D6.1 and D6.2 Guidance for SWIM Service Providers and Consumers

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	Guidance for SWIM Service Providers and Consumers
Deliverable ID	D6.1 and D6.2
Edition	1.2
Template Version	01
Task contributors	

Please complete the advanced properties of the document

Abstract

This document is the Initial guidance for SWIM Service Providers and Consumers to use the European Aviation Common PKI (EACP) solution developed by the project "SWIM Common PKI and policies & procedures for establishing a trust framework".

The project plan identifies that Task 6 has to produce two deliverables:

- D6.1 – Guidance for SWIM service providers;
- D6.2 – Guidance for SWIM users.

However, Task6 came to the conclusion that it was useless to separate the guidance into two documents as a significant part applies to both SWIM service providers and users.

Consequently, this document is both D6.1 and D6.2.

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
Alessandro Manzo ENAV	Project contributor Task leader	10/11/2021
Patrick MANA EUROCONTROL	Project Manager	11/11/2021
YOUSSOUF Abdel EUROCONTROL	Project contributor	10/11/2021
Kruger Oliver DFS	Project contributor	10/11/2021

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	14/07/2021	Draft	Alessandro Manzo YOUSSOUF Abdel Oliver Krueger	Table of content
0.2	21/10/2021	Final Draft	Patrick Mana Alessandro Manzo YOUSSOUF Abdel Oliver Krueger	Final Draft for internal review
0.3	10/11/2021	Final Draft	Patrick Mana Alessandro Manzo YOUSSOUF Abdel Oliver Krueger	Final Draft for internal review – editorial fixes
0.4	11/11/2021	Final Draft	Patrick MANA	Final Draft for internal review – editorial fixes
1.0	03/12/2021	Released Issue	Patrick MANA	Released issue after review by project members
1.1	07/12/2021	Released Issue	Patrick MANA	Released issue after review by project members
1.2	07/03/2022	Released Issue	Abdel Youssouf	Updated version taking into account comments raised

				during the 1st SDM consultation cycle.

Table of Contents

Contents

Table of Figures

Table of Tables

1. Introduction

This document is the guidance for SWIM Service Providers and Consumers to use the European Aviation Common PKI (EACP) solution developed by the project "SWIM Common PKI and policies & procedures for establishing a trust framework".

However, as the EACP can be used not only by SWIM service providers and consumers, this deliverable will provide guidance for the use of EACP within any aviation system.

The project plan identifies that Task 6 has to produce two deliverables:

- D6.1 – Guidance for SWIM service providers;
- D6.2 – Guidance for SWIM users.

However, Task6 came to the conclusion that it was useless to separate the guidance into two documents as a significant part applies to both SWIM service providers and users.

Consequently, this document is both D6.1 and D6.2.

1.1 Content

This guidance for SWIM Service Providers and Consumers and other users of the European Aviation Common PKI is composed of:

- An overview of the key activities to be conducted towards using EACP;
- Steps to be implemented to use EACP;
- A set of high-level use cases to illustrate the use of EACP;
- References to training material supporting the use of EACP.

1.2 Objective of this Deliverable

The objective of this Deliverable D6.1 and D6.2 is to provide initial guidance for SWIM Service Providers and Consumers in order to support the use and integration of the European Aviation Common PKI into their systems.

Therefore, project members as well as potential future users of the solution will be able to better understand what the changes are to be made both at system and organisational levels in order to use EACP services.

1.3 Project description

The project "SWIM Common PKI and policies & procedures for establishing a trust framework" aims to 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 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 CP1 family 5.1 (EC 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.

2. Key activities towards EACP use

This chapter introduces the main steps and activities in order to introduce the use of EACP within an organisation. Thus, it is worth to mention that a preliminary analysis of the services or systems involved in the adoption of a digital certificate is needed.

2.1 Definition of what services (or application or servers) use EACP

- Some SWIM related use cases have been used as illustrative examples and are further described in section 4. It is reminded that it will be required (as per EC 2021/116 – see mandatory scope of EACP) to use digital certificates for the SWIM Yellow Profile.
- Moreover, whenever communications can be secured (extended scope of EACP) with a security protocol compatible with X.509 digital certificates, EACP may help by providing such digital certificates.
- It shall be considered that the reference guidelines shall not be considered as an exhaustive source or reference but as a guidance material to support the final user.

