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

D1.2 Final Trust Framework - Annex A3.d - EACP Criteria and Methodology for Interoperability

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	Final Trust Framework – Annex A3.d -EACP Criteria and Methodology for Interoperability
Deliverable ID	D1.2
Edition	1.1
Template Version	01
Task contributors	

Please complete the advanced properties of the document

Abstract

This document is part of the Trust Framework for the European Aviation Common PKI (Public Key Infrastructure).

This document defines the interoperability criteria between PKI domains of the future European Aviation Common PKI (EACP).

This document is the Annex A3.d of D1.2 Final Trust Framework

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
Patrick MANA EUROCONTROL	Project Manager	11/06/2021

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	30/06/2021	Draft	P.MANA	Final
0.2	30/06/2021	Draft	P.MANA	Review of DFS comments
0.3	08/10/2021	Draft	A.YOUSSOUF	Review of comment during Thread B meeting and Add annex for Local PKI Assessment
0.6	09/11/2021	Draft	A. YOUSSOUF, P. MANA	Draft version submitted to Project Members for final review.
0.7	11/11/2021	Draft	P.MANA	Transform it into D1.2 Annex A3.d
1.0	06/12/2021	Released Issue	P.MANA	Released Issue taking into account project members comments
1.1	07/03/2022	Released Issue	P.MANA	Released Issue taking into account comments raised during the 1st SDM consultation cycle.

Table of Contents

Table of Figures

1. Introduction

This document is the interoperability criteria for the future European Aviation Common PKI (Public Key Infrastructure), deliverable D1.2 Annex A3.d of the future EACP Trust Framework.

1.1 Objective of this Deliverable

The objective of this Deliverable is to define a methodology and a set of criteria to ensure the interoperability between PKI domains for the future European Aviation Common PKI (EACP).

2. Interoperability criteria

2.1 General Principles

Achieving interoperability and trust with public key cryptography can be completed for multi PKI domains that meet a common set of minimum requirements through the widespread Cross-Certification, Bridge Certification Authority (BCA) or CTL.

Each technology can meet different objectives and alleviate constraints such as risk, policy consideration, cost and integration with other technologies. It is unlikely that different objectives can meet by a single scheme without compromising security and increasing risk at one end, or cost at other.

The classical way to handle the problem of interoperability is CA-CA cross certification. This solution can be appropriate mean to establish a trust relationship between a small numbers of PKI domains, where their policies are aligned. However, this solution becomes inappropriate when the number of CA increases. Cross certifying n PKI Domains requires n(n-1)/2 mutual cross certification and n(n-1) certificates to install in local stores and browsers. Establishing this relationship requires a time consuming review of policies and practices, besides other problems related to relying party application may show up such as: limitation to construct certificate paths and to access certificate information maintained by the concerned CAs. This architecture rapidly becomes a complex problem.

An alternative solution to cross certification could be Bridge Certification Authority (BCA). This solution overcomes most of the problems encountered with cross-certification case, and alleviates the validation mechanisms and the complexities added to relying party applications. However, this technology requires that the BCA signs all participating CAs, which may not be aligned with most of the PKI domain local policies.

An alternative solution, which surmounts all these constraints, can be CTL. A CTL consists in using multiple CAs as trust anchors. The certification path build uses the same approach as the one used in the hierarchical model. The difference is that a certificate path will be constructed and be verified back to any of the trust anchors contained in the list. This method is used by the most popular browsers, who are shipped with a list containing many CAs considered as trusted by the browser manufacturers. While this approach simplifies the certification path build, it induces some vulnerabilities. In fact, some client applications allow relying parties to import other root certificates as required, this can be exploited by malicious code that could add rogue CA certificates. Some proprietary applications have addressed this problem by designing an entity who digitally signs the CTL. CTLs will be centrally managed by trusted signing entity, according to predefined security policies, criteria and methodology.

Unlike Cross CA certificate and Bridge CA certificate, Certificate Trust List (CTL) does not give granularity and control over exactly what types of end entity certificates and for what purposes they can be trusted. In Cross CA certificate and Bridge CA certificate, this information is expressed in term of policy validation setting. But there are ways on how to add these validation policy setting to the CTL such that relying parties are aware on which policies to map between PKI domains during their validation processes.

