OBJ

INF10.2 — Stakeholders' SWIM PKI and cyber security

Download Progress Report

This Objective is dealing with the Stakeholders' SWIM PKI and cybersecurity. It aims at implementing basic/generic public key infrastructure management at each civil or military stakeholder, in line with their own Security Management System approved by their National Supervisory Authority (NSA). The local implementation may differ depending on whether the stakeholders will become a CA (Certificate Authority) themselves or use the European Common Aviation PKI (EACP) to generate certificates.

The stakeholder's local implementation includes two options (the options are also addressed in the description of the individual SLoAs):

• If the stakeholder decides to develop its own PKI:
o definition of local policies and procedures for authorising and mandating local organisation to do certificate management in compliance with EACP policies;
o implementation of audit programmes ensuring continuous compliance with common and local policies and standards;
o implementation of its own local PKI while benefiting from the interoperability with other PKIs by using the EACP solution;
o adaptation of systems (equipment and procedures) to use local certificates and EACP services.

• If the stakeholder decides to use the EACP solution
o Use of EACP policies and procedures for authorising and mandating local organisation to use EACP certificates and services;
o implementation of audit programmes ensuring continuous compliance with EACP policies and standards;
o adaptation of systems (equipment and procedures) to use EACP solution;

• Whatever the decision will be, the following activities must be operated:
o training of technical personnel;
o monitoring and control, e.g. establish a local or multi-stakeholders Security Operations Centre (or equivalent) to monitor and protect the IT systems against cyber-attacks.

Combining both options is a valid and acceptable approach (they are not exclusive) as:
• National regulation may impose to use a national PKI for critical infrastructure or operator of essential service or government-related organisations;
• Some stakeholders may already have a PKI that would have to be upgraded to be auditable and conform with EACP solution and they may wish to keep on using it;
• Some stakeholders may decide to implement a local PKI for internal or specific uses and use EACP for other purposes.

System requirements:

Stakeholders shall implement, on one hand a Public Key Infrastructure (PKI) and, on the other hand cyber-security monitoring and control means. To implement the PKI, stakeholders have two main options:

• To use the European Aviation Common PKI (EACP) solution. In such case, stakeholders must:
o define the local framework to use digital certificates (policies, procedures);
o implement audit programmes to ensure that their organisation and its policies & procedures are auditable and that consequently they can be trusted to use EACP certificates and thus by parties with whom information exchanges are secured using EACP digital certificates;
o adapt their systems to use the EACP solution (e.g. access to EACP certificate publication and validation services);
o train their staff to ensure that they have the required demonstrated level of competence to use EACP digital certificates and services.

• To deploy their own local PKI and to benefit from the EACP solution only to ensure the interoperability of their local PKI with other stakeholders. In such case, stakeholders must:
o define the local framework to deploy their local PKI (policies, procedures). If stakeholders want to benefit from the EACP interoperability and validation services, they will have to ensure that the policies and procedures of their local PKI is also compliant with EACP framework trust framework;
o implement audit programmes to ensure that their organisation and its policies & procedures are auditable and that consequently they can be trusted to benefit from EACP interoperability service and thus by parties with whom information exchanges are secured using EACP interoperability and validation services;
o adapt their systems to use their local PKI solution as well as EACP validation service;
o train their staff to ensure that they have the required demonstrated level of competence to use their local digital certificates and EACP interoperability and validation services.

Combining both options is a valid and acceptable approach (they are not exclusive) as:
o National Regulation may impose to use a national PKI for critical infrastructure or operator of essential service or government-related organisations;
o some stakeholders may already have a PKI that would have to be upgraded to be auditable and conform with EACP solution and they may wish to keep on using it;
o some stakeholders may decide to implement a local PKI for internal or specific uses and use EACP for other purposes.

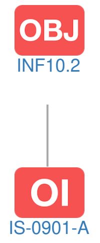
NOTE: For a description of the EACP solution, see Family 5.1.1 of the Deployment Programme.

NOTE FOR MILITARY AUTHORITIES: It is the responsibility of each military authority to review this Objective IN ITS ENTIRETY and address each of the SLoAs that the military authority considers RELEVANT for itself. This has to be done on top and above of the review of "MIL" SLoAs which identify actions EXCLUSIVE to military authorities.