2.2 Risk assessments

Before implementing a PKI solution to any application, a safety (support) assessment and security risk assessment need to be conducted in order to evaluate the vulnerabilities and to find out about the best implementation options.

Failures and vulnerabilities of systems should be evaluated by conducting a Safety (Support) Assessment and a Security Risk Assessment of the aviation service or system.

2.2.1 Security Risk Assessment

In order to keep the level of security commensurate to the degree of risk, and to minimize the impact of security incidents, it is recommended for an EACP PKI user to conduct a Security Risk Assessment for each system using EACP services and apply the appropriate controls to mitigate the risks. These controls can rely on EACP services.

Many standards already provide guidelines for conducting a security risk assessment (e.g. ISO/IEC 27001, NIST Risk Management Framework (RMF), CIS, EUROCAE ED-201A and ED-205 (A)) including Acceptable Means of Compliance and Guidance Material to the future Part-IS regulation.

2.2.2 Safety Assessment

As for the security risk management, it is needed that each organisation conducts a Safety (Support) Assessment in case relevant safety related systems are affected by the use of EACP certificates or services.

International and European regional regulations require to conduct a Safety (Support) Assessment in case of changes to the functional system is applied. That would be the case of e. g. a flight data management server or a surveillance system where a digital certificate provided by EACP will be implemented.

The main European applicable regulations are:

- EU Regulation N. 2017/373
- EASA - AMC3 ATS.OR.205(a)(2) Safety (support) assessment and assurance of changes to the functional system

3. EACP readiness at user level.

This section addresses how EACP users may integrate EACP certificates in their service or systems by a simple description of the main steps to follow.

3.1 Guidance to use EACP services

3.1.1 How to use an EACP certificate – EACP CERTSuite

EACP users must follow some steps to implement digital certificates in their system as well as update their system to ensure appropriate use and verifications.

EACP implements specific requirements related to revocation checking (take into account CRL generation and update, CRL size; maybe use delta CRL and OCSP). Information to access the certificate revocation checking is contained in the digital certificate attribute (namely the CDP (CRL Distribution Point) directing to the CRL URL location and the AIA (Authority Information Access) extension directing to the OCSP URL location).

EACP has proposed to match the Identity Assurance Level structure, as under development by the IATF (International Aviation Trust Framework) CP (Certificate Policy). Here 11 identity assurance levels are introduced. The nature of the IATF Assurance Levels recommends that the key pairs may be created and hosted either in software or in hardware environment.

In the case where key pair generation is based on software environment, users need to be aware of the application that will use the key pairs. In most cases, windows operating systems provide the native libraries based on the Microsoft Cryptographic API (CAPI) or Cryptographic Next Generation (CNG) to perform the key generation and other cryptographic operations. Other custom libraries such as OPENSSL or Java Cryptography Architecture can also perform the same cryptographic operations, in either Windows OS or Linux OS environment. Users should pay attention to use the latest up-to-date versions of cryptographic libraries.

In case where key pair generation is based on hardware environment, user must install the driver associated with the hardware that will be in use, and follow the instructions as per the vendor on how to initiate the hardware. Particular attention is given to the Identity Assurance Level 11, where the Hardware Security Module (HSM) is used for the key pair lifecycle management, inducing the need to precisely follow the EACP key management procedures.

EACP users must follow some steps to implement digital certificates in their system as well as update their system to ensure appropriate use and verifications. Specific steps for service providers and consumers are addressed in section 3.2.

Once the key stores are set up, users need to adapt their applications to be able to use digital certificates. The workflow for using digital certificate need to be identified, tested and implemented. A typical workflow would be as follows:

- Use cryptographic libraries and make the necessary changes to the user's application to conduct identification & authentication of the entities before granting them authorisation to access or use a service.

- Use cryptographic libraries and make the necessary changes to the user's application to be able to digitally sign objects, such as codes, documents, xml files, etc. Users need to be aware of the nature of the files to be signed and their associated protocols to be used in its application, for instance xml file signing requires xmldsig. Some applications may natively support digital signatures. Users need then to configure them to use their key pair and digital certificates. An example is Microsoft Outlook, Microsoft Word, Adobe, etc. For some specific application, where the use of digital signature has not been standardised, users need to make sure to use/integrate digital signature standard (e.g. for SWIM refer to SWIM signing message Cryptographic Message Syntax (CMS)).

