SESAR
DEPLOYMENT MANAGER

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

Certificate Policy
Annex A3.a of D1.2 Final Trust Framework

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	Annex A3.a - EACP Certificate Policy
Deliverable ID	Annex to 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 is the Certificate Policy document for the European Aviation Common Public Key Infrastructure, and is the Annex A3.a of D1.2 Final Trust Framework.

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
Abdel YOUSSOUF EUROCONTROL		28/11/2019

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	25/06/2019	Draft	A.Youssouf	Initial draft
0.1.2	01/11/2019	Draft	A.Youssouf	Review Eik Kristensen's comments
0.1.3.3	22/05/2021	Draft	A.Youssouf	Review and discuss the "Task 2" team remarks
0.2	07/06/2021	Draft	A.Youssouf	Submit version 0.2 for review
0.3	06/07/2021	Draft	A.Youssouf	Draft version submitted to SDM for comments further to Progress Meeting
0.6	09/11/2021	Draft	A.Youssouf	Draft version submitted to Thread A - Thread B Project Members for final review
0.7	11/11/2021	Draft	A.Youssouf	Draft version submitted to Project Members for final review
1.0	06/12/2021	Released Issue	P.Mana	Released issue taking into account project members comments
1.1	07/03/2022	Released Issue	A.Youssouf	Draft integrating comments raised during the 1st SDM consultation cycle.

Table of Contents

Table of Figures

Table of Tables

1. INTRODUCTION

1.1 Overview

1.1.1. Introduction to the European Aviation Common PKI

The European Aviation Common PKI (EACP) 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 different aviation organisation. 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 in CP1 (EU2021/116). The digital certificates will allow user authentication, signing 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 EACP and its associated trust framework for Europe, its integration and validation with some Stakeholders. It will ensure the interoperability of digital certificates within European[1] aviation stakeholders and with other regions.

1.1.2. CP Overview

A Certificate Policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. The Certificate Policy is further supported by a Certification Practice Statement (CPS), which is a statement of the practices that a Trust Service Provider (TSP) uses when issuing, managing, revoking, and renewing or re-keying certificates. EACP Legal Entity (EACP LE)[2] is the TSP for EACP.

The TSP shall issue digital certificates in accordance with this Certificate Policy document. This document contains the TSP's own stipulations regarding the list of stakeholders and participants in this EACP project, restrictions on usage of certificates, some technical details of the certificate(s) such as key length and cryptographic algorithm, on additional liability provisions, etc.

This Certificate Policy document describes also stipulations affecting Subscribers and Relying Parties, which are further defined in the Subscriber Agreement and Relying Party Terms and Conditions.

In all Certificates Issued under a specific certificate class are linked to a specific Certificate Policy document through an Object Identifier (OID). This OID is logically held within the digital certificate and described in the associated Certificate Policy document.

This Certificate Policy document is formatted according to the guidelines provided by IETF RFC 3647 [1] and responsibility for the Certificate Policy lies with a body known as the Policy Management Authority (PMA). Any queries regarding the content of this Certificate Policy should be directed to the Policy Management Authority.

[1] Throughout this document European shall mean ECAC-nations –

[2] EACP Legal Entity is the entity that be the one running EACP. Due to discussion outside this project about the governance in general for SWIM, SDB etc. this will be settled later. For now it is just a place holder.

This Certificate Policy document, in conjunction with the Subscriber Agreement and Relying Party Terms and Conditions specifies:

- Those who can participate in EACP including SWIM users.
- The primary rights, obligations and liabilities of the participants governed by this Certificate Policy.
- The purposes for which certificates issued under this Certificate Policy may be used.
- Minimum requirements to be observed in the issuance, management, usage and reliance upon Certificates.

The various terms used throughout this document are explained in the Glossary.

1.2 Document name and identification

This Certificate Policy is named “EACP Certificate Policy”.

EACP digital certificates are linked to this Certificate Policy through an Object Identifier (OID) contained within each Certificate. The Object Identifiers associated with this Certificate Policy and assigned to the respective EACP certificates are defined in section 1.2.1.

1.2.1 Object Identifier

EACP certificates shall be linked to this certificate policy document through an Object ID (OID) that is physically held within the associated digital certificate. By including an object identifier in its certificate, EACP provides assurance of its conformance to the identified certificate policy requirements as published in RFC 3647 [1].

EACP OID arc shall be based on the one registered for EACP. For the time being, no decision has been done yet under which organisation EACP shall be registered.

EACP OIDs arc is presented in Figure 1 below.

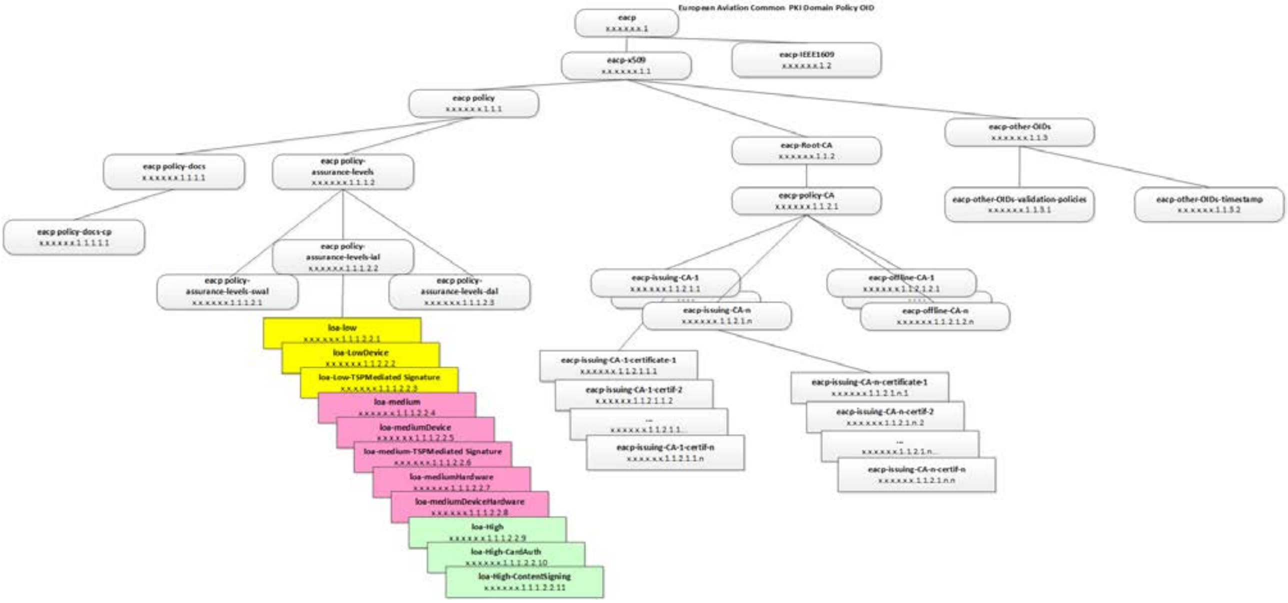
European Aviation Common PKI Domain Policy OID
eacp x.x.x.x.x.x.1
eacp-x509 x.x.x.x.x.x.1.1
eacp-IEEE1609 x.x.x.x.x.x.1.2
eacp policy x.x.x.x.x.x.1.1.1
eacp policy-docs x.x.x.x.x.x.1.1.1.1
eacp policy-assurance-levels x.x.x.x.x.x.1.1.1.2
eacp policy-docs-cp x.x.x.x.x.x.1.1.1.1.1
eacp policy-assurance-levels-ial x.x.x.x.x.x.1.1.1.2.2
eacp policy-assurance-levels-swal x.x.x.x.x.x.1.1.1.2.1
eacp policy-assurance-levels-dal x.x.x.x.x.x.1.1.1.2.3
loa-low x.x.x.x.x.x.1.1.1.2.2.1
loa-LowDevice x.x.x.x.x.x.1.1.2.2.2
loa-Low-TSPMediated Signature x.x.x.x.x.x.1.1.1.2.2.3
loa-medium x.x.x.x.x.x.1.1.1.2.2.4
loa-mediumDevice x.x.x.x.x.x.1.1.1.2.2.5
loa-medium-TSPMediated Signature x.x.x.x.x.x.1.1.1.2.2.6
loa-mediumHardware x.x.x.x.x.x.1.1.1.2.2.7
loa-mediumDeviceHardware x.x.x.x.x.x.1.1.1.2.2.8
loa-High x.x.x.x.x.x.1.1.1.2.2.9
loa-High-CardAuth x.x.x.x.x.x.1.1.1.2.2.10
loa-High-ContentSigning x.x.x.x.x.x.1.1.1.2.2.11
eacp-Root-CA x.x.x.x.x.x.1.1.2
eacp-policy-CA x.x.x.x.x.x.1.1.2.1
eacp-other-OIDs x.x.x.x.x.x.1.1.3
eacp-other-OIDs-validation-policies x.x.x.x.x.x.1.1.3.1
eacp-other-OIDs-timestamp x.x.x.x.x.x.1.1.3.2
eacp-issuing-CA-1 x.x.x.x.x.x.1.1.2.1.1
eacp-issuing-CA-n x.x.x.x.x.x.1.1.2.1.n
eacp-offline-CA-1 x.x.x.x.x.x.1.1.2.1.2.1
eacp-offline-CA-n x.x.x.x.x.x.1.1.2.1.2.n
eacp-issuing-CA-1-certificate-1 x.x.x.x.x.x.1.1.2.1.1.1
eacp-issuing-CA-1-certif-2 x.x.x.x.x.x.1.1.2.1.1.2
... x.x.x.x.x.x.1.1.2.1.1...
eacp-issuing-CA-1-certif-n x.x.x.x.x.x.1.1.2.1.1.n
eacp-issuing-CA-n-certificate-1 x.x.x.x.x.x.1.1.2.1.n.1
eacp-issuing-CA-n-certif-2 x.x.x.x.x.x.1.1.2.1.n.2
... x.x.x.x.x.x.1.1.2.1.n...
eacp-issuing-CA-n-certif-n x.x.x.x.x.x.1.1.2.1.n.n

