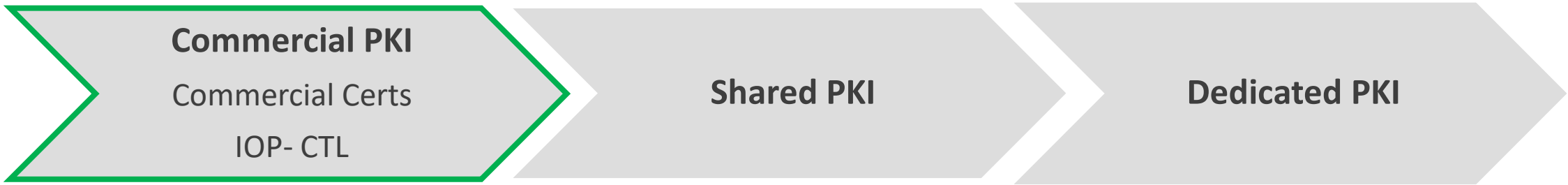
	Mandatory Scope Extended Use cases	Extended Technical Scope
Commercial PKI with CTL COTS certificate, certificate policy of the provider CTL signed by end entity certificate	Y	N

Option identified as most relevant for starting EACP (project discussions and various consultations)

- **No EACP CP**
- **Group buy of a batch of certs (different types) for EACP members**
- **Interop: Implement a CTL to managed by EACP Members**
- **Local Registration Authority: few candidates**

Based on needs, other options could be selected in the future

EACP Stepwise approach
Rationale



EACP Initial Solution

Commercial PKI
Commercial Certs
IOP- CTL

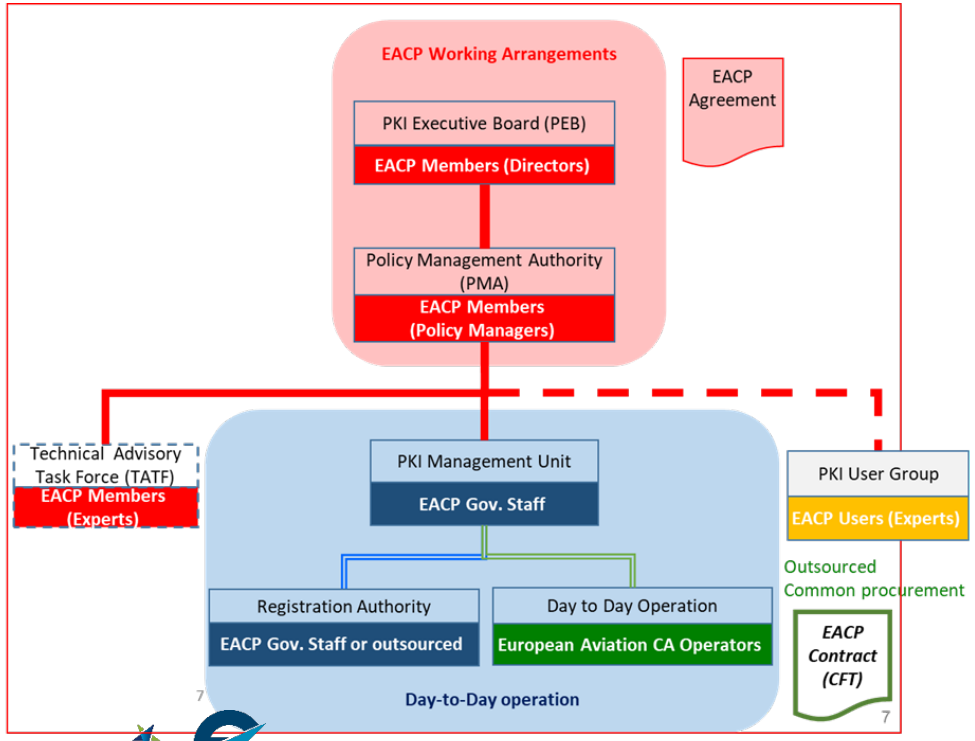
Current need

Shared PKI

When need arise (size or feature)

Dedicated PKI

When need arise (size or feature)