- Use cryptographic libraries and make the necessary changes to the user's application to be able to encrypt objects, e-mails, etc. Users need to be aware of nature of the files to be encrypted and their associated protocols to be used in its application, for instance xml file signing requires xmldsig. Some applications may natively support encryption. Users need then to configure them to use their key pair and digital certificates. An example is Microsoft Outlook.

- Use cryptographic libraries and make the necessary changes to the user's application to be able to validate digital signatures before processing a transaction. Users need to use adequate libraries to be able to integrate digital signature checks in their workflow. Validating a digital signature guarantees integrity and proof of origin.

- Use cryptographic libraries and make the necessary changes to the user's application to be able to validate the digital certificate that has signed a transaction. The validation process can be based either on the basic validation process or on the advanced validation process:
    - The basic validation process is based on accessing the revocation checking service, and assert whether a digital certificate is still valid or has been revoked. The user' application must implement the changes to be able to parse a certificate and to access the Certificate Distribution Point (CDP) to download a Certificate Revocation List (CRL), or use the Authority Information Access (AIA) to access the OCSP responder. CRL or OCSP responses should give information about the certification status.
    - Advanced validation service based on Server Certificate Validation Protocol (SCVP). For this specific item, use EACP ValidSuite. Users can contact EACP to have a specific set of SCVP API, to be integrated with their application. ValidSuite allows users to delegate the validation process to a central server hosted by EACP. ValidSuite allows to validate among others:
        1. Certificate expiry check
        2. Certificate digital signature check
        3. Revocation check
        4. Key usage and Extended key usage check
        5. Certificate Policy OID check
        6. Name validation, policy mapping and other related checks

3.1.2 How to use Interoperability - EACP IOPSuite

EACP IOPSuite supports the following interoperability schemes:

- Interoperability by Cross-Certification
- Interoperability by Bridge Certification
- Interoperability by Certificate Trust List

The following sub-sections guide SWIM providers and consumers on how to use the interoperability scheme.

3.1.2.1 Cross-Certification and Bridge Certification

Once Cross-Certification or Bridge Certification process has been accomplished, EACP and its cross-certified partner will have to publish the cross certified certificates on their repositories respectively. Users and relying parties can rely on the newly created certificate to construct a path discovery up to a trusted anchor either by:

- using the Authority Information Access extension in their certificates where a pointer to the new certificate exists in their subordinate certificates;
- download the newly created certificates to their applications (i.e. Microsoft Local Trust List, Local Java key stores, etc.)

3.1.2.2 Certificate Trust List (CTL)

Users and relying parties access to EACP website and download the latest CTL. Before processing CTL, users and relying parties have to ensure the integrity and the authenticity of the CTL by validating its digital signature. Once this achieved, they can trust the different CAs contained in the CTL, by installing them in their applications, i.e. Microsoft Local Trust List, Local Java key stores, etc.

3.1.3 How to use Signing as a Service – EACP SignSuite

EACP Signing as a Service (Sa^2) – so-called EACP SignSuite - is one of the EACP Suite that provides EACP users with the capability of signing their objects by connecting to a central server host by EACP and dedicated for this signing process only. EACP Sa^2 alleviates EACP users from the effort of extra development and customisation of the signing process, and provides a direct interface to interact with the EACP solution or a set of API to integrate with the application workflow.

Typically to be able to use EACP Signing as a Service, users need to follow these generic steps:

1) Users get access to the EACP Signing as a Service documentation, which gives ample information on the different signing profiles, the URL address of the EACP Signing server, etc.

2) Users request the Signing API, such that they can integrate it in their workflow. To that end, users can contact EACP Policy Management Authority (PMA) for that purpose. On the other hand, EACP will offer in its training portfolio a module, named "Elective training", allowing users to be trained on how to develop "Signing API" and get help and support if needed.

3) Users select a specific profile that matches their needs and query the Signing server to sign their objects.

3.1.4 How to use Validation as a Service – EACP ValidSuite

EACP Validation as a Service (Va^2) – so-called EACP ValidSuite - is based on the SCVP protocol. It allows users and relying parties to validate digital certificates by either discovering the path of a digital certificate up to a trusted root, or discovering the path and validating every certificate by lookingat its validity period, its validity status and some specific components that characterises that certificate.