Figure 1: EACP OID arc

EACP Identity Assurance Levels is presented in Table 1 below:

Identity Assurance Level	Definition	Variant levels	Object Identifiers
Low	This level is relevant to environments where risks and consequences of data compromise are low.	IAL 1: Low (software)	x.x.x.x.x.1.1.1.2.2.1
		IAL2: Low (hardware)	x.x.x.x.x.1.1.1.2.2.2
		IAL3: TSP Mediated	x.x.x.x.x.1.1.1.2.2.3
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.	IAL4: Medium Software	x.x.x.x.x.1.1.1.2.2.4
		AL5: Medium Hardware	x.x.x.x.x.1.1.1.2.2.5
		AL 6: Medium TSP-Software	x.x.x.x.x.1.1.1.2.2.6
		AL7: Medium TSP-Hardware	x.x.x.x.x.1.1.1.2.2.7
		AL8: Medium HSM	x.x.x.x.x.1.1.1.2.2.8
High	This level is relevant to environments where risks and consequences of data Compromise are High. This may include transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.	AL9: high Software	x.x.x.x.x.1.1.1.2.2.9
		AL10: high hardware	x.x.x.x.x.1.1.1.2.2.10
		AL11:high-HSM	x.x.x.x.x.1.1.1.2.2.11

Table 1: EACP Identity Assurance Levels' Object Identifier

1.2.2 Policy Qualifier

A policy qualifier is an attribute defined in the certificate policies extension of a digital certificate. See [2] for more details on which fields are supported by EACP certificates.

This Certificate Policy and its associated Certification Practices Statement are made publicly available.

Subscribers and relying parties can use the link explicitly given in the policy qualifier of the certificate policy extension to download those documents.

1.3 PKI participants

As a TSP, EACP LE has an obligation to operate a Public Key Infrastructure in accordance with the defined Certificate Policy. EACP LE does not however have to conduct all aspects of Public Key Infrastructure operations itself. There may be a set of services that can be logically and conveniently grouped and outsourced.

For EACP solution, the participant roles are:

- EACP.
- Policy Management Authority.
- Certification Services providers:
  - Registration Authority,
  - Certificate Authority,
  - Dissemination Authority,
  - Revocation Management Authority,
  - Revocation Status Service ,
  - Subject Device Provision Service .
- Subscriber (Airports, Aircraft, etc.),
- Relying Party.

Under this scheme Subscribers and Relying Parties only have a contractual relationship with EACP LE. These relationships are defined by EACP Subscriber Agreements and EACP Relying Party Terms and Conditions.

1.3.1 Trusted Service Providers

TSPs is an entity responsible for managing PKI services that uses strong mechanisms for authentication, digital certificates and electronic signatures.

Mechanisms on how TSP performs authentication and non-repudiation services and how they are to be regulated and recognized can be found in [10].

1.3.2 The PKI Policy Management Authority

EACP Management Authority (PMA) is a body designated by EACP LE to oversee the creation, update and approval of Certificate Policies, including evaluation of changes requested by EACP users including SWIM civil and military bodies, and plans for implementing any accepted changes.

EACP Policy Management Authority shall review the results of any EACP compliance audits to determine if EACP CAs are adequately meeting the stipulations of approved CPS documents and make recommendations to EACP CAs regarding corrective actions, or other measures that might be appropriate.

In cases where the technical mechanism of "policy mapping" is being considered, EACP PMA shall establish the suitability of external policies for compatibility with at least one EACP Certificate Policy in support of cross-certification. EACP PMA shall establish the suitability of external PKIs for other forms of interoperability.

EACP PMA shall provide guidance to EACP Program and Project Managers and EACP regarding the appropriateness of certificates associated with EACP Certificate Policies for specific implementations.

1.3.3 EACP Policy Management Unit

The Policy Management Unit, supported by "Technical Advisory Task Force", made of PKI expert from EACP members and "PK User Group" made of PKI expert from EACP users shall provide EACP PMA with PKI technical consultancy, advices and guidances, proposing technical prioritisation where needed, and PKI technical research and policy development activities.

1.3.4 Certification Authorities

A Certification Authority is an entity of EACP, named EACP CA, authorised by EACP LE to create, sign, issue and manage digital certificates. EACP is comprised of hardware, software, personnel, processes and procedures that are required to implement the SWIM PKI digital lifecycle management described in this policy. EACP is responsible for all aspects of the issuance and management of a certificate. This include control over the registration process, the certificate issuance process, revocation process, publication of certificates, validation of certificates, renewal and/or rekey, etc.

1.3.5 Subscribers

A subscriber is the entity responsible for enrolling a certificate on behalf of a subject. A subject is an entity whose name appears as the subject in the certificate. The subscriber asserts that the use of the certificate and its associated keys will be made in accordance with this policy.

The targeted PKI subscribers include but are not limited to the following categories of entities:

- ANSP / ADSP / ATSP
- Airlines (Passenger Services, Pax info with Authorities Admin, Flight Entertainment, etc)
- Airport Operators (e-Passport, Security Access Control, Border Control)
- EUROCONTROL (CRCO, SWIM NM B2B, EAD, MUAC, IANS)
- MET providers

Subscribers must adhere to the terms and conditions of EACP Subscriber Agreement prior to apply and use of any EACP certificate.

1.3.6 Registration Authorities

A registration authority is an entity that implements the registration, identification and authentication processes by collecting and verifying subscriber’s identity and information that is to be input into certificates. The RA approves or denies the certificate issuance and deals with revocation and suspension requests. The RA performs its functions in accordance with the processes as set forth in this Certificate Policy and its associated Certificate Practice Statement.

1.3.7 Local Registration Authorities

As EACP participants are widely dispersed geographically, it may be useful to delegate some central RA functions to a Local RA named Local Registration Authorities (LRAs). The primary purpose of an LRA is to off-load certain functions from the central Registration Authority and to enhance scalability and decrease operational costs.

The functions implemented by the LRA shall support the main functions of the central RA.

1.3.8 Revocation Authorities

Revocation Authority is an entity within EACP services performing revocation of certificates when they become compromised. The Revocation Authority publishes a list of revoked certificates in a specific flat file named Certificate Revocation List (CRL) containing the serial numbers of certificates revoked by the Issuing Certificate Authority and giving the reason of revocation.

1.3.9 Relying Parties

A relying party is the entity who trusts the certificate, and per consequent, the validity of the binding of the subject's name to a public key. This reliance may result from using another subject's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate.

A relying party shall determine the suitability of the certificate for the intended purpose prior to use. The relying party may use information in the certificate (such as Certificate Policy identifiers) to determine this suitability.

A relying party may be a subscriber of EACP, or a subscriber of a separate PKI that has a formally approved trust relationship with EACP (e.g. is cross-certified or otherwise interoperable with EACP.) Relying parties include subscribers, subordinate EACP CA’s and RA's which require a reliance on certificates issued by EACP.

Relying party must read carefully the Relying Party Terms and Conditions prior processing an EACP certificate.

1.3.10 Other Participants

Other participant in EACP are:

- Auditors
- Signing (as a service) Authority
- Validation (as a service) Authority
- OCSP

1.4 Certificate usage

Certificate asserting a policy as defined in this document shall only be used for transactions related to the European Aviation business. EACP CAs shall state this requirement in their CPS and impose a requirement on subscribers to abide by this limitation.

