European Aviation Common PKI

Presentation by: Patrick MANA
EUROCONTROL
EATM-CERT Manager
Digital "passports" for aviation

Enhance security of information exchanges
Aviation Trust Framework
Common service reducing costs

Part of EC 2021/116 (Common Project1)
Why a European aviation PKI?

Specific …

- Certificate Interoperability
  Recognised by other European & Global trusted parties

- Aviation specific PKI configuration
  Aviation PKI standards, safety

- Dedicated to Aviation Users only
  Best practice to limit cross-domain cyber threats

But based on Commercial Off the Shelf solution

- State of the Art Solution
  TimeStamping, Signing, Validation, Automation, Authorisation

- Offload users of PKI deployment pain
  Delegate design, implementation & day-to-day operations

- Financially Attractive
  Common Service for all Aviation Stakeholders
  Public funding - tbc
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

Targeting hundreds of users

We are as strong as the weakest link
Roadmap

**PCP Mandate**

- Prepare Call for Tenders
- Define Governance & Funding Principles
- Prepare Tech Framework & Procedures

**European PKI – CEF Project Preparation**

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

**European Aviation Common PKI 2022-20**

- To be retendered periodically
- Possible Public Funding
- Devt Operation
- Governance Set up

**CEF**
EACP

Product portfolio

European Aviation Common PKI Product Portfolio

- RASuite
- IOPSuite
- ValidSuite
- SignSuite

FlexSuite
CertSuite

ATIEC 2021
EACP Trust Framework

Operational Trust Framework

Fully aligned with ICAO Trust Framework

Governance Trust Framework

Registration

Relying Party Agreement

EACP

Procedures

EACP Policies

EACP Technical Framework

PKI System Design And Implementation

Validation/Publication

Certification

User Agreement

Certificate Policy

Certificate Practice Statement

PKI Specification

PKI Governance Model

Key Management Policy & Procedures

EACP Governance

Membership Agreement

Charging Policy

EACP Policies

User Agreement

Certificate Policy

Certificate Practice Statement

Relying Party Agreement

PKI Governance Model

PKI Specification

PKI System Design And Implementation

Key Management Policy & Procedures

Audit

Smart.

Secure.

Shareable.

Aviation Information.
Draft governance

EUROCONTROL

WORKING ARRANGEMENTS

ND TECH
NM Technical Directors

IMT
Information Management managers & Experts

CYBERG
Cybersecurity Experts

EACP Working Arrangements

PKI Executive Board (PEB)

EACP Members (Directors)

Policy Management Authority (PMA)

EACP Members (Policy Managers)

Technical Advisory Task Force (TATF)

EACP Members (Experts)

PKI Management Unit

EACP Gov. Staff

Registration Authority Services

EACP Gov. Staff or outsourced

Day to Day Operation

European Aviation CA Operators

Day-to-Day operation

Outsourced

Common procurement

EACP Contract (CFT)

PKI User Group

EACP Agreement

Strategic coordination
Membership & charging

EACP Member

EACP User

Criteria to be trusted

€ Pay Membership
€ Fee commensurate to use

Governance
Establish the service
Fund the common procurement & set-up
Decide on Policy, Charging, Strategy

Services

€ Fee commensurate to use
PKI Architecture

Intra Europe

European Aviation Root CA

European Interoperability CA

European Aeronautical Identity CA

European Aviation Safety Critical CA

European Aviation Aircraft Manufacturer CA

European Aviation Other CA

Well Known CA

External PKI Domains

European Aviation Bridge CA

European Aviation Interoperability CA

European Aviation Aeronautical Identity CA

European Aviation Aircraft Manufacturer CA

European Aviation Safety Critical CA

European Aviation Other CA

European Aviation Issuing CA

X-cert, CTL, Root Sign

European Aviation Safety Critical CA
Global Interoperability

Interoperability between certificates
Relationships
EACP / IATF

- Technical:
  - Global interoperability of various solutions
  - Tests between FAA and EUROCONTROL
ESPHOC Overview

EUROCONTROL Cloud Lab

FAA CyTF Lab

Florida Test Bed

Use cases

- **certificates**
  - AMHS
  - A-CDM
  - SWIM Registry
  - NM B2B
  - VoIP
  - Aircraft
  - SWIM
  - Remote TWRs

- **Client/Server**
  - AIM/AIP
  - Remote sensors
  - MET

- **Proof of identity**
  - CNS
  - Surveillance

- **Object Signing**
  - Proof of origin

- **Personal Certificate**
  - EFB
  - Pilot License
  - Badge

- **Smart. Secure. Shareable. Aviation Information.**
  - SWIM Registry
  - SWIM
  - +++
  - C/CDM
  - Remote TWRs

- **Feedback**
  - CNS
  - SBAS
  - Future Datalink

- **Short term**
- **Long Term**
Challenges

We are as strong as the weakest link!

Scope – what are users’ needs?

Ability to invest at COVID time

Initial financing low if limited number of early adopters

Wide deployment needed to secure the network