EACP Validation as a Service will implement multiple validation profiles. Every validation profile is identified by a validation policy. Users and relying parties can request the list of validation policies from the EACP Validation server.

Typically to be able to use EACP Validation as a Service, users and relying parties need to follow these generic steps:

1) Users and relying parties get access to the EACP Validation as a Service documentation, which gives ample information on the different validation profiles, the URL address of the EACP Validation server, etc.

2) Users and relying parties request the Validation API, such that they can integrate it in their workflow. To that end, Users and relying parties can contact EACP Policy Management Authority (PMA) for that purpose. On the other hand, EACP will offer in its training portfolio a module, named "Elective training", allowing users and relying parties to be trained on how to develop "Validation API" and get help and support if needed.

3) Once the validation client application is ready to send validation requests and to receive and process validation answers, users and relying parties can query the validation server about the different validation policies that are configured by the validation server.

4) Users and relying parties select a specific profile that matches their needs and query the server about the certificate validation status.

3.1.5 How to fulfil the Local Registration Authority (LRA) role

An LRA is an entity that is designated by his organisation to fulfil registration functions for a specific region/stakeholder to cover a subset of EACP certificates. The organisation must be part of the "Governing member" who has signed the "Memorandum of Cooperation" (MoC).

The LRA will have to agree and sign the LRA Agreement, and then follow the Registration Authority (RA) training which is part of the EACP Core training. The LRA training will detail amongst others the process and procedures for identifying and registering end entities. Next, the LRA will receive the LRA credentials allowing him to access the LRA interface.

Once connected to the interface, an LRA will process the different requests related to certificate management, by either accepting, deferring, or denying certificate requests or revocation requests.

3.2 User level

3.2.1 SWIM Services

The classical approach of exchanging SWIM messages is achieved over TLS connection between SWIM Providers and SWIM Consumers. SWIM Providers and SWIM consumers purchase TLS server and TLS client certificates and perform mutual authentication before establishing the TLS channel.

With TLS, the exchanged SWIM messages themselves are not signed (not required) and therefore their integrity cannot be guaranteed. An advanced approach consists in enhancing the SWIM security exchange by adding another security layer over the TLS connection, i.e. signing SWIM messages using dedicated SWIM signing certificates. Moreover, an advanced validation process is introduced at the producer side, to validate the consumer client certificate, and at the consumer side by validating the SWIM signing certificate. Figure 1 gives an example of an enhanced SWIM security exchange process (with message broker).