EACP shall support the following security services: access control, confidentiality, integrity, authorisation, authentication and non-repudiation. EACP provides these security services by the mean of digital certificates.

1.4.1 Appropriate certificate uses

The level of assurance associated with a public key certificate is an assertion by the Common PKI CA of the degree of confidence that a relying party may reasonably place in the binding of a subject's public key to the identity and authorisations asserted in the certificate. Level of assurance depends on the criticality level of information/data to be protected and is reflected in the proper registration of subscribers and the proper generation and management of the certificate and the associated private key, in accordance with the stipulation of this policy. Personnel, physical, procedural and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.

1.4.2 Prohibited certificate uses

The digital certificates issued within EACP shall only be used for the purpose(s) defined within this Certificate Policy. All other usage outside of this Certificate Policy is prohibited.

1.5 Policy administration

1.5.1 Organization administering this document

EACP Policy Management Authority administers this document. In the first instance, all questions and comments regarding this Certificate Policy should be addressed to the contact person listed in 1.5.2.

1.5.2 Contact person

Give the contact of the PMA

1.5.3 Person determining CPS suitability for the policy

EACP PMA determines the suitability of any Certification Practice Statement operating under this Certificate Policy.

1.5.4 CPS approval procedures

EACP Policy Management Authority determines the suitability and approves the use of any Certification Practice Statement, which is used to support this Certificate Policy.

1.6 Definitions and acronyms

1.6.1 Definitions

Advanced Electronic Signature:	An Electronic Signature that meets the following requirements: ▪ It is uniquely linked to the signatory; ▪ It is capable of identifying the signatory; ▪ It is created using methods that the signatory can maintain under his sole control; and

	▪ It is linked to the data to which it relates to in such a manner that any subsequent change of the data is detectable
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certificate Validity Period	The time interval during which the CA warrants that it will maintain information about the status of the certificate. (Time interval between start validity date and time and final validity date and time).
Certificate Revocation List (CRL)	A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certificate Trust Chain	An ordered list of certificates that contains the end-entity certificate, intermediary certificates and the certificate for the Root CA such that a relying party may follow the trust chain up to and including the top-level trust anchor.
Trust Service Provider (TSP)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Certification Practice Statement (CPS)	A formal statement of the practices that a certification service provider employs in issuing, managing, revoking, and renewing or re-keying certificates.
CRL Distribution Point	A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.
Digital Certificate	An electronic attestation, which links signature verification data to a person and confirms the identity of that person.
Digital Signature	An electronic signature created using digital certificate cryptography.
Electronic Signature	Means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.
End Entity	A certificate holder that uses its private key for any purposes as specified in his/her certificate and always other than signing certificates.
EACP participants	The term used to refer to all of the participants that are required to follow the practices defined CPS. The participants within EACP are: ▪ Certification Authorities (Root and subordinate CAs); ▪ Registration Authorities; ▪ Subscribers; ▪ Relying Parties, and; ▪ Other Participants such as the OCSP responder and SCVP
EACP CAs	The term used to refer to EACP Root or its subordinate CAs.
Object Identifier (OID)	A sequence of numbers that uniquely and permanently references an object.
PKI Management Authority	The management team that acts on behalf of EACP LE Authority and is responsible for the compliance of the Common Certification Authorities with this Certification Practices Statement.

Public Key	That key of an entity's asymmetric key pair that can be made public.
Private Key	That key of an entity's asymmetric key pair that should only be used by that entity
Secure Signature Creation Device	a secure device handling the private key of the subject.
Secure User Device	Device that holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Signature Creation Data	Means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.
Signature Creation Device	Means configured software or hardware used to implement the signature creation data.
Signer	Entity that creates an (electronic) signature.
Signatory	A person who holds a signature creation device and acts either on his own behalf or on behalf of the natural legal person or entity he represents.
Signature Policy	requirements imposed / committing the GOM PKI actors with respect to the application of electronic signatures on documents and data that should be signed in the context of a particular transaction, process or business in order for these signatures to be considered as valid (technical) signatures
Signature Verification	A process performed by a verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.
Subject	Entity to which a Certificate issued.
Subscriber	Entity that request and subscribes to a Certificate and for which it is either the Subject or not.
Time Stamp	A proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum.
Verifier	An entity that validates or verifies an electronic signature. This may be a relying either party or a third party interested in the validity of an electronic signature.
Validation Data	Additional data, collected by the signer and/or a verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include certificates, revocation status information, time-stamps, etc.

1.6.2 Acronyms

ANSP	Air Navigation Service Provider
AIS	Aeronautical Information Services
BCA	Bridge Certification Authority
CA	Certification Authority
CDP	CRL Distribution Point
CRL	Certificate Revocation List

CRCO	Central Route Charges Office
EACP	European Aviation Common PKI
EACP LE	EACP Legal Entity
EAD	European AIS Database
EC	Elliptic Curve
FAA	Federal Aviation Administration
IANA	Internet Assigned Number Authority
IATF	International Aviation Trust Framework
ICAO	International Civil Aviation Organisation
MIL	Military Organisation
MUAC	Maastricht Upper Area Control Centre
NM B2B	Network Manager Business to Business
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RFC	Request For Comment
RA	Registration Authority
SCVP	Sever Certificate Validation Protocol
SLA	Service Level Agreement
SSCD	Secure Signature Creation Device
SSL	Secure Socket Layer
SWIM	System Wide Information Management
TSP	Trust Service Provider
VA	Validation Authority
VPN	Virtual Private Network

2. Publications and Repository Responsibilities

2.1 Repositories

An information Repository shall be made available under the terms of this Certificate Policy. EACP LE is the entity with overall responsibility for the operation of the Repository, which it may delegate to Participants providing Certification Services.

2.2 Publication of certification information

EACP shall ensure that at least the following items are published and made continuously available for all PKI Participants:

- This Certificate Policy
- The Certification Practices Statement (CPS)
- Subscriber Agreement
- Relying Party Terms and Conditions
- All CA Certificates issued by the TSP
- Certificate status information for all Certificates Issued under this Certificate Policy.

The location of or mechanism to obtain access to this Certificate Policy shall be provided in Certificates issued under this Certificate Policy.

When superseded, the documents listed above shall be archived at location:

http://repository.common-pki.eacp.int/Archive and made continuously available for all PKI Participants.

2.3 Time or frequency of publication

Information as listed in 2.2 shall be published promptly upon its creation, with the exception that if Certificate Revocation Lists (CRLs) are used to provide Revocation information, they shall be published according to section 4.9.7 and 4.9.8 of this Certificate Policy.

2.4 Access controls on repositories

The Repository shall make available the information specified in section 2.2. The Repository may control access to this information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Within EACP, each entity shall have a clearly distinguishable and unique Distinguished Name (DN) in the certificate subject name field. This unique DN shall not be blank and shall be in the form of a X.501 UTF8 Printable String and in accordance with RFC5280. Each entity may use an alternative name via the subjectAlternateName extension field, which shall also be in accordance with RFC5280, or issuerAlternativeName extension field, which is in accordance with ETSI EN 319 412-2 V2.2.1 (see [9]).

3.1.2 Need for names to be meaningful

Names used within EACP shall identify the entity to which the certificate is assigned. EACP CA or RA shall ensure that an affiliation exists between the subject and any organisation that is identified by any component of any name in its certificate.

In the DNs, the common name shall represent the subject in a way that is easily understandable for humans. For people, this will typically be a legal name. For device, this may be a model name and serial number, MAC address or an application process, etc.

EACP shall use the naming convention for managing the DNs and DN namespace. Table 2 and Table 3￼￼￼￼give the Subject Name Forms for CAs and for entities respectively.

Subject Name Form for CAs			
USAGE	**ATTRIBUTE**	**REQUIRED COUNT**	**CONTENT**
Required	CN	1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
Optional	OU	0..N	"Certification Authorities" or similar text
Required	O	1	Issuer name, e.g., "O=XYZ Inc"
Optional	C	1	Country name, e.g., "C=FR"

Table 2: Subject Name Forms for CAs

Subject Name Form for entities			
USAGE	**ATTRIBUTE**	**REQUIRED COUNT**	**CONTENT**
Required	CN	1	Descriptive name for CA, e.g., "CN=XYZ"
Optional	OU	0..N	"organization unit" or similar text OU="IT"
Required	O	1	Issuer name, e.g., "O=ADP"
required	C	1	Country name, e.g., "C=FR"

Table 3: Subject Name forms for entities

EACP CAs and RAs shall co-ordinate with EACP to determine the proper elements for a given subject.