Edition	2022
Stakeholders	Air Navigation Service Provider / Airport Operator / Airspace Users / Network Manager
Type	CP1
Scope	ECAC+
Status	Active

Context

Related Elements



Applicability Area(s) and Timescales

Applicability Area 1:	All EU SES States *(All SES EU States)*
Applicability Area 2:	Georgia, Israel, Moldova, Montenegro, Serbia, United Kingdom

Timescales	From	By	Applicable to
Initial Operational Capability	01-01-2021	-	Applicability Area 1 + Applicability Area 2
Full Operational Capability / Target Date	-	31-12-2025	Applicability Area 1 + Applicability Area 2

Links to ATM Master Plan Level 2

OI Operational Improvment Steps

Code	Title	IOC	FOC	Related Elements
IS-0901-A	SWIM for sharing G/G data, traffic flow management information and aeronautical information	31-12-2023	31-12-2029	SOL OI EN OBJ DS PCP ICAO

SOL Links to SESAR Solutions

Code	Title	Program	Related Elements
No record found			

PCP Links to PCP ATM Sub-Functionalities

Code	Title	Related Elements
No record found		

ICAO ICAO Block Modules: No associated data

References

Applicable legislation
Regulation (EU) 2021/116 on the establishment of the Common Project One
Applicable ICAO Annexes and other references
None
Deployment Programme 2022
Family 5.2.1 - Stakeholders' SWIM PKI and cybersecurity
Operating Environments
-

Expected Performance Benefits

Safety	-
Capacity	-
Operational efficiency	-
Cost efficiency	-
Environment	-
Security	-

Stakeholder Lines of Action

Code	Title	From	By	Related Enablers
ASP01	Local PKI framework	01-01-2021	31-12-2025	
ASP02	Continuous PKI audit process has been set up	01-01-2021	31-12-2025	
ASP03	Adapt systems to use PKI	01-01-2021	31-12-2025	
ASP04	Implement local PKI	01-01-2021	31-12-2025	
ASP05	Training	01-01-2021	31-12-2025	
ASP06	Implement cyber monitoring and control	01-01-2021	31-12-2025	
APO01	Local PKI framework	01-01-2021	31-12-2025	
APO02	Continuous PKI audit process has been set up	01-01-2021	31-12-2025	
APO03	Adapt systems to use PKI	01-01-2021	31-12-2025	
APO04	Implement local PKI	01-01-2021	31-12-2025	
APO05	Training	01-01-2021	31-12-2025	
APO06	Implement cyber monitoring and control	01-01-2021	31-12-2025	
USE01	Local PKI framework	01-01-2021	31-12-2025	
USE02	Continuous PKI audit process has been set up	01-01-2021	31-12-2025	
USE03	Adapt systems to use PKI	01-01-2021	31-12-2025	
USE04	Implement local PKI	01-01-2021	31-12-2025	
USE05	Training	01-01-2021	31-12-2025	
USE06	Implement cyber monitoring and control	01-01-2021	31-12-2025	
NM01	Local PKI framework	01-01-2021	31-12-2025	
NM02	Continuous PKI audit process has been set up	01-01-2021	31-12-2025	
NM03	Adapt systems to use PKI	01-01-2021	31-12-2025	
NM04	Implement local PKI	01-01-2021	31-12-2025	
NM05	Training	01-01-2021	31-12-2025	
NM06	Implement cyber monitoring and control	01-01-2021	31-12-2025	
MET01	Local PKI framework	01-01-2021	31-12-2025	
MET02	Continuous PKI audit process has been set up	01-01-2021	31-12-2025	
MET03	Adapt systems to use PKI	01-01-2021	31-12-2025	
MET04	Implement local PKI	01-01-2021	31-12-2025	
MET05	Training	01-01-2021	31-12-2025	
MET06	Implement cyber monitoring and control	01-01-2021	31-12-2025	

Supporting Material

Title	Related SLoAs
SDM - Standardisation and Regulation support to CP1 deployment 2021, Deliverable D1.1.1 07/2021 https://www.sesardeploymentmanager.eu/publications/deployment-programme	APO01, APO02, APO03, APO04, APO05, APO06, ASP01, ASP02, ASP03, ASP04, ASP05, ASP06, MET01, MET02, MET03, MET04, MET05, MET06, NM01, NM02, NM03, NM04, NM05, NM06, USE01, USE02, USE03, USE04, USE05, USE06

Consultation & Approval

Working Arrangement in charge	-
Outline description approved in	-
Latest objective review at expert level	-
Commitment Decision Body	-
Objective approved/endorsed in	-
Latest change to objective approved/endorsed in	-