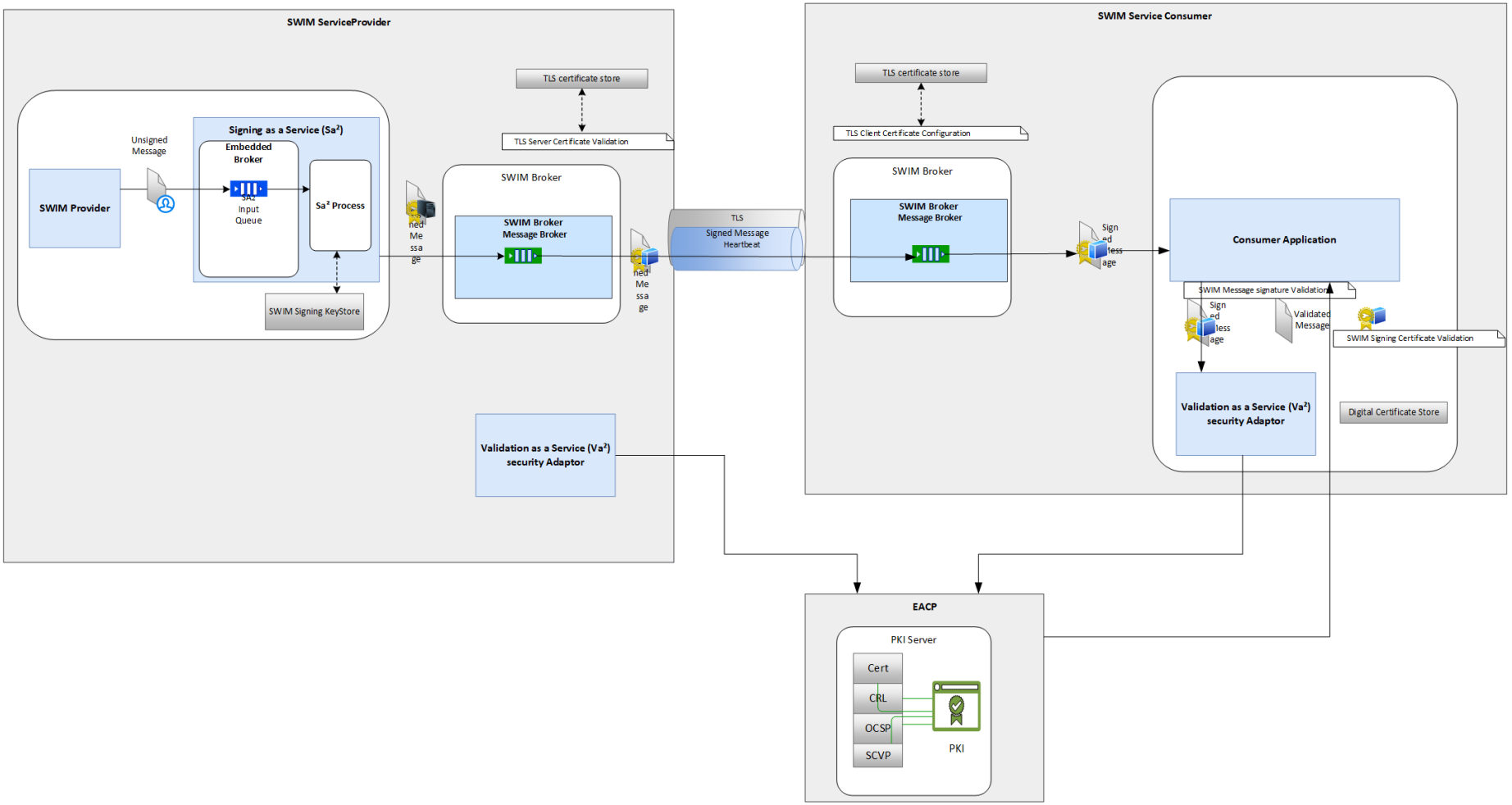

Figure 1: Example of enhanced SWIM Security exchange process

The main steps for achieving this process are presented in the two subsections below:

3.2.2 SWIM Service Providers

In order to enhance the SWIM exchange workflow, SWIM Providers need to use the following specifications:

A. PKI and Digital certificates

At the SWIM Provider side, the following digital certificates are needed:

- TLS Server certificate
- SWIM Signing certificate

The SWIM Provider purchases the two certificates from EACP (or certificate service provider) by registering and following the required registration steps, including providing the necessary credentials to obtain the required certificates. If the two certificates are not linked to a well-known CA in the certificate store used by the SWIM application, then their issuers' certificates need to be imported to that store...

The TLS Server certificate is a classical X.509 digital certificate having as an "Extended Key usage" the flag "server Certificate" asserted.

The SWIM signing certificate is a classical X.509 digital certificate that signs messages. For this certificate class, it is recommended to have a specific flag in its "Extended Key Usage", dedicated to the SWIM signing operations, though the protocol works without this flag. In a test campaign, the Enhanced Security Harmonisation Proof Of Concept (ESHPOC), conducted between EUROCONTROL and FAA, an "Extended Key Usage" flag identified by an Object Identifier has been introduced, tested successfully and proposed for its adoption at ICAO level.

B. SWIM digital signature (Signing as a Service concept)

SWIM Provider may need to implement the digital signature capability, commonly known as "Signing as a Service (Sa^2)", within its SWIM infrastructure. This feature can be implemented either locally or outsourced to external platforms. Provisions for handling the signing keys need to be taken into account when outsourcing the Sa^2.

In addition, the SWIM Provider needs to take into account the following SWIM message specifications:

1. The syntax of the SWIM message is made of the signature part and the payload, in such way to allow an application that cannot handle a digital signature to consume the payload;
2. Use a standardised message syntax such as Cryptographic Message Syntax (CMS) (RFC 5652) and by extension on Secure/Multipurpose Internet Mail Extensions (S/MIME) 4.0 (RFC 8551) or higher, to host the signature as well as associated data in a context where interoperable security frameworks are based on X.509v3 certificates technology.

C. Digital Certificate Validation (Validation as a Service)

SWIM Provider may need to make provisions for validating client certificates of the SWIM consumers. To that end, SWIM Provider need to integrate the validation process into their application workflow, and make sure to have access to the PKI repositories.