EACP asserting this policy shall only sign certificates with subject names from within a name space approved by EACP. In the case where delegation is given, the certifying entity must impose restrictions on the name space authorised in its domain, which are at least as restrictive as EACP name constraints.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity is not permitted within EACP. The provision of pseudonymity to subscribers is neither explicitly permitted nor prohibited by the Policies defined within this document. Pseudonymity shall not be used in conjunction with nonrepudiation services. CA's providing these services shall include within their CPS documents, the procedures for providing pseudonymity for subscribers, the mechanisms used internally to explicitly map these identities to the persons holding them, and the regulations and procedures for breaking this service. EACP PMA shall review the CA's procedures for the provision of this service to determine whether the operational requirement has been appropriately vetted, and whether the provision of the service is within the best interest of EACP community as a whole.

3.1.4 Rules for interpreting various name forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.2) and are established by EACP PMA. The naming authority (CAs) shall be identified in EACP CPS.

3.1.5 Uniqueness of names

Distinguished names shall be unique for all End-Entities of EACP CA. For each subject, additional numbers may be appended to the commonName, or a serial number field may be added to the DN to ensure the RDN's uniqueness. The Unique Identifiers capability to differentiate subjects with identical names shall not be supported.

3.1.6 Recognition, authentication, and role of trademarks

PMA, as the naming authority, has the right to make all decisions regarding names in all EACP assigned certificates. A party requesting a certificate shall demonstrate its right to use a particular name. Where there is a dispute about a name in a repository not under its control, EACP shall ensure that there is a name claim dispute resolution procedure in its agreement with that repository.

Trademarks, logos or otherwise copyrighted graphic or text material are not permitted in EACP Certificates.

It is solely the subscriber's responsibility that their choice of name does not violate any trademark and copyright or Intellectual Property infringement of any person or entity, whether fraudulently, negligently, innocently or otherwise. EACP or Participants providing Certification Services are not obligated to check such rights. If the TSP is notified of a violation of such rights, it has the right to revoke the Certificate.

Subscribers are required to declare legitimacy of their registration details as part of the Registration Process.

Name claim disputes are resolved in conformance with this Certificate Policy.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Prior to the issuance of EACP, the subscribers shall authenticate themselves to EACP platform. Acceptable mechanisms for this authentication include pre-shared secret or PKIX Certificate Management Protocol [6].

For all Certificate types, technical means employed to ensure possession of Private Keys shall be PKCS#10: the subject shall use its private key to sign a value and provides that value to the issuing EACP CAs. The issuing CA will then validate the signature using the party's public key.

3.2.2 Authentication of organization identity

Requests to participate in EACP can be addressed by European Aviation stakeholders. Participants shall sign the "Master and/or User Participation Agreement" that set forth among others the eligibility criteria to become EACP Participant. Request shall include the organization name, address, and some documentation of the existence of the organization. EACP shall verify the information provided and the authenticity of the requesting representative, and the representative's authorization to act in the name of the organization prior to accepting the candidate to become an effective EACP Participant.

3.2.3 Authentication of individual identity

The identity of the Subscriber and, if applicable, any specific attributes of the Subscriber, shall be verified during the vetting process.

In case of face to face identification and authentication is required, EACP CA or RA shall compare the identity of the individual with a piece of Government issued photographic identification. Face to face authentication shall occur at every certificate request (including during renewal). EACP CA or RA shall keep a record of the type and details of identification used.

For EACP CA Certificates, , the Identity of the CA's authorised representative(s) shall be carried out using a procedure, developed in EACP Key Management Procedures, and approved by the Policy Management Authority.

3.2.4 Non-verified subscriber information

All information collected to ascertain the identity of a subscriber, and that will be included in a certificate shall be verified.

3.2.5 Validation of authority

Certificates shall be issued only after ascertaining that the subscriber has the authorisation to act on behalf of the organisation. Examples of these include organisation such as delegated CAs, RAs, role certificates, etc.

3.2.6 Criteria for interoperation

The criteria by which another TSP wishing to operate within or interoperate with EACP governed by this Certificate Policy, shall be defined in the Criteria and Methodology for interoperability [17] and approved by EACP PMA.

EACP LE shall determine whether any specific TSP is approved for interoperability.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

For end entity certificates issued under this policy, identification and authentication for routine re-key shall be achieved by the current signature key or by following the procedure used for initial Certificate issuance and conform to the policy requirements defined in section 3.2.

For CA Certificates, identification and authentication for routine re-key shall be carried out using a procedure developed in Key Management Procedures and approved by EACP PMA Authority.

3.3.2 Identification and authentication for re-key after revocation

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key, EACP shall authenticate a re-key in the same manner as for initial registration. Any change in the information contained in a certificate shall be verified by EACP CA or RA authorised to act on behalf of that EACP before that certificate is issued.

3.4 Identification and authentication for revocation request

EACP CA or RA acting on its behalf, shall authenticate a request for revocation of a certificate. EACP shall establish and document the process by which it addresses such requests and the means by which it establishes the validity of the request. Requests for revocation of certificates shall be logged.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Digital certificate application can only be processed by authorised subscribers to act on behalf of a subject. A subscriber is an individual representing an European Aviation organisation, or a European Civil or Military Aviation body to which the subject is attributable for the purposes of accountability and responsibility.

An application for a European Civil or Military organisation to be a Registration Authority shall be made by a sponsor representing that organisation and authorised to act on behalf of that organisation. Identification and authentication and authorisation of the prospective sponsor shall conform to this policy. A sponsor is an individual or a European Civil or Military Aviation body representing that organisation who shall be accountable and responsible for vetting the registration services as per this policy.

An application for an existing Certification Authority (Local PKI) to be interoperable with EACP can only be made by the sponsor of that Local PKI , authorised by EACP Advisory Group and approved by EACP PMA.

External subscribers (external to the European Aviation stakeholders) may submit applications for certificates subject to vetting by EACP LE.

4.1.2 Enrolment process and responsibilities

The applicant and EACP CA or RA shall perform the following steps when an applicant applies for a certificate:

- Provision of accurate information in support of identification and authentication of the applicant (per Section 3.2);
- obtain a certificate request (or in some cases generate public/private key pair and associated certificate request) for each certificate required;
- establish that the public key forms a functioning key pair with the private key held by the subscriber;
- Acceptance of the subscriber agreement, and of the applicable terms and conditions governing their use of the certificate.

Requests for a new and internal EACP CA certificate shall be submitted to EACP PMA using the contact provided in section 1.5.2, and shall be accompanied by a modified CP and CPS for the approval purpose. EACP PMA shall evaluate the submitted CPS for acceptability.

Request for a delegated CA shall be made by an aviation stakeholder, submitted to EACP Advisory group and approved by EACP PMA using the contact provided in section [1.5.2], and shall be accompanied by a modified CP and CPS for the approval purpose. EACP PMA shall evaluate the submitted CPS for acceptability. EACP PMA may require an initial compliance audit, to ensure that the new CA is prepared to implement all aspects of the submitted CPS, prior to EACP PMA authorizing EACP CA to issue and manage certificates asserting EACP Certificate Policy.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Upon receiving the request, EACP CA or RA shall:

- verify the identity of the requestor according to the associated Identity Assurance Levels;
- verify the authority of the requestor and the accuracy and integrity of the information in the certificate request;
- if all certificate requirements have been met, then build and sign a certificate;
- make the certificate available to the subscriber.

The requested certificate shall not be signed until all verifications and modifications, if any, have been completed to EACP CA's satisfaction. If a certificate request has been denied by a Registration Authority, then EACP CA shall not sign the requested certificate and shall report the problem to the applicant.

While the subscriber may provide most of the data entry (the DN and some extra data), it is still the responsibility of EACP CA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing prefilled DN's fields or through personal contact with the specific attribute authority (as put forth in EACP CPS). If databases are used to confirm subscriber attributes, then these databases shall be protected from unauthorised modification to a level commensurate with the level of assurance specified for the certificates conveying the subscriber attributes.

EACP CAs shall verify all authorization and other attribute information received from an applicant. In most cases, the RA is responsible for verifying applicant data, but if EACP CAs accept applicant data directly from applicants, then EACP CA is responsible for verifying the applicant data. In case of delegated CA or RA, information regarding attributes shall be verified via those offices or roles that have authority to check the information or attribute. Relationships with these offices or roles shall be established prior to commencement of EACP CA duties, and shall be described in EACP CPS.

4.2.2 Approval or rejection of certificate applications

An application for a certificate does not oblige EACP to issue a certificate. The Registration Authority shall either approve or reject a certificate application.

Where an application fails to achieve the specified authentication requirements or the level of assurance of authentication as required under this CP cannot be met, a certificate application will be rejected.