This document describes the steps and decision criteria the EACP uses to complete CA-CA interoperability activities in a rigorous and cost-effective manner. The criteria and methodology described in this document apply for the cross certification, the Bridge CA or the CTL interoperability schemes. EACP will be able to accommodate these three schemes in principle. However, some of them will be actually deployed based on users' needs.

Interoperability with the EACP is not a right and the discussions and activities leading to CA-CA interoperability should not be seen as a commitment to issue an interoperability certificate or a CTL. The EACP may revoke an issued interoperability certificate at its sole discretion if the Member is not in good standing following the EACP Audit and assessment procedures.

2.2 Time to implementation

Interoperability activities is an interactive process between the two parties. A full process may complete anywhere from 1 month to six (6) months in calendar time depending on the readiness, resource availability, and complexity of the cross-certifying party and its environment.

Any review by the EACP of any information from an Applicant is for the use of the EACP in determining whether or not interoperability is possible and beneficial to the trust framework and will be treated as proprietary in accordance with applicable Agreements.

In most cases, the goal of interoperability is to integrate the candidate in the EACP network of Trust. As such, EACP will determine whether the Applicants meets the policy and legal requirements required for interoperating with EACP at one or more of its assurance levels.

2.3 Methodology for Interoperability

The steps and methodology for the Interoperability is depicted in Figure 1.