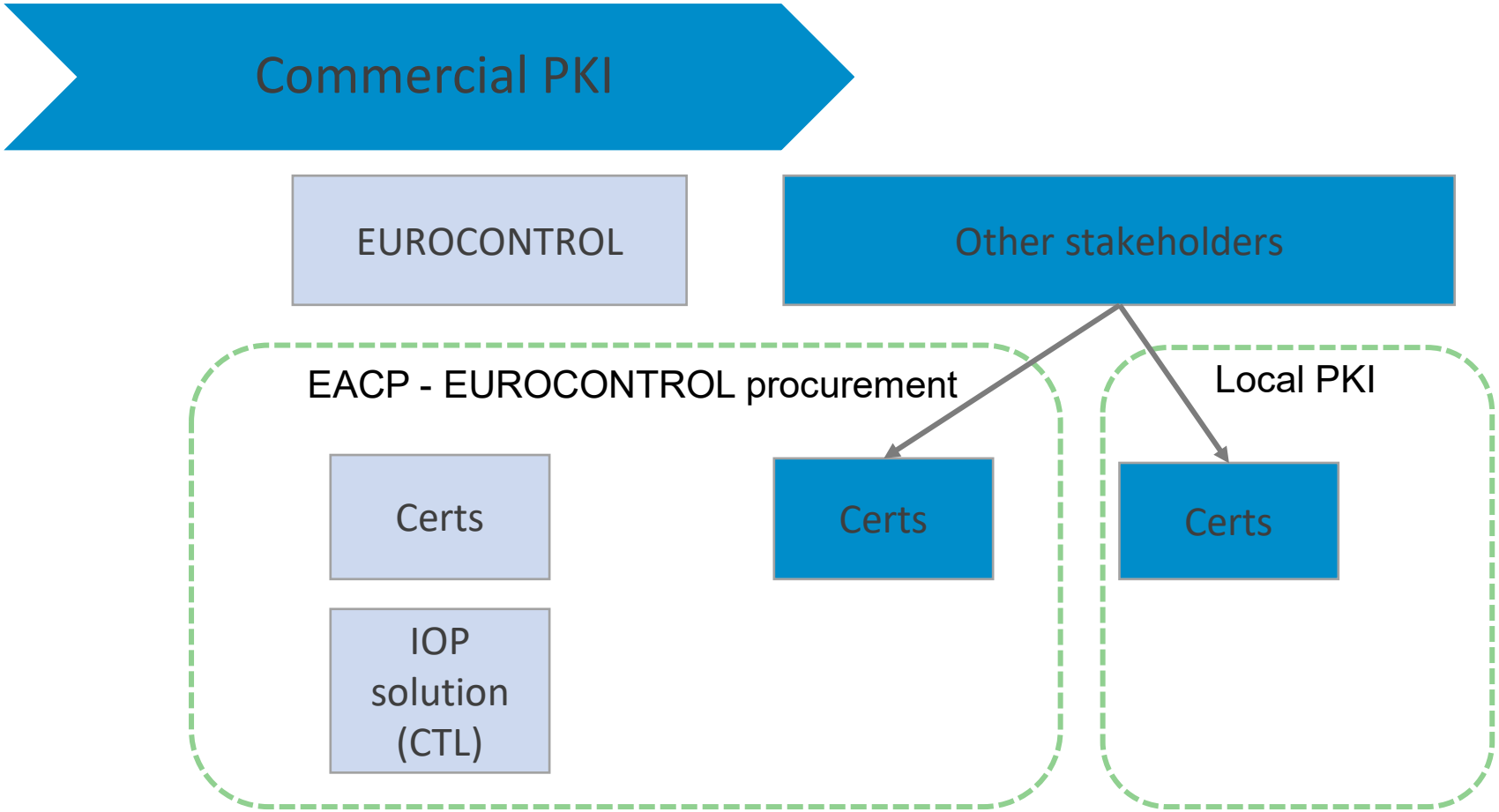
EACP Governance designed for target solution not suited for initial situation

- No EACP CP => limited role (and liabilities) of the PMA
  - Technical assessment of the EACP candidates
  - Ensure that the solution performs iaw users needs
- No investment, no complex technical management (Certs only)
- Project members + SDM consultation called for a simple, effective and commensurate internal governance

EACP Initial Solution

- Interim institutional set-up required to manage the Certificate Trust List
- Proposal to use existing working arrangements (e.g. sub-group of the NDTECH/CYBERG composed of EACP users only) to:
  - Agree on the list of stakeholders to be added to the EACP CTL
  - Provide feedback on the CTL technical solution and the PKI technical solution
  - Ensure that the solution performs iaw users needs
- EUROCONTROL ready to procure CTL and certs (using models such as ARTAS)
  - Technical steering from CYBERG (EACP users only)
  - SLA with users of certs and CTL
  - Charging mechanisms then straightforward (price per cert + fee for CTL + fee for LRA)