Where approved, the certificate application will be digitally signed by the appropriate EACP CA.

For Safety related certificates, it shall not be possible for a single individual acting in a Registration Service trusted role to process and approve a certificate application resulting in the issuance of a certificate. Authorisation from a minimum of two persons shall be required before any Certificate is issued.

4.2.3 Time to process certificate applications

Certificates shall be processed in a reasonable time frame, while ensuring that all required steps are completed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The issuance and publication of a certificate by an EACP CA indicates a complete approval of the certificate application by EACP CA.

Any EACP CA who includes authorizations in a certificate shall document in its CPS the mechanisms used to verify authorizations and to notify EACP CA of the withdrawal of authorization. Withdrawal of authorization shall result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate authorizations.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Where enrolment is completed directly at the CA or RA, notification is deemed to be completed at the end of a successful enrolment process which may include the publication of the certificate within the directory or an e-mail, triggered automatically by EACP CA, informing the subscriber that a certificate has been generated on his behalf, and giving instructions on how to load the certificate.

Where remote enrolment is completed, the publication of the signed certificate within the directory is deemed to be the notification. Notification of certificate issuance to other parties within this document is deemed to be the publication of the relevant certificates within the directory or an automated e-mail generated by EACP CA, and sent to the subscriber with a notification of issuance of the certificate with the instructions on how to load the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Before entering into a contractual relationship with an applicant, EACP shall inform the applicant of the terms and conditions regarding the certificate use, as expressed through the Subscriber Agreement and any other applicable document outlining the terms and conditions of the certificate use, and record their explicit acceptance of these terms and conditions.

A Subscriber shall acknowledge that he agrees to the terms and conditions stipulated in the Certificate Policy and associated Subscriber Agreement and any other applicable contractual commitments prior to first use of the Certificate.

Before EACP allows a subscriber to make effective use of its private key, EACP shall:

- explain to the subscriber its responsibilities as defined in this policy;
- inform the subscriber of the creation of a certificate and the contents of the certificate;

- require the subscriber to indicate acceptance of its obligations and its certificate ; and
- record and archive the subscriber's acceptance of its responsibilities and its certificate.

The ordering of this process, and the mechanisms used, shall depend on factors such as where the key is generated and how certificates are posted. In the case of non-human components (router, firewalls, etc.), the subscriber shall perform these functions.

4.4.2 Publication of the certificate by the CA

CA Certificates shall be published to the Repository. End entities certificates shall not be published.

4.4.3 Notification of certificate issuance by the CA to other entities

See paragraph 4.3.2

4.5 Key pair and certificate usage

4.5.1 CA private key and certificate usage

EACP shall ensure that its certificate signing private key is used only to sign certificates and CRLs. EACP Root CA shall only issue certificates to its subordinate CAs and to their own operational roles as defined within this policy. EACP subordinate CAs shall issue general purpose certificates to subscribers as defined in this policy.

EACP shall ensure that private keys issued to its personnel to access and operate EACP CA software are used only for such purposes. If required, EACP CA operators may be issued a subscriber certificate and keys for purposes other than EACP CA use.

4.5.2 Subscriber private key and certificate usage

The subscriber shall use the keys and certificates only for the purposes identified in the Certificate Policy and associated Subscriber Agreement.

Subscribers shall ensure that use of the Private Key associated with the Certificate is consistent with the usage restrictions in the Certificate as stipulated and published by EACP, and take all reasonable measures to prevent their loss, disclosure, modification, or unauthorised use.

CAs shall only use CA key pairs and associated Certificates for purposes defined in the CA Certificate key usage extension

4.5.3 Relying party public key and certificate usage

Relying parties shall only rely on Subject' public keys and certificates when they are being used for their intended purposes as defined by this document and the relevant CPS documents. It is the responsibility of the relying party to use the most adequate and supported validations tools (OCSP or SCVP) and if needed ensure that they check the most recent CRL and ARL information.

4.6 Certificate renewal

Certificate renewal is not allowed by EACP. All applications for certificate renewal shall be treated as applications for a new certificate.

CA certificate renewal is not supported.

4.6.1 Circumstance for certificate renewal

This policy does not support certificate renewal

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Certificates which have not been revoked may be re-keyed prior to their expiry. Certificates should be re-keyed in a timely fashion prior to their expiry, taking into consideration operational impact and continued requirements for the certificates. Prior to deployment, subscribers shall ensure that their remaining certificate life prior to expiry is sufficient for the required mission.

4.7.2 Who may request certification of a new public key

The re-key process shall only be initiated by a subscriber, or the CA / RA managing those entities.

4.7.3 Processing certificate re-keying requests

See section 4.2.

4.7.4 Notification of new certificate issuance to subscriber

Notification of new certificate issuance to a subscriber shall follow the procedure used for initial Certificate issuance. See section 4.3.2

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Conduct constituting acceptance of a re-key Certificate shall follow the procedure used for initial Certificate acceptance. See section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed CA Certificates shall be published to the repository. Re-keyed end entity certificates shall not be published. See section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

Certificate modification occurs when changes other than the public key is required to an existing certificate. In EACP, certificate modification is not allowed. EACP CA or RA shall proceed to certificate re-keying instead of certificate modification.

4.8.1 Circumstance for certificate modification

A certificate modification may be required for a number of reasons, including:

- ➢ Following a reorganisation of affiliation resulting in a change of distinguished name (DN) other than the CN
- ➢ Following a change in policy OIDs or policy constraints
- ➢ For a CA certificate following a change in the DN, signature algorithm or any certificate extension

EACP CA or RA that supports certificate modification should specify the circumstances under which a modification is permissible in its CPS, and conditions for proceeding with rekeying the existing certificates.

4.8.2 Who may request certificate modification

An existing subscriber or sponsor may request modification of its certificate, or of any certificate under its control.

The CA or RA may request modification of any existing certificate within the CA or RA domain of control. This will normally be done when some significant change is required for all certificates of a particular type.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate shall be revoked when:

- a Subscriber requests that the certificate be revoked, and the request is properly authorised in accordance with section 3.4
- the certificate contains invalid information,
- there is suspection or known compromise of the private key;
- there is suspection or known compromise of the media holding the private key;
- termination of affiliation with EACP civil or military aviation body;
- termination of need for EACP Certificate;
- determination that registration information was invalid;
- the subscriber is decreased or no longer authorised to use the certificate;

- any certification Services provider associated with certificate issuance does not comply with EACP CPS;
- EACP ceases its operations;
- a suspended certificate has exceeded the permitted certificate suspension period.

EACP CA in its discretion may revoke a certificate when a subscriber fails to comply with obligations set out in EACP Certificate Policy, the CPS, any agreement or any applicable law.

Where an external CA is cross-certified with EACP CA, EACP PMA, through EACP Interoperability CA, shall revoke the cross-certified certificate:

- when any of the information in the External CA certificate changes;
- upon compromise of the External CA private key;
- upon compromise of the media holding the cross-certified External CA private key;
- When the External CA certificate is revoked.

EACP PMA, in its discretion, may direct EACP Root CA to revoke any subordinate CA it is no longer trusted by the Policy Management Authority.

EACP PMA, in its discretion, may direct EACP Root CA to revoke a cross-certificate when an external PKI fails to comply with obligations set out in its Certificate Policy, CPS, any agreement or any applicable law.

4.9.2 Who can request revocation

The revocation of a certificate shall only be requested by:

- the subscriber or subject in whose name the certificate was issued;
- the individual which made the application for the certificate on behalf of a device (the Sponsor or his authorised designate);
- relevant Security Officer
- EACP PMA

The revocation of a subordinate CA shall only be requested by:

- EACP PMA.

The revocation of a cross-certificate shall only be requested by:

- the External PMA on whose behalf the cross-certificate was issued;
- EACP PMA.

4.9.3 Procedure for revocation request

Revocation requests shall be authenticated and authorised. An authenticated revocation request, and any resulting actions taken by EACP CA, shall be recorded and retained. In the case where a certificate is revoked, full justification for the revocation shall also be documented. Where a subscriber certificate is revoked, the revocation shall be published in the appropriate CRL. EACP CA or RA personnel revoking certificates shall notify the subscriber or sponsor of the certificate to minimise operational impact.

Where reliable authentication of the revocation request is not possible or even omitted, EACP Revocation Service is authorised to conduct revocation after seeking confirmation of the request to the greatest extent possible. Processes may involve additional checking and information gathering to allow EACP Revocation Service to achieve a satisfactory level of assurance in the validity of the request.

Where a cross-certificate or EACP subordinate CA certificate is revoked, the revocation shall be published in the ARL of the Issuing EACP Root CA.