Validation can be scaled from a basic validation process up to an advanced validation process. The basic validation process is based on revocation checking services by either using the CRL file, or the OCSP service.

The advanced validation process is based on SCVP protocol (RFC 5055), where different validation profiles can be implemented at the server side. Both OCSP service and SCVP service require a client to be developed and integrated to the SWIM Provider application workflow.

3.2.3 SWIM Service Consumers

In order to enhance the SWIM exchange workflow, SWIM consumers need to use the following specifications:

A. PKI and Digital certificates

SWIM consumers purchase client certificates from EACP (or another certificate service provider) by registering and following the required registration steps, including providing the necessary credentials to obtain the required certificate. If the certificate is not linked to a Well-known CA in the certificate store, then its issuers need to be imported to that store.

The TLS Client certificate is a classical X.509 digital certificate having as an "Extended Key usage" the flag "Client Certificate" asserted.

B. Client tools to validate SWIM message and signing certificate

A SWIM consumer may, at his convenience, proceed to the validation of the digital signature and to the validation of the SWIM signing Certificate. To that end, SWIM consumers need to integrate these features in his application workflow before processing SWIM messages.

Specific attention goes to the digital certificate validation tool, where the SWIM consumer can either develop his own validation tool, or delegate the validation process to EACP.For the latter, the SWIM consumer needs to contact EACP to query the client validation API, to complete the integration with his application.

In addition, the SWIM consumer needs to be aware of the different validation profiles implemented by the EACP, such that he can select a suitable profile forthe validation. The different validation profiles are described in the EACP documentation and can be obtained upon request made to the EACP PMA, or can be queried from the EACP Validation (SCVP) server.

3.2.4 Other users

Other users need to follow the same process, i.e. purchasing the EACP digital certificates following the registration procedures, and using other EACP features as the need evolve.

4. High level use cases and examples

4.1 Class 1: connection always available

This section describes use cases and examples where a 24/7 connection to EACP PKI services is needed.

4.1.1 Example Use Case 1.1: "Authenticate Network Manager/Users"

This section describes the use case of the Network Manager SWIM services provided over B2B. Communication between the Network Manager and its users is achieved over mutual authentication provided by the TLS protocol as explained below.

Usage and management of TLS Certificates:

- The implementation and operation of certificate management should be simple, preferably with tools already available at OS level.
- A TLS certificate integrated into the pan-European trust framework can be validated by checking its signature against a locally stored public key, i.e. without having access to a centrally managed certificate hierarchy at time of validation.
- Any standard TLS certificate must be usable for securing mandated SWIM once signed with a key identifying the issuing organization as a regulated/certified ATM stakeholder.
- Management and access to a pan-European certificate revocation list and /or certificate trust list must be granted.

4.1.2 Example Use Case 1.2: G/G SWIM Service

As per the CP 1 Regulation (Reg. EU 2021/116) and the EUROCONTROL Yellow Profile the operational stakeholders have to implement common EACP services by the end of 2024 and the corresponding local PKI solutions to exchange information via SWIM in a secured way by end of 2025.

Thus, the following relevant use cases have been identfied (the statements made in the previous chapter apply):

- TLS-Communication (https, AMQP)
    - o TLS Certificate for Servers
    - o TLS Certificate for Clients

Potentially (not required) the following use cases may apply:

- o Payload encryption
- o Payload signature

To implement the cyber-security requirements mandated by the CP1 the following EUROCONTROL Yellow Profile security requirements need to be complied with:

Identifier	Title	Statement
SWIM-TIYP-0008	TLS	The Service Interface Binding **shall** support the following versions of the Transport Layer Security Protocol (TLS): + IETF RFC 5246 (TLS v1.2)
SWIM-TIYP-0010	HTTP over TLS	The Service Interface Binding **shall** comply with IETF RFC 2818 (HTTP over TLS).
SWIM-TIYP-0037	AMQP Transport Security Authentication	The Service Interface Binding **shall** support at least one of the following authentication methods: + TLS server authentication and SASL PLAIN + TLS mutual authentication and SASL ANONYMOUS + TLS mutual authentication and SASL PLAIN.
SWIM-TIYP-0042	TLS Authentication	The Service Interface Binding **shall** support one of the following authentication mechanisms for TLS: + Mutual authentication with X.509 certificates + Server authentication with X.509 and Client authentication with HTTP Basic or HTTP Digest.
SWIM-TIYP-0052	AMQP over TLS	The Service Interface Binding **shall** use the AMQP over TLS (amqps) for transport security.
SWIM-TIYP-0064	Validation of X.509 Certificates	The SWIM-TI **shall** validate X.509 certificates using a trusted Certificate Authority.
SWIM-TIYP-0065	Cryptographic Algorithms	The SWIM-TI **shall** select cryptographic algorithms and key sizes in accordance with: + Applicable national or international regulations on cryptographic algorithms and key sizes or; + NIST SP 800-57 Part 1.
SWIM-TIYP-0071	Cryptographic Key Life-cycle Management	The SWIM-TI **should** manage the life-cycle of its cryptographic keys in accordance to NIST SP 800-57.

Table 1 - SWIM Yellow Profile cryptographic requirements

4.2 Class 2: limited bandwidth

When the operational situation prevents that a connection to the EACP PKI Services is accessible at all times, specific techniques need to be implemented to ensure an uninterrupted and reliable supply of data.

4.2.1 Example Use Case 2.1: Check certificate with limited bandwidth or risk of losing connections

- CRL Caching

  To check whether a certificate is still valid, the PKI clients need to have access to a CRL, which normally is provided as a central service. During the flight period, the access point for a centrally provided CRL might not always be available.

  To have a faster access to the CRL when checking a certificate, systems usually cache the CRL for a time that is determined by the date and time of the next foreseen update of the CRL.

  For the operational case of an aircraft in flight, it needs to be ensured that the CRL is valid on the airborne system site during the complete flight period, even if the “natural” lifetime of the CRL has been exceeded. Therefore, it shall be ensured, that the CRL for all involved CA domains is cached upfront the beginning of the flight phase and valid during the whole flight phase.

- OCSP Stapling

  For the checking of certificate validity via OCSP during the flight period, with a potential loss of connection to the OCSP Server, the OCSP-Stapling function can be used. The certificate owner receives an OCSP answer from the OCSP Server with a time stamp and can attach this to the TLS handshake. This OCSP stapling process needs to be executed on both sides between all potential communication partners. It needs to be ensured, that the times stamp exceeds the foreseen duration of the flight.

- Certificate Caching

  During the execution phase of a flight, all certificates which are planned to be used may be cached at least for the duration of the flight.

5. EACP Training material and Guidance to support users

5.1 EACP Services

The EACP services are described in the EACP Product Portfolio document (see D1.2 – Final Trust Framework Annex A2 European Aviation Common PKI (EACP) Product Portfolio)

5.2 Training materials

The training package is an important EACP deliverable. It aims at guiding EACP users on how to access and use EACP services effectively. The courses and learning transcript allow trainers to interact seamlessly with EACP interfaces and support them to develop or enhance competencies required to be effective in their job role.

The training materials contain information for subscribers to access EACP interfaces, instruction for LRA to access RA interfaces, procedures to collect and archive registration data, guidelines for PKI operators to enrol local subscribers, hints to relying parties to access validation and revocation checking services. etc.

Training can be offered either in live session, or available as a modularised or self-paced replay. In all cases, where applicable, documentation will be supplied to the trainers during training, retraining, or otherwise. The self-paced replay will be available all time.

All trainings require an enrolment in advance and may be arranged for a group. Information on training enrolment can be obtained from EACP website, or from EACP CPS.

EACP training and guidance courses can been placed into four categories: Core, Basic, Elective and Help Desk and support.

- Core: A training that is fundamental to the job function and covers a required knowledge or skill. This training covers both the PKI Operator Job and LRA job.
- Basic: A training and guidance to expand users' knowledge about EACP interfaces. This training guides users on how to access EACP interfaces to request issuance or revocation of an EACP digital certificate or on how to request interoperability with EACP.
- Elective: Atraining and guidance on how to access EACP advanced services such as ValidSuite and SignSuite.
- Help Desk and support: An interface allowing users and relying parties to post their support cases and look in the knowledge base database to query responses for the most known support cases.

Retraining sessions may be organised as the need evolve, or whenever there is a new release with new feature in the product or services.