EACP Initial Solution



EACP Deployment Steps

Commercial PKI

Commercial Certs

IOP- CTL

Shared PKI

Dedicated PKI

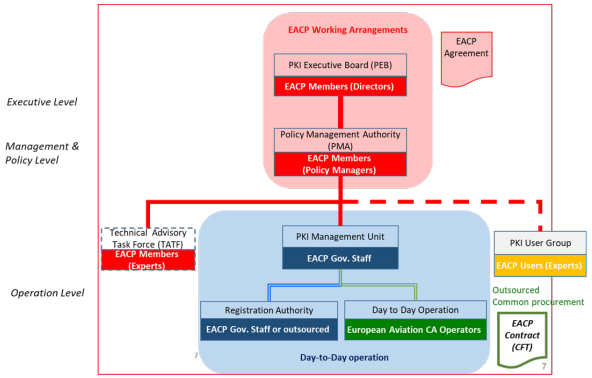
Current need

When need arise (size or feature)

When need arise (size or feature)

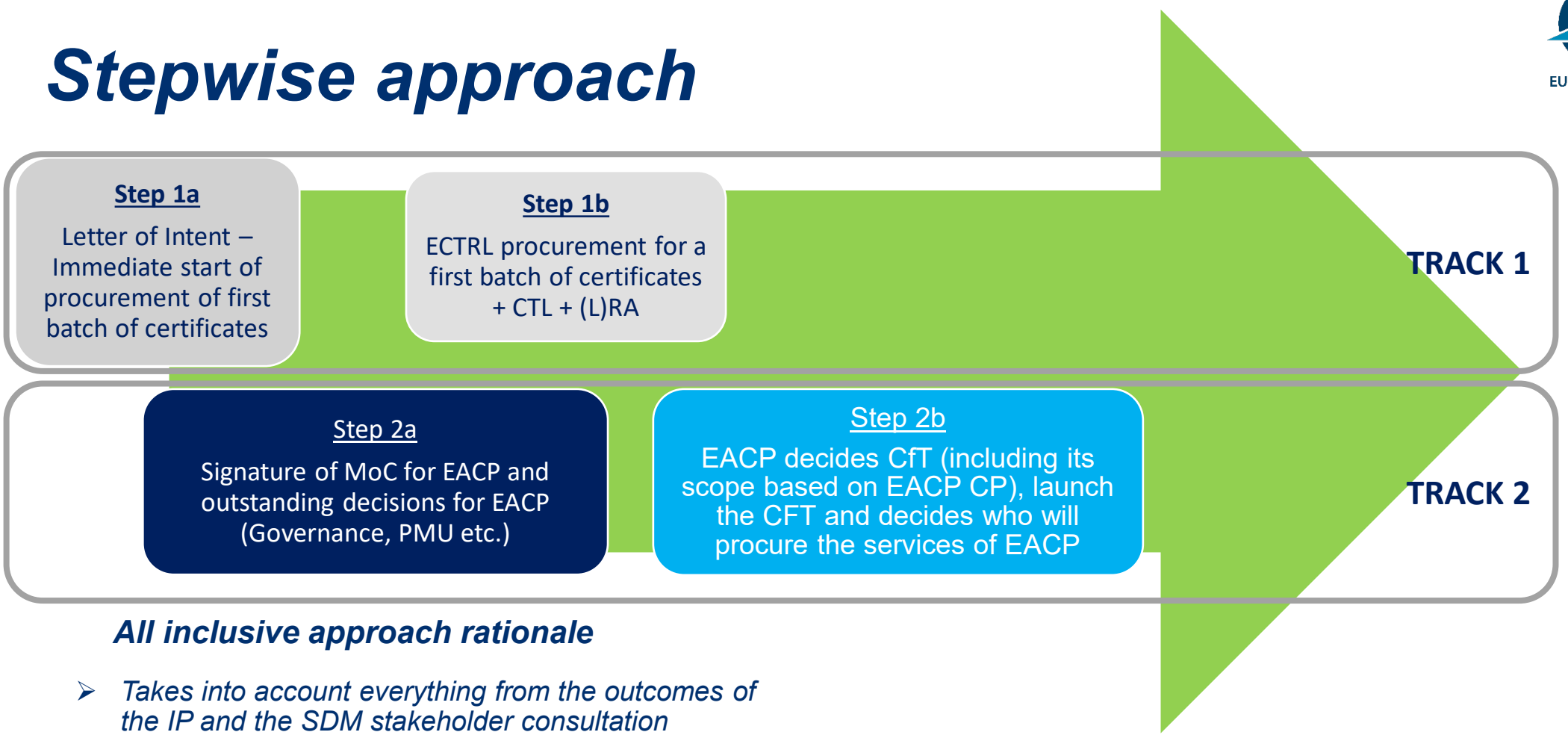
Steered by CYBERG
Operational immediately