EACP shall ensure that any procedures for the expiration, revocation and re-key of a certificate are expressly stated in the subscriber agreement and any other applicable document outlining the terms and conditions of the certificate use.

4.9.4 Revocation request grace period

If a revocation request is approved, it shall be reflected in the next scheduled publication of a CRL and in the next update of the certificate status services (see 4.10). EACP shall publish a new CRL instantly after a revocation request has been approved.

Revocation of a Cross-certified certificate or subordinate CA certificate shall result in a new CRL being issued promptly. This action shall be carried out in accordance with a timescale defined by the TSP and agreed with EACP PMA.

4.9.5 Time within which CA must process the revocation request

The time to process a Certificate Revocation request is made up of two elements:

- The time for the request to be validated, approved and action taken by EACP Revocation Service.
- The time taken for the certificate generation Service to respond to the authorised Certificate revocation request and for updated certificate status information to be published.

Any action taken by the CA as a result of a request for revocation of a certificate shall normally be completed within one hour from the time of notification. Where the investigation requires more than 24 hours (e.g. for a Cross-CA revocation request or subordinate CA revocation request), EACP Certification services shall notify EACP PMA, of the requirement to extend the processing time. Once the requirement to revoke a certificate has been ascertained, the revocation shall be completed accordingly.

Revocation services shall be available 24 hours a day and 7 days a week continuous.

4.9.6 Revocation checking requirement for relying parties

Relying Parties shall comply with the requirements defined in the Relying Party Terms and Conditions. The Relying Party shall check the validity of a certificate on which they may wish to rely and all certificates in the certificate chain. Additionally, the suspension and revocation status of a certificate on which the Relying Party may wish to rely and all the certificates in the certificate Chain up to but not including the Root CA certificate shall be checked. If any of the certificates has expired or has been suspended or revoked, any reliance on the certificate for the validation purpose is solely at the Relying Party’s own risk. To this end the Relying Party shall on the occasion of each reliance refer to CRL or OCSP status information in accordance with this policy.

Certificate status information shall be made available via CRLs, OCSP and the SCVP protocols. CRL certificate status information shall include status information on expired Certificates.

Subscriber CRLs are published at least daily. CA CRLs are published at least every 90 days.

The definitive status of a certificate is provided via the OCSP and SCVP methods. It is recommended to use these two mechanisms. Relying parties may also check certificate revocation lists, these however, are provided for assistance and convenience only.

4.9.7 CRL issuance frequency

CRLs are periodically issued and posted to a repository, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which EACP will post early updates, these shall be spelled out in its CPS. EACP shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL. The repository shall ensure that superseded CRLs are removed from the directories with which the repository has replication agreements.

EACP Root CA CRL shall be published at least every 90 days.

EACP subordinate CA CRLs shall be published on daily basis.

4.9.8 Maximum latency for CRLs

CAs shall make allowances for the latency of the network environment within which they are operating. To ensure that CRLs are fully propagated prior to the expiry of the previous CRL, CA’s shall set the next update value within CRLs to a value which allows for the propagation of the CRL prior to the expiry of the previous CRL. Where manual transfers are required (such as for the offline Root CA) the next update value shall be 15 days.

The increase afforded to online CA’s may be up to an hour or more depending on the number of directory replications required to promulgate the CRL across the entire alliance. The CA CPS shall provide detailed rationale as to the time allowance required to address the latency of the directory system. An EACP CA shall also to the best of its ability ensure that its CRL issuance is synchronised with any directory synchronisation to ensure the accessibility of the most recent CRL to relying parties prior to the expiry of the previous CRL. When a certificate is revoked due to key compromise, the updated CRL shall be issued immediately within the 1-hour limit defined in section 4.9.5.

4.9.9 On-line revocation / status checking availability

This Certificate Policy implements Online Certificate Status Protocol (OCSP) and Server Certificate Validation Protocol (SCVP). OCSP and SCVP responders shall be hosted in the back end zone of the PKI, as the CA part one, and therefore shall conform to the same technical and security standards as EACP CA(s) which it supports.

OCSP and SCVP responders shall meet the same system security and availability requirements as the certificate repository. Specifically, the OCSP and SCVP responders shall have the same redundancy requirements as the certificate repository. The hardware cryptographic module for the OCSP and SCVP responders shall meet the standards as defined for the CA hardware cryptographic module.

4.9.10 On-line revocation checking requirements

Subscribers may choose between the use of any available revocation checking mechanism including WEB and LDAP directories hosting the CRL's files, and OCSP and SCVP. The requirements for validating certificate paths and certificate status are however provided by the SCVP. The location of the WEB and LDAP directories as well as the OCSP shall be published within the CDP or AIA fields of the certificate as appropriate.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements re key compromise

In the event of the compromise, or suspected compromise, of any subscriber’s private keys, the entity shall notify EACP Issuing CA immediately.

In the event of the compromise, or suspected compromise of an EACP Issuing CA or Root CA, EACP CA shall immediately notify EACP PMA who will take the necessary actions.

In the case of the compromise of an external cross-certified CA, the PMA of the cross-certified CA shall immediately be notified by EACP PMA.

EACP shall ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.9.13 Circumstances for suspension

Certificates shall be suspended in the following circumstances:

- When a Subscriber requests a Certificate suspension
- When a Subscriber requests a Certificate revocation and the revocation procedure is not yet completed
- When a request is received with appropriate authentication from a person who has power of attorney, or any reliable party such as an RA, Security Officer, etc.

4.9.14 Procedure for suspension request

An approved request for Certificate suspension shall result in the suspension of the certificate held by the Subscriber under this Certificate Policy.

Certificate suspension requests shall include sufficient information to uniquely identify the certificate which is the subject of the request.

Suspension requests shall be made to EACP Revocation Service which shall:

- Conduct authentication of the requestor;
- Validate the reason for the request;
- Ensure sufficient information is available to uniquely identify the Certificate(s) which is/are the subject of the request.

Where reliable authentication of the suspension request is not possible or even omitted, EACP Revocation Service is authorised to conduct suspension after seeking confirmation of the request to the greatest extent possible. Processes may involve additional checking and information gathering to allow EACP Revocation Service to achieve a satisfactory level of assurance in the validity of the request.

Subscriber requested Certificate un-suspension shall only be undertaken as part of a process that requires the authentication of the Subscribers and verifies their identity and shall result in the unsuspension of all Certificates held by the Subscriber under this Certificate Policy.

4.9.15 Limits on suspension period

There is no limit on a period of suspension.

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status services shall be provided by CRLs, OCSP and SCVP. For OCSP, certificate status services shall be capable of verifying the validity of certificates in an automated and transparent fashion. This shall be maximised by leveraging the use of well-defined certificate extensions such as Authority Information Access (AIA) and CRL distribution point (CDP) extensions to automate the downloading of revocation information without the need for subscriber input.

4.10.2 Service availability

Validation services shall be available 24 hours a day and 7 days a week continuous. In addition, Validations services shall be implemented in such a way as to provide high availability delivery of certificate status information. This will require redundancy of implementation, including geographic and network diversity.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

EACP is dedicated to the European Aviation stakeholders including (ANSPs, Airports, Aircrafts, MIL, etc.). This domain is a dynamic environment with a significant degree of rotation of subscribers within its staff due to the nature of the different stakeholders. The procedures for ending a subscriber's relationship with EACP shall be based on the revoking its associated certificates.

EACP PMA may terminate any certificate subscription at its discretion at any time. This will result in certificate revocation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

See section 6.2 of this document for further information on key backup, key escrow and key archive provisions. The provision of recovered confidentiality keys to any person other than the certificate owner shall be governed by the data recovery policy of EACP CA. The data recovery policy shall be an integral part of EACP CA CPS and shall be approved by EACP PMA.

4.12.2 Session key encapsulation and recovery policy and practices

Not Supported.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The CA facility that will host EACP services shall at least be compliant with the site location requirement as set forth in [7], [8] and [11].

5.1.2 Physical access

The CA equipment including software, hardware, administration workstations and monitoring stations shall be protected from unauthorised physical access. The physical security requirements pertaining to EACP CA equipment include the following requirements:

- a clearly defined and protected perimeter through which all entry and exit are controlled;
- an entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;
- a site access log is maintained and inspected periodically for compliance with the CPS;
- resources not on the access list are properly escorted and supervised;
- at all times, unauthorised intrusion is manually or electronically monitored;

All RA sites shall be located in areas that satisfy at minimum the following controls:

- a clearly defined and protected perimeter through which all entry and exit are controlled;
- an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area;
- For all other individuals, provision shall be made for escorts or equivalent controls; to prevent unauthorised access to European Aviation classified information and uncontrolled entry to areas subject to technical security

5.1.3 Power and air conditioning

The CA facility shall ensure that the power and air conditioning facilities are sufficient to support the operation of EACP CA system.