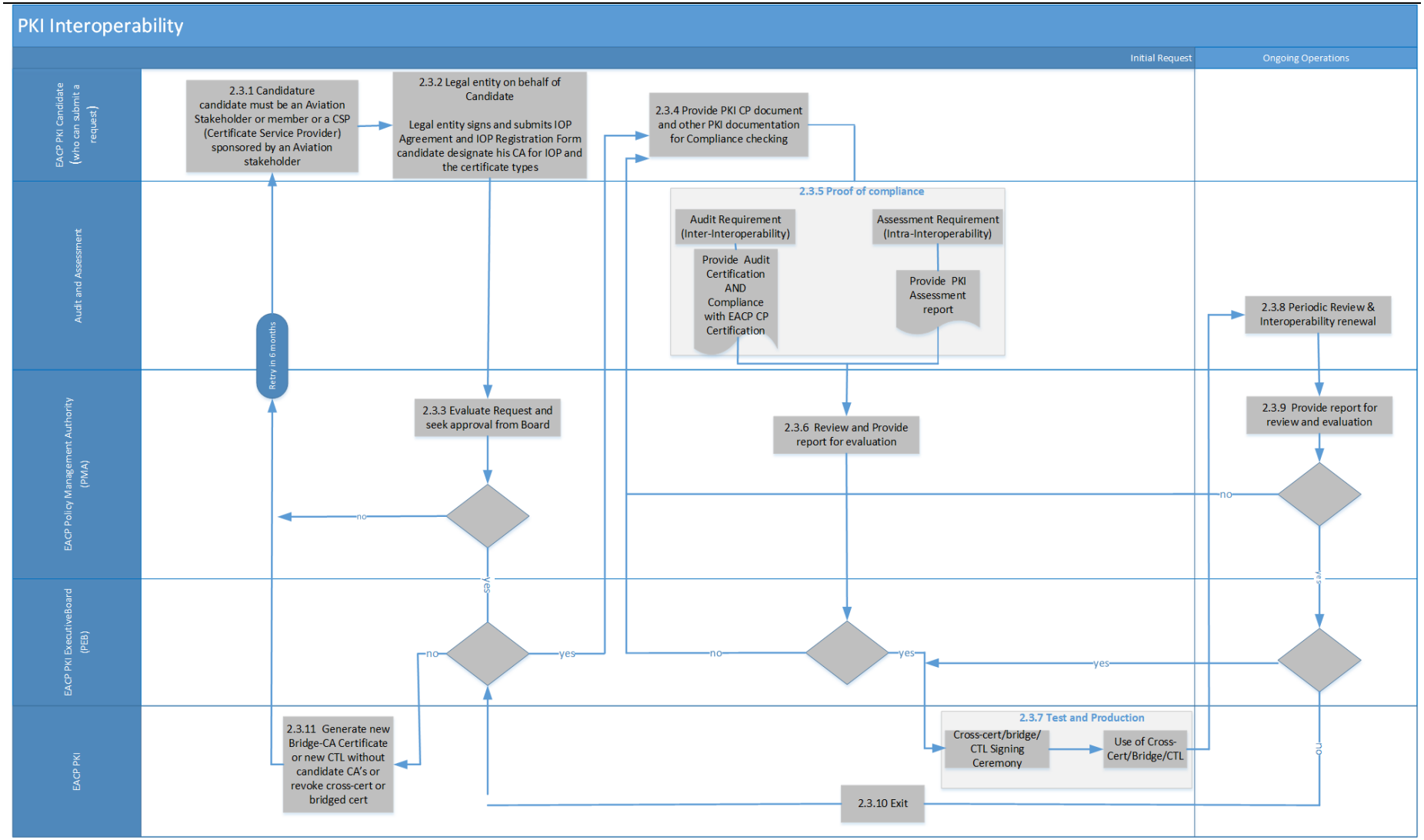

Figure 1: EACP Interoperability methodology

2.3.1 Candidature

Only eligible Aviation stakeholders (called hereafter candidate) can apply for the Interoperability Services offered by EACP (named IOPSuite in the EACP portfolio).

- Intra-interoperability membership: Membership is open to all EACP Members
- Inter-interoperability membership: Membership is also opened to extra-to-Europe Aviation Stakeholders whose main business is aviation or who are providing services to aviation.

Intra-Interoperability and Inter-Interoperability candidates will have to sign the "Master Participation Agreement" and acknowledged the "Interoperability Agreement". In the Interoperability Agreement, there is an "Interoperability Registration Form" where the applicant will indicate to which certificate type he wishes to interoperate.

All Applicants for Interoperability with EACP will have a Local PKI, installed and configured following the best security practices and PKI standards, completed by an EACP Assessment certification (as described in 2.3.4 and 2.3.5). In addition, this PKI will have to obtain a unique certificate Object Identifiers (OIDs) identifying their PKI domain and/or their assurance levels. Theses OIDs need to be 9logically held in their digital certificates, and also will be mapped with the EACP one(s). This mapping exercise will be logically incorporated in the interoperated certificate, more precisely in its "Policy Mapping" certificate extension.

The OIDS will be registered in the standard International Organization of Standardization (ISO) object identifier registry from the appropriate commercial or national registration authority.

Submission of a Cross Certification request, Bridge Certification request or CTL request will be fulfilled by a legal entity which has a final liability and responsibility on the candidate CA.

2.3.2 Candidate - Who can submit IOP Request

This step allows a candidate to submit its Interoperability request dully signed by an appropriate senior official (an officer or executive) of the stakeholder who is authorized to commit the organization to completing the interoperability process. Such a commitment would include bearing any expenses incurred by the organization during the interoperability process, and the authorization of any submission of information or statement required from the candidate.

The candidate will acknowledge and sign the "Interoperability Agreement" and will have to fill in and dully sign the "Interoperability Registration Form" (See Annex A1 “Interoperability Agreement”).

The "Interoperability Registration From" contains the following information:

- Name and contact information (email address, phone number and address) for a primary and alternate point of contact (POC).
- Information on the candidate’s CA to interoperate with.
- The proposed EACP certificate assurance levels at which interoperability is sought.

2.3.3 Interoperability Evaluation

The candidate submits a completed and signed Application for Interoperability to the PMA using the PMA address provided in the CP.

The PMA will review the Interoperability request, vote on a recommendation to accept or reject the application:

- If the recommendation is to not accept the application, then the PMA will send a notification to the candidate, explaining the detail of the rejection. Candidate may update and resubmit another submission after six (6) months based on the PMA comments
- If the recommendation is to accept the application, then the Interoperability request is forwarded to the PEB to further investigate and take the final decision.
    - If the final decision is to not accept the application, the PEB will justify the rejection and the candidate can only submit a new request after 6 months and provide the mitigation that he has applied to its PKI solution.
    - If the final decision is to accept the application, the candidate will provide EACP with its PKI documentation (CP, CPS, Processes and Procedures, etc.) and any other document required by EACP.

2.3.4 Candidate - Submit PKI CP document and other PKI documentation for compliance checking

The candidate submits its Certificate Policy (CP), Certificate Practice Statement (CPS), and its own PMA Charter or other supporting PKI documents to the EACP PMA for review. The candidate then demonstrates and defends that its CP and CPS are comparable to the requirements in the EACP CP and CPS at the levels of assurance for which the candidate requests interoperability and that the candidate PMA Charter is sufficient to ensure that its PKI Policy is adequately governed. The candidate and the EACP PMA mutually agree on the methodology to be followed. Specific document requirements are:

- **CP and CPS**. The candidate's CP will be stable, not be in draft version. If multiple candidate CPs apply then all such applicable candidate CPs will be submitted. If the CPS is not drafted or stable at this point, it can be submitted later. Both the CP and CPS will be finalized and signed in time to support the Assessment.
- **Candidate's PMA Charter.** The PMA Charter or other governance documents describing the process for managing and approving PKI policy and domain governance.
- **The candidate's PKI hierarchy specification including any Cross-Certifications**. The PKI Specification document details the candidate's PKI hierarchy and it documents any existing cross-certifications and domain CAs. In addition, it gives the OID arc and describes the different domain or assurance levels.

2.3.5 Proof of compliance

The candidate will provide evidence that its PKI has successfully passed the EACP Assessment.

2.3.5.1 Assessment requirement for Intra-Interoperability

The EACP Assessment for Intra-Interoperability is based on an Assessment instructed by the EACP PMA and conducted by the EACP PMU, in accordance with Annex A3.d.1.

2.3.5.2 Audit requirement for Inter-Interoperability

For external PKI domain, the EACP Assessment will consist in an Audit certificate delivered by an accredited and recognised Audit body, regardless of the desired level of identity assurance with which the candidate wishes to interoperate.

In all cases, the Audit will focus on the candidate's CA, its PKI documentation and PKI processes. At the end of the Audit process, the Auditor will supply the candidate with a Letter of Compliance and/or an Audit report declaring his conclusions, which may detail further actions to undertake in order to reach compliance.

At the end of the Audit, the candidate submits the Auditor's Letter of Compliance and any supplementary documents to the EACP PMA.

If no significant Audit action items are reported, the PMA notifies the candidate in writing of the results of the Auditor letter of compliance. If significant Audit action items are reported, the PMA requests that the candidate develop and implement a remediation plan with ninety (90) days.

Other assessments (technical, operational, etc.) may be conducted to assess if the candidate CA is compliant with the European Aviation PKI policies. The assessment can be conducted by the European Aviation Advisory Group. Of particular interest, the assurance levels, associated registration processes, and OID policy mappings build between the candidate CA and European Aviation PKI.

- The technical assessment will look, among others, to the CA and End Entity X.509 based certificates. The candidate will demonstrate the compliance to the different registration procedures of the different assurance levels.
  In addition. All end-entity certificates will contain a combination of KeyUsage and ExtendedKeyUsage extensions detailing the purpose of using the certificate. All end entity certificate will contain a certificate policy extension which indicate an assurance level that could be mapped to EACP one.

- The operational assessment will check, among others, if the candidate does support at least revocation checking services (OCSP or CRL), and will demonstrate a capability to revoke certificates upon any actual or suspected loss, disclosure or other compromise of the subscriber's private key. Candidate has to show ability to revoke its own CA certificate in case of compromise.

2.3.6 Compliance Review and report for evaluation

The EACP PMA will review the Audit/Assessment reports.

- If the PMA rejects the reports, it will inform the candidate accordingly and will indicate the reasons for such rejection and seek for a reassessment in accordance with criteria defined in 2.3.4 and 2.3.5 with a grace period of six months.
- If the PMA accept the reports, then it will forward it to the PEB, who up to its satisfaction, decide either to go/no go with the interoperability process:
    - In case of no go, notification will be submitted to the candidate indicating the reasons for such rejection and requesting fine tuning its PKI solution based on the Assessment findings;
    - In case of approval, the go decision will be forwarded to the EACP to perform the technical part of the interoperability solution, i.e. to cross-certify, to bridge or to sign a CTL with the candidate CA.

The candidate CA will continue to pass the EACP Assessment, at least once every two years. In addition to the Assessment, the candidate CA will continuously conform to the European Aviation Common Certificate Policy requirements.

2.3.7 Submittal and Preparation for Interoperability – Test and Production Environment

2.3.7.1 Test Environment

Once the candidate has successfully completed the EACP Assessment and any remediation to the satisfaction of the EACP PMA and PEB, the candidate submits a complete set of sample Test and Production certificates to include:

- List of all policy OID to map.
- PKCS#10 Certificate Signing Request of the CA that will interoperate with EACP (to be used either in cross certification or bridge interoperability schemes).
- The candidate CA Certificate (to be used in case of CTL interoperability scheme).

The EACP PKI performs interoperability testing using the candidate's certificate and/or its certificate request (PKCS#10). The interoperability is achieved by organising a Key Ceremony to generate a root- signed certificate, bridge certificate or to sign CTL.

The tests are done in a test environment, which simulates production one. Interoperability testing is performed to validate the trust path between the candidate CA and the EACP.

The reviews and test will demonstrate:

- In case of CTL, the candidate will validate the CTL digital signature before processing the CTL.
- In case of cross certification or bridge certification, the newly created certificate matches the Certificate Profile(s) in the EACP's CP(s). If the profile is not in the EACP's CP, then the EACP will provide the appropriate document for verification

- Access to the newly created certificate or CTL is accessible to Relying Parties over the Internet via HTTP and/or directory.
- The CRL are accessible to Relying Parties over the Internet via HTTP and/or a Directory Repository.
- Validate the path and certificate chaining up to EACP Root CA.
- Validate end candidate certificates (if applicable) to validate policy mapping.

A test report containing the test result is submitted to the PMA (PMU).

- If the test results shows failure, EACP PMA instructs to conduct further tests by exploring different configurations and fine tune the certificate content until reaching an acceptable solution.
- If the test result shows satisfaction, EACP PMA (PMU) instruct organising a formal Key Ceremony in presence of the candidate to achieve one of the interoperability scheme.

2.3.7.2 Production Environment

Upon successful test, PMA instruct proceeding with Key Ceremony to officially root-sign, bridge or sign CTL accordingly. PMA requests the EACP-PKI to initiate officially interoperability scheme with the candidate CA.

1) EACP and the candidate provide their respective PKCS#10 CSR (Certificate Signing Request) files and Cross Certificate Naming Forms to each other to provide the necessary technical information needed to create cross certificates or bridge certificates.
2) EACP organises a formal and witnessed key ceremony to achieve the production interoperability scheme and, then verify the generated certificates are in compliance with the applicable CP and are concordant with the test certificates tested successfully early.
3) EACP publishes the newly created certificate(s) or CTL to its PKI Repository.
4) Notify all EACP Members that a new EACP candidate has joined the EACP network of Trust.

2.3.8 Periodic Review and Interoperability Renewal

This is the maintenance phase. It includes, every two years, the renewal process and other maintenance tasks that sustain the interoperability relationship over time. EACP PMA will send multiple reminders to the participant, at least one hundred twenty (120) days and thirty (30) days prior to the date of expiration of the certificate or the CTL.

The member will perform, at least once every two years, an Assessment of its operations covering all the items listed in section 2.3.4 above. This Assessment will cover two years of operations from the end date of coverage from the last Assessment.

The member sends the following items to the EACP PMA:

- Latest CP signed (and a track changes version of the CP from the last CP reviewed by the PMA, if applicable)
- Auditor Letter of Compliance in case of inter-interoperability, and any Remediation Plan and Evidence of Remediation if applicable
- Candidate CA Certificate and CRL.

