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

Why this initiative?

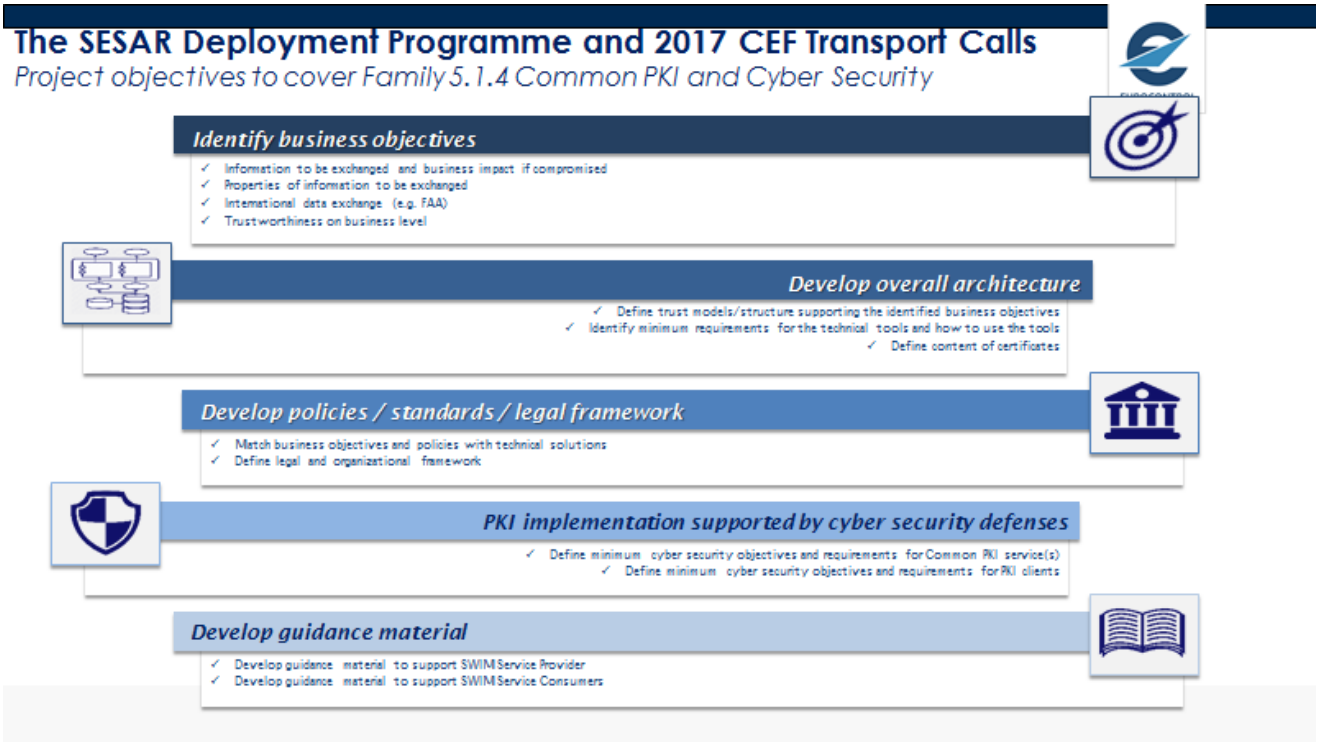
The local deployment of a Public Key Infrastructure (PKI) at a stakeholder is a well-established technical undertaking that can rely on proven technology and best practices. Even the basic processes and policies required to operate the PKI locally are a local issue in the first place. However to establish the required trust in the other parties on a European scale, a commonly agreed set of processes and policies is required especially with the aim to ensure the interoperability of digital certificates.

Description/Scope/Objective

- 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 in the family 5.1.4. 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.

- 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 project also aims at developing 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), user interfaces, systems supporting the Registration Authority and Policy Management Authority roles. These systems will be developed through procurement, which will make use of the EUROCONTROL procurement process through a Call For Tenders (CFT) based upon specifications developed within the project. The system developments will be based on existing and mature COTS Hardware and Software.



Tasks & Deliverables

1. Develop the Trust Framework policies and procedures
    - Define the governance structure (in alignment with SWIM governance)
    - Define funding/charging policy
    - Set-up the Policy Management Authority (PMA) (Terms Of Reference (ToR), procedures)
    - Develop/approve the initial Certificate Policy/Certification Practices Statement(s)
    - Develop the Membership Agreement
    - Develop interoperability framework (criteria, checklist)
    - Ensure interoperability with others PKIs, e.g. USFB
    - Set-up the Registration Authority (RA) (tools and procedures)
2. Develop Common PKI specifications (for both development and operations)
    - Develop high-level architecture
    - Develop the technical part of the CFT:
        - Functional Technical Specifications (including certificates specs)

- Statement of Work
- Service Level Agreement

3. Define the (SWIM) interfaces to the Common PKI, e.g.
    - Define Relying Parties interface
    - Define Users interface
    - Define validation interfaces (e.g. OCSP interface (Online Certificate Status Protocol), CRL interface (Certification Revocation List))
    - etc.
4. Launch a CFT under a common procurement process
    - Develop the Common Procurement Framework
    - Develop the contractual part of the CFT
    - Set-up CFT review/comment process (including meeting)
    - Publish Updated CFT
5. Assess tenders and select winning tender
    - Conduct the technical and financial assessment
    - Select/publish the winning Tender
    - Negotiate/finalise the Contract
6. Develop the Common PKI contract (from contract signature until acceptance)
    - Contract Management
    - Review and approve contractor's deliverables
    - Attend and approve lifecycle milestones
    - Approve the system acceptance review
7. Prepare for operations
    - Develop guidance for SWIM service providers
    - Develop guidance for SWIM service consumers
    - Training
    - Validation with Stakeholders
8. Project Management

Administrative Information

Project lead: Eurocontrol

Duration: Q3/2018-Q4/2022, to be refined by the project partners