5.1.4 Water exposures

The CA facility shall ensure that EACP equipment is protected from water exposure.

5.1.5 Fire prevention and protection

The CA facility shall ensure that EACP equipment is protected with a fire suppression system.

5.1.6 Media storage

The CA facility shall ensure that EACP equipment shall ensure that storage media used by EACP system is protected from physical access by unauthorised entities and environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste disposal

All media used for the storage of information such as keys, activation data or EACP CA files shall be de-classified or destroyed before released for disposal.

5.1.8 Off-site backup

AEACP shall ensure that facilities used for off-site back-up, have the same protection level as the main facilities for EACP site.

5.2 Procedural controls

5.2.1 Trusted roles

5.2.1.1 EACP CA Trusted Roles

EACP CA shall ensure a segregation of duties for critical EACP CA operations to prevent a single person from compromising, maliciously or unintentionally using or modifying a PKI or supporting system without detection.

Each resource ’s system access is to be limited to those actions for which he or she is required to perform in fulfilling his or her responsibilities. EACP shall assign distinct EACP resource roles, distinguishing between, critical operations such Key Ceremonies, day-to-day operation of EACP services, Registration operations, the management and audit of those operations and the management of substantial changes to requirements on the system including its policies, procedures or personnel.

The classification of responsibilities between the roles shall be defined in EACP Governance model and in EACP CPS. There are multiple classes of responsibilities possible. The choice of roles shall provide strong resistance to insider attack. Only those resources responsible for the duties outlined in the CPS shall have access to the software and hardware that controls EACP CA operation.

EACP CPS documents shall define EACP CA role required to implement the trusted roles.

5.2.1.2 RA Trusted Roles

EACP shall ensure that RA personnel understand their responsibility for the identification and authentication of prospective subscribers and perform the following functions:

- acceptance of subscription, certificate change, certificate revocation and key recovery requests;

- verification of an applicant’s identity and authorizations;
- transmission of applicant information to EACP;
- provision of authorization codes for on-line key exchange and certificate creation.

EACP may permit all duties for RA functions, with the exception of the review and management of audit data, to be performed by one individual.

EACP CPS documents shall define the RA roles required to implement this functionality.

5.2.2 Number of persons required per task

Multi-person control is required for all operations on CA keys. Multi-person controls shall be established for the performance of critical functions associated with the build and management of EACP systems, including the hardware configuration and software controlling CA Certificate generation operations. All other duties associated with EACP CA roles may be performed by one resource operating alone. EACP CA shall ensure that any verification process it employs provides for oversight of all activities performed by privileged EACP CA role holders.

RA tasks for high assurance level certificate shall require multi person controls.

RA tasks for low or medium assurance level certificate shall not require multi person controls.

5.2.3 Identification and authentication for each role

All EACP CA and RA personnel shall identify and authenticate themselves before being permitted to perform their duties. To that end, they shall be:

- included in the access list for the logical access to EACP CA or RA site;
- included in the access list for physical access to EACP CA system;
- if needed, to have a certificate for the performance of their EACP CA or RA role;
- if needed, to have an account on EACP system.

Each of these certificates and accounts (with the exception of EACP CA signing certificates) shall:

- be directly attributable to a resource;
- not to be shared;
- be restricted to actions authorised for that role through the use of EACP CA software, operating system and procedural controls.

5.2.4 Roles requiring separation of duties

Roles requiring separation of duties are Key Manager, Cryptographic Officer, Security Officer, Administrator, Operator, and Auditor as defined in EACP Governance Model [12].

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

EACP CA shall ensure that all resources performing duties with respect to the operation of EACP CA or RA shall be appointed, and their specific trusted role identified.

All resources filling trusted roles shall be selected on the basis of trustworthiness, integrity and loyalty, and shall be subject to background checks. Resources appointed to trusted roles shall:

- have received comprehensive training with respect to the duties they are to perform;
- be bound by contract and job description to the terms and conditions of the position they are to fill as defined by the position description;
- Be bound not to disclose sensitive security-relevant information or Subscriber information and maintain required protection of personal information;
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties; and
- not be assigned duties that may cause a conflict of interest with their EACP CA or RA duties.

EACP shall ensure that all resources performing duties with respect to the PKI operation shall hold a Security Clearance of a minimum equivalent to NATO SECRET clearance.

5.3.2 Background check procedures

All background checks shall be performed in accordance the relevant organisation’s internal procedures. The procedure shall be audited.

5.3.3 Training requirements

EACP shall ensure that all personnel performing duties with respect to the operation of EACP CA or RA shall receive comprehensive training in:

- EACP CA/RA security principles and mechanisms;
- all EACP software versions in use on EACP CA system;
- all EACP duties they are expected to perform;
- disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

Personnel operating EACP CA and RA shall be retrained when changes occur in EACP CA or RA systems. Examples of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, etc. Re-training shall be conducted as required, and EACP CA shall review re-training requirements at least once a year.

5.3.5 Job rotation frequency and sequence

EACP CA shall ensure that any change in the staff will not affect the effectiveness of the PKI services or security of the PKI system.

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorised action by a person performing duties with respect to the operation of EACP CA or RA, EACP shall be authorised to suspend his or her access to EACP CA system and initiate, if appropriate, disciplinary actions.

If the unauthorised actions concerns CA activities, EACP PMA shall perform an analysis to determine if CA certificate should be revoked.

5.3.7 Independent contractor requirements

Independent contractors holding Trusted Roles shall be subject to the same background, trustworthiness and competence check as other EACP resources. See section 5.3.1.

EACP Services shall ensure that contractor access to its facilities is in accordance with this Certificate Policy.

The actions of contracting staff are subject to the same audit arrangements and requirements as those of the resources providing Certification Services.

5.3.8 Documentation supplied to personnel

EACP CA shall make available to its EACP CA and RA personnel the Certificate policies it supports, its CPS, and any other specific PKI documentation, policies or contracts relevant to their position. Additionally, information providing the technical specifications or describing the operation of relevant hardware and software in use shall also be made available to the appropriate EACP CA and RA personnel to perform their duties.

5.4 Audit logging procedures

5.4.1 Types of events recorded

EACP CAs and RAs shall record in audit log files all events relating to the security of EACP CA system. These include as a minimum such events as:

- system start-up and shutdown;
- login and logoff attempts;
- attempts to create, remove, set passwords or change the system privileges of EACP privileged roles;
- CA services start-up and shutdown;
- unauthorised attempts at network access to EACP CA system;
- unauthorised attempts to access system files;

- changes to EACP CA configuration and/or keys;
- changes to certificate policies e.g., adding/changing an extension, changing validity period;
- generation of own and subordinate subscriber keys;
- creation and revocation of certificates;
- attempts to initialise remove, enable, and disable subscribers, and update and recover their keys;
- Delete or modify the audit file

All logs, whether electronic or manual, shall contain as a minimum the date and time of the event, and the identity of the entity which caused the event. EACP CA shall also collect and consolidate, either electronically or manually, security information not EACP CA-system generated such as:

- physical access logs;
- system configuration changes and maintenance;
- personnel changes;
- discrepancy and compromise reports;
- Records of the destruction of media containing key material, activation data, or personal subscriber information.
- Security relevant logs from the Directory
- Firewall and IDS Logs

All key ceremony records and information used to verify key ceremony attendee identity shall also be retained.

CA and RA audit information shall be collected and stored at EACP CA. To facilitate decision-making, all agreements and correspondence relating to EACP CA services shall be collected and consolidated, either electronically or manually, in a single location for EACP CA.

5.4.2 Frequency of processing log

EACP CAs and RAs shall ensure that their audit logs are reviewed by EACP CA (or RA) personnel as appropriate to the items being recorded and shall provide details of all significant events in an audit log summary. Reviewing the log shall verify as a minimum that the log has not been tampered with, and then briefly inspect all log entries. If any action is deemed suspicious, more thorough investigation of any alerts or irregularities in the logs should be possible. Actions taken following these reviews shall be documented. The CPS shall document the minimum requirements to be followed for the audit review.

5.4.3 Retention period for audit log

Audit logs shall be retained for a period of no less than 20 years (TBC) according to ECAP asset policy (TBD).

5.4.4 Protection of audit log

Any electronic audit log system shall include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information shall be protected from unauthorised viewing, modification and destruction.

5.4.5 Audit log backup procedures

Audit logs and audit summaries shall be backed up or if in manual form, shall be copied and stored in independent locations.