Target governance (MoC)
To be set-up in parallel to EACP initial solution deployment)



Proposed approach and next steps for the deployment of EACP to fulfil family 5.1.1 requirements

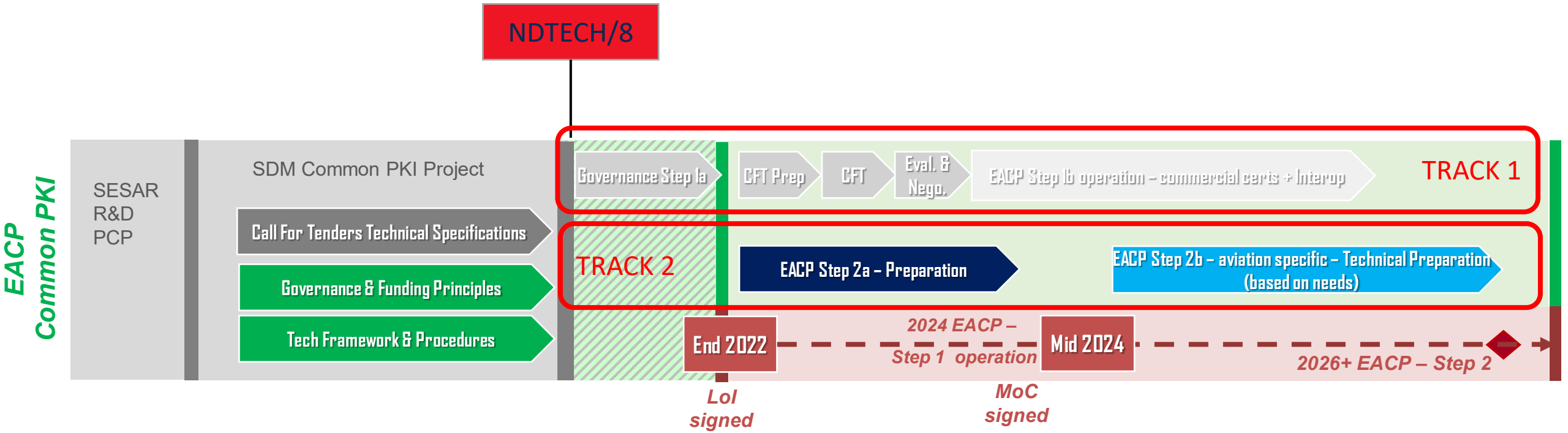
Stepwise approach



All inclusive approach rationale

- *Takes into account everything from the outcomes of the IP and the SDM stakeholder consultation*
- *Pragmatic approach towards fulfilling the CP1 req, limited need for certificates*
- *Preparation for potential needs of the future*
- *Takes into account EUROCONTROL need to renew its certificate contract in 2023*

Common Procurements Timeline



Track 1

- Step1a: T0 = Nov 2022
  - Agree on Letter of Intent content
  - Get early adopters intention formalised by signing the Letter of Intent (LoI)
  - Activate the NDTECH/CYBERG sub-group steering EACP Track 1
  - Initial steering:
    - Early adopters to identify their initial needs
    - Support finalising the Tech Specs of the CFT
    - Assessment of candidate Local PKIs and LRAs
  - Prepare and launch CFT
  - Based on winning Tender:
    - Commitment of early adopters: sign SLA with ECTRL
    - Contract signature
- Step1b:
  - Operate initial EACP
  - Assess new candidates

Track 2

- Step2a: T0 = Jan 2023
  - Set-up group of founding members
  - Finalise MoC
  - Sign MoC by founding members

- Step2b:
  - Activate the EACP Track 2 governance
    - Identify new needs
    - Approve EACP CP
    - Support finalising the Tech Specs of the CFT
  - Prepare and launch CFT
  - Based on winning Tender: Finalise relationships between governance / users and contractor
  - Operate EACP Track 2
  - Assess new candidates

Track 2
Decision open points for founding members

- Relationships of the governance with external bodies
- Procurement model
- Charging mechanisms

Next actions

- Inform NDTECH about progress and status and recommend:

  support the roadmap for EACP stepwise deployment to comply with EC 116/2021 CP1, stemming from the Implementation Project and the SDM stakeholder consultation

  agree to the creation of a sub-group of CYBERG to:
  - steer the deployment of the EACP initial solution
  - finalise the EACP MOC for the preparation of the deployment of the EACP target solution

  invite its members to indicate by end of November their willingness to sign the EACP Initial Solution Letter of Intent and **nominate** representatives to the dedicated sub-group of CYBERG

- SDM will continue to monitor the progress until full implementation, including track 2

THANK YOU