5.2.1 Core Training

The Core training is organised as "hands on training", and require face to face meetings, because it involves the creation and grant (handling) of the (LRA or PKI Operator) credentials, required for operators to perform their jobs accordingly.

The relationship between EACP and the LRA or the PKI Operator is regulated by associated agreements that address the obligations, the procedures, the requirements of EACP and an LRA or the PKI Operator. In these agreements, the LRA or the PKI Operator guarantees to follow the procedures of verification of subscribers.

An organisation designates the members of its staff that fulfils the LRA or the PKI Operator function. It is recommended (business continuity) to have two persons per LRA or PKI Operator function that are accredited and have accomplished the core training so that the LRA or the PKI Operator role is operational.

These designated persons must be physically present to follow a hands on training on how to access or use the LRA/PKI Operator interfaces. During the training session, LRA/PKI Operator receive a special credential (usually in term of key pair and associated certificate stored on a physical token). This credential is strictly personal and will be immediately revoked if the person leaves or is no longer accredited.

In addition, during the training period, LRA/PKI Operators will learn about the processes of vetting (authenticating and validating) subscribers as well as on the procedures associated with the issuing of EACP certificates or revoking them.

How to access the (L)RA interface

- how to login and authenticate himself to the (L)RA interface
- how to collect vetting information on subscribers and user and map them to the assurance levels
- how to generate key pairs and associated certificate on behalf of users (centralised certificate provisioning)
- how to approve/deny/defer certificate issuance request
- how to revoke a digital certificate
- how get audit information and statistics

How to access the PKI operator interface

- how to login and authenticate himself to the PKI operator interface
- how to submit certificate request on behalf of user
- how to request certificate revocation
- how to get audit information and statistics

5.2.2 Basic Training

Basic training is offered to subscribers and aims at guiding them on how to access and use EACP interfaces to request issuance or revocation of an EACP digital certificate.

The basic training describes among others processes on how to:

- request EACP digital certificate
    - distributed certificate provisioning
        - direct interface
        - PKI Operator interface
    - centralised certificate provisioning
- how to request certificate revocation
- how to access revocation checking services

In addition to EACP subscribers, basic training also gives guidelines to local PKI users on how to interoperate with EACP and explains the criteria and methodology for interoperability.

This training can be provided in a manual, in a downloaded format, or presented in EACP website, or to be organised as self-paced replay.

5.2.3 Elective training

This training is dedicated to selective EACP users who have decided to use the enhanced EACP services, i.e. ValidSuite and SignSuite.

The training aims at guiding users on how to get the required client tools, and gives hints on how to integrate them to their local applications and workflow, and how to access the services and use them effectively.

The training materials contain also some specific documents related to ValidSuite and SignSuite that help explaining the different validation policies and signing protocols used by EACP solution. These documents can be obtained by addressing specific request to the EACP PMA.

External courses that are vendor specific are not treated in the EACP training material.

1. How to access EACP Services:
    - how to access EACP ValidSuite
    - how to use EACP SignSuite
2. Guidance: Provide PKI related documents to specific subject matter (Validation as a Service, timestamping, Signing as a Service, etc).

5.2.4 EACP Help Desk and support

The EACP provides support to all stakeholders dealing with its solution. EACP support answers questions from, provides information to and resolves problems raised by the stakeholders as they relate to the subscribed EACP services .

The EACP provides first line support to its stakeholders. EACP applies an e-ticketing system and allows the stakeholders to forward their questions via e-mail, but EACP makes also available a hotline to solve urgent issues.

The EACP provides support only for duly reported incidents or problems to the authorized stakeholders registered with EACP.

TheEACP provides information on the status of the problem resolution process via Status Reports. EACP acknowledges the start of the problem resolution process by sending an Initial Status Report to the stakeholders designated support contact specified in the Service Context.

When it has been confirmed that EACP provided all the necessary information to resolve the problem, EACP closes the Call ID.

The EACP uses its website to announce events related to the service delivery, such as suspension and upgrade or a maintenance window. With respect to problems related to any suspected service disruption, stakeholders should first verify whether it concerns an announced maintenance window.

The EACP provides also in its website, via its support tab, a knowledge base giving hints, allowing stakeholders to solve quickly the most known issues, without the need to create support cases.

Appendix A References

[1] D1.2 – Final Trust Framework Annex A2 - European Aviation Common PKI (EACP) Product Portfolio