The member also sends the following items to the PMA when requested:

- "Interoperability Registration Form"
- PKCS#10 the candidate CA Certificate Signing Request

2.3.9 Report Review and Evaluation

Candidate provides PMA with an Assessment report. When the PMA is satisfied that the renewal package is complete, it informs EACP PEB accordingly, and request EACP PKI to proceed with the renewal process, leading to step 2.3.7.

2.3.10 Exit procedure

If the PMA is not satisfied with the Assessment report and think that there has been significant discrepancies noted in the Assessment that have not been remediated, PMA will grant the member a grace period of one hundred twenty (120) days, during which the member need to remediate or come up with remediation plan.

2.3.11 Revoking a candidate CA

Passed this time (one hundred twenty (120) days), then PMA will inform PEB accordingly and proceed with revoking the member by either generating new CTL without the member's certificate or by revoking the member's signed certificate.

EACP does not support suspension of the candidate CA in either cross certification, Bridge CA or CTL.

3. Interoperability Termination process

EACP has prepared/foreseen a termination process should an existing member wishes to terminate the interoperability agreement.

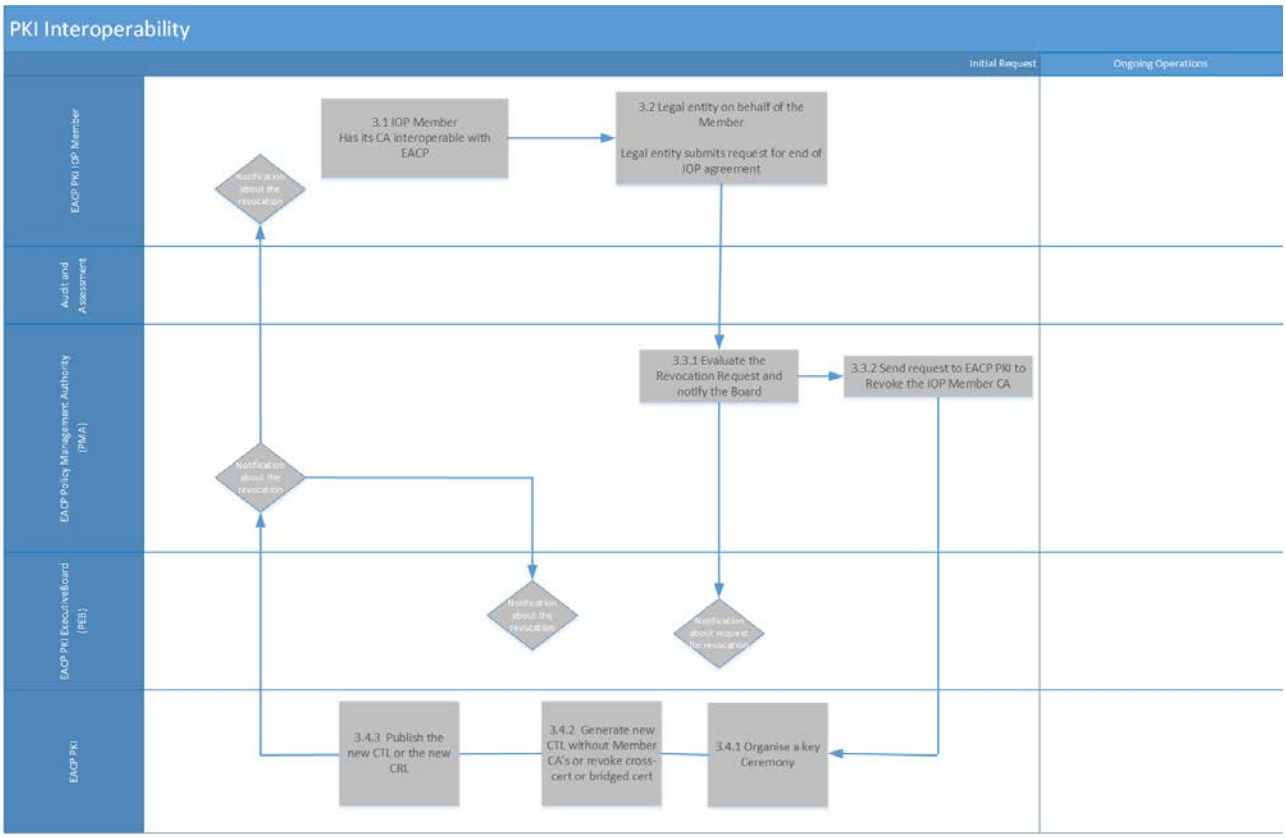

Figure 2: IOP Termination process

3.1 Who can request the Termination of an IOP agreement

Only EACP Interoperability members who have joined the EACP network of trust by one of the interoperability schemes that are explained in section 2.1 can request termination of the IOP agreement with EACP. The termination of the IOP agreement implies either revoking the member CA in case of bridge or cross-certification or withdraw the CA from the CTL that was signed by the EACP IOP CA. In either both cases, a new CRL file or new CTL will be generated and published to the EACP repositories accordingly.

3.2 How to submit Termination request

Submission for a termination to an interoperability agreement will be fulfilled by a legal entity which has a final liability and responsibility on the member CA. The legal entity will submit the request to EACP PMA. The request can be formulated by a registered letter or signed e-mail.

3.3 Processing request for termination

EACP PMA will analyse the request for termination, and notify the PEB accordingly. In addition, PMA will instruct EACP PKI to start the organisation of termination process.

3.4 Revoking a member

EACP PKI will organise a key ceremony to revoke the CA member or to withdraw the CA member from a CTL according to the EACP Key Management Procedures. EACP key ceremony is a witnessed operation and requires the presence of the CA member representative. In case the CA member representative can't witness the key ceremony, then it will send a delegation letter to EACP so that to proceed without its presence.

During the key ceremony, EACP will proceed to either generate a new CRL containing the CA member serial number, or to produce a new signed CTL without the candidate CA.

The newly created files will be published to the EACP repositories. A notification will be sent to the PMA on the completion of the task.

PMA will inform the EACP PEB and the IOP member accordingly.

4. Annex A3.d.1

The assessment report will address different aspects surrounding Local PKI environment. The main aspects is depicted in Figure 3 and presented below:

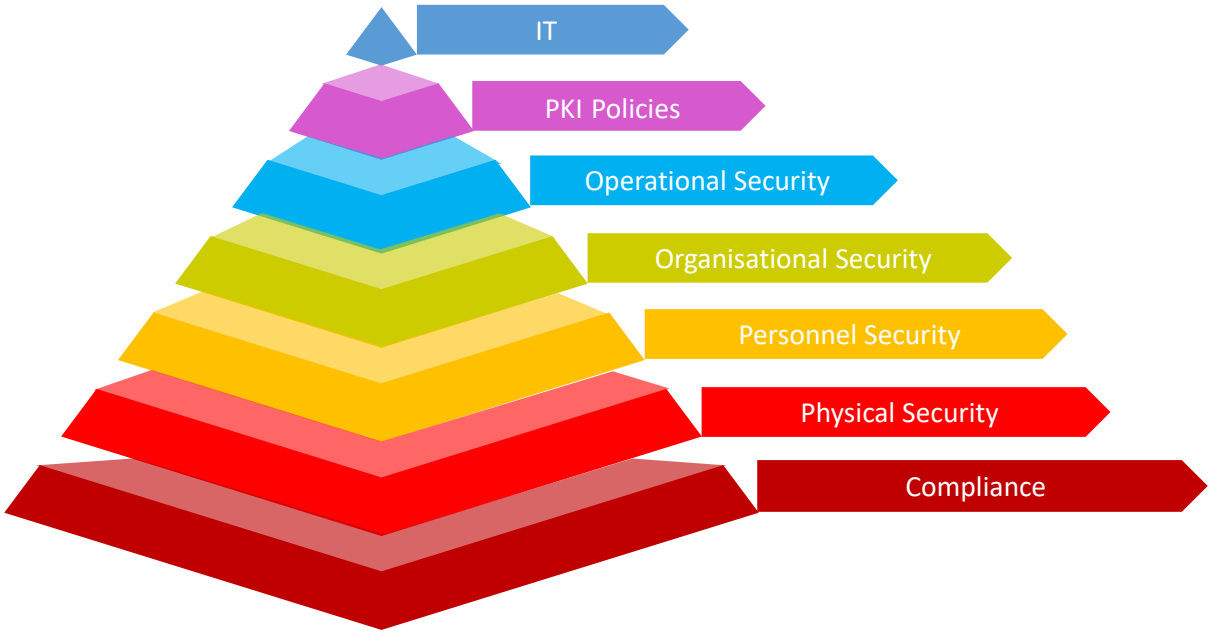

Figure 3: PKI Assessment domains

1) Compliance
   - Check if the Local PKI has been designed according to the PKI standards. Depending on the digital certificates type, one can assess the existing Local PKI to conform to ETSIor X509 rfc 5280, or eIDAS.
   - Ensure that a proper security risk assessment has been conducted to develop necessary security controls to protect the PKI (people, process and technology).
2) Check the Physical Environment:
   - Inspect the physical environment that is hosting the Back end part of local PKI (determine the security zone).
   - Check the physical security environment.
   - Review the physical and logical access to the back end part of the PKI servers.
   - Check the selection of participant personnel with assigned trusted roles to access the security zone.
3) Personnel Security controls
   - Inspect a selection of Participant personnel with assigned trusted roles to determine whether these personnel have undergone a background check in accordance with the local PKI CP/CPS.
   - Ensure that the segregation of duties is well understood and respected.
   - Inspect job descriptions for a selection of Participant personnel in trusted roles to determine whether their roles and responsibilities are defined and documented.
   - Inspect training records for a selection of Participant personnel in trusted roles to determine whether these personnel had completed required training in accordance with CP/CPS.
   - Check whether a governance is in place (at least PMA).
4) Organisational Security Management

- Inspect Local PKI Information Security Policy documentation to determine whether physical security, personnel security, and technical and procedural controls are defined (This can be part of the ISMS documentation).
- Inspect evidence that the Information Security Policy has been approved by management and communicated to employees (check the main sec doc…).
- Inspect whether a Local PKI maintains an inventory of the PKI systems.
- Inspect Local PKI management's Monitoring and Compliance procedures.

5) Operations Management
   - Inspect Local PKI security incident reporting procedure to determine whether a process for the identification, resolution and reporting of security incidents has been defined.
   - Inspect if changes made to the Local PKI systems are tracked and documented.
6) Review the Local PKI policies:
   - Inspect the Local PKI CP/CPS and check technically if what is described (claimed) in the PKI documentation is actually implemented.
   - Inspect the Local PKI CP and CPS to determine whether CPS sections address topics in the related CP sections.
   - Review the CA key management procedures, and ensure the hardware security modules is effectively implemented and correctly configured.
7) Technical Review of the Local PKI infrastructure:
   - Ensure that all PKI servers are hardened and are patched in accordance with the ISMS.
   - Ensure that the PKI back end is separated from the demilitarised zone (DMZ) and that the DMZ is protected from the public (internet) zone.
   - Review the network topology of the Local PKI and ensure that there are dedicated VLANs for at least the following sub-zones: secure, production and management.
   - Inspect the digital certificate profiles and check consistency with the standards and best practices.
   - Inspect the Local PKI CP/CPS to determine whether requirements and procedures for certificate revocation have been defined and respected.
   - Inspect if the Local PKI repositories list and their URLs are present for the local CA's.
   - Ensure that the CRL(s) (and OCSP if used) is(are) effectively generated and accessed
   - Inspect the Local PKI CP and CPS to determine whether it specifies the Authority Information Access URLs for Local PKI Issuing CA.
   - Inspect the Local PKI CP and CPS to determine whether identification and authentication procedures for authentication and signing certificates have been defined.
   - Inspect the Local PKI CP and CPS to determine whether certificate assurance levels and certificate policy OIDS are defined with corresponding object identifiers ("OIDs").