All backups shall be provided with the same level of security as the originals and shall be commensurate with the data contained within them.

5.4.6 Audit collection system (internal vs. external)

The audit log collection system shall cover all EACP components including the third-party products that makes the PKI system such as Database, Hardware Security Module, LDAP directory, etc.

Audit processes shall be invoked at EACP components start-up, and stop only at their shutdown. If an audit system is suspected to have failed, then an investigation shall start immediately to assess the risk associated with it and to decide if CA activities should be suspended until the problem is remedied.

5.4.7 Notification to event-causing subject

Where an event is logged by the audit collection system, no notice need be given to the individual, organisation, device or application that caused the event.

5.4.8 Vulnerability assessments

EACP PMA shall ensure that a security vulnerability assessment is performed at the beginning of the project or when significant changes to EACP are made.

5.5 Records archival

5.5.1 Types of records archived

EACP system (including the third party products) archive records shall be detailed enough to establish the validity of a signature and of the proper operation of EACP. At a minimum, the following data shall be archived.

- any contractual agreements to which EACP CA or RA is bound;
- CA and RA accreditation documentation;
- CPS documents for EACP CA and RAs;
- EACP system configuration;
- modifications or updates to any of the system configuration;
- certificate requests and revocation requests including bulk requests;
- subscriber identity authentication documentation as required by Section 3.2.3;
- subscriber agreements;
- documentation of receipt and acceptance of certificates as described in Section 4.4;
- documentation of receipt of tokens as described in Section 4.3.1;

- all certificates and CRLs (or other revocation information) as issued or published;
- security audit data (in accordance with Section 5.4);
- other data or software sufficient to verify archive contents
- all work related communications to or from EACP PMA, other EACP CAs or RAs, and compliance auditors.

5.5.2 Retention period for archive

The retention period for archive data shall depend on the legal and business requirements and is set forth in the respective CPS and be compliant with EACP backup and retention policy. However, the archive data must be kept for a minimum retention period of XXX years. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Software and hardware necessary to read and process the archives shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of archive

Archive media shall be stored in a separate, safe, secure storage facility with physical and procedural security controls equivalent or better than those for EACP components. The archive shall also be adequately protected from environmental threats such as humidity, temperature, radiation, and magnetism, etc.

Prior to archive, records shall be labelled with a clear distinguished name, the date, and the classification.

No unauthorised individual shall be able to view, modify or delete the archive. The archive can only be released if authorised by EACP PMA for EACP CAs and RAs, or if required by law.

Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognised agents. The request must be approved by EACP PMA.

5.5.4 Archive backup procedures

Archive backup shall be in place so that in the event of loss or destruction of the primary archives, a complete set of archive copies held in a separate location will be available. The CPS shall describe how archive records are backed up, and how their backups are managed.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Media storing EACP archive information shall be verified upon creation. Periodically, a statistical sample of archived information shall be tested to verify the continued integrity and readability of the information.

Requests for access to archived information for reasons other than audit review or system recovery shall meet the requirements of section 9.3 and 9.4. Procedures detailing how EACP CA or RA shall create package and send the archive information shall be published in EACP CA CPS. Only authorised EACP CA operators and EACP auditors shall be allowed to access the archive.

5.6 Key changeover

Key changeovers shall be initiated for one of EACP CAs or one of the system certificate (OCSP, SCVP, or timestamp keys) provided that their previous certificate(s) have not expired or been revoked.

Automated key changeover for CAs is not possible as any CA key changeover must be carried out during an official and witnessed key ceremony.

Automated key changeover for end entity system certificates (OCSP, SCVP, or timestamp) shall be permitted. The procedures, protocols, and data structures required to ensure that a CA key changeover and system certificate changeover shall be defined within the Key Management Policy and Procedures and in the CPS.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

EACP CA shall establish business continuity plan to protect its critical Public Key Infrastructure processes from the effect of incident or compromises, failures or disasters. These shall enable the recovery of all EACP services. Business continuity plans shall be detailed in the CPS and/or other supporting documentation.

The party responsible for providing EACP Services shall provide evidence that such plans have been exercised.

In the case of comprise of a CA or CA keys, EACP shall as a minimum require the following:

- Immediately suspend the validation services for all issued Certificates affected by a compromise, failure or disaster. This will stop any of these Certificates from being accepted by any Relying Party;
- Suspend any further Certificate Issuance from the affected CA.

EACP PMA shall make any decision relating to Revocation of CA Certificates.

EACP PMA shall notify the relevant parties of any breach of security or loss of integrity that has a significant impact on EACP Trust Service provided or on the personal data maintained therein.

5.7.2 Computing resources, software, and/or data are corrupted

Disaster recovery from the failure of computing resources can range from the provision of spares (e.g. cold standby) to the provision of fully redundant hardware with automated failover (e.g. hot standby or clustering). There are other solutions which fall between these two which require operator intervention as part of the process (e.g. warm standby).

Within EACP infrastructure, the most common failure modes to date have been shown to be network availability, database replication and general software malfunctions which required a restart of computing environments. Within these scenarios, the worst-case scenario occurs when the failure is detected as the CA attempts to generate an updated CRL file and propagate it toward the OCSP and SCVP servers. This scenario represents the worst-case scenario because it affects the validation services and per consequent the accuracy of certificate status.

EACP shall include mechanisms to detect the failure of the systems and network environments including CAs and critical repositories in a timely fashion such that the disaster recovery process is able to restore operations prior to further degradation of services.

EACP systems shall include mechanisms to notify the on-duty operator that a failure has occurred.

5.7.3 Entity private key compromise procedures

The Subscriber shall report any suspected or real compromise of their Private Key to their issuing CA or RA. The CPS shall detail the steps that a subscriber has to undertake in such situation.

5.7.4 Signature key compromise

In case of EACP subordinate CA compromise, EACP Root CA shall revoke that certificate and shall publish an ARL immediately to the repository. Subsequently, EACP CA installation shall be re-established as above.

If EACP CA is EACP Root CA, the recovery process shall include the removal of the trusted self-signed certificate from all relying party devices, and the secure out-of-band installation of the new EACP Root CA certificate.

In the event of the need for revocation of EACP CA’s Digital Signature certificate, EACP CA shall immediately notify:

- EACP PMA;
- In the case of EACP Root CA, external CAs to whom it has issued cross-certificates;
- all of its subordinate EACP CAs and RAs;
- all subscribers;
- all individuals or organisations that are using the Root CA certificate.

EACP CA shall notify all relying parties of the revocation by publishing an ARL.

EACP CA shall also:

- In the case of EACP Root CA, revoke all cross-certificates;

- For other EACP CA's, request the appropriate superior EACP CA to revoke the certificate and post an updated ARL;

After the resolution of the factors that led to revocation of the Digital Signature certificate and following authorisation by EACP PMA, aEACP shall:

- generate a new EACP CA signing key pair;
- re-issue certificates to all subscribers and ensure all CRLs and ARLs are signed using the new key.

In the case of EACP Root CA, the revoked certificate shall be removed from each relying party device, and the new self-signed certificate distributed via secure out-of band mechanisms as part of the recovery procedure.

5.7.5 Confidentiality key compromise

Where a subscriber suspects private key compromise, he or she shall immediately notify the issuing EACP CA or RA in a manner specified by the appropriate CPS. Where any relying party suspects private key compromise, the relying party shall immediately notify the related EACP CA.

Where the direct notification of compromise to the issuing EACP CA or RA is not possible within a timely fashion, the subscriber or relying party shall immediately notify their RA or security officer of the event. A list of acceptable entities for notification shall be included in the CPS, in the subscriber agreement and in the Relying Party Terms and Conditions.

In the event of the need for revocation of EACP CA’s certificate, the Certificate serial number shall be included on an appropriate ARL. The procedures for a trusted recovery from EACP CA certificate revocation shall be documented in its CPS.

5.7.6 Business continuity capabilities after a disaster

The business continuity plan for the TSP shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide the service. A separate alternative backup facility to maintain, at a minimum, certification and validation services shall be made available.

Any backup facility used for relocation following a disaster shall maintain compliance with this Certificate Policy. The provisions of this Certificate Policy shall be maintained during any relocation/transition procedures.

5.8 CA or RA termination

In the event of the termination of EACP CA or RA, the CA or RA shall take all the necessary measures to ensure that all the information, data, documents, repositories, archives and audit trails are preserved for the purpose of providing evidences if needed as set forth by this policy.

EACP PMA shall be responsible for the execution of the termination plan.

Before EACP terminates its services, the following procedures have to be completed as a minimum:

- Inform EASA and the different European Civil Aviation stakeholders of the termination and its possible consequences;
- Inform all Subscribers, cross-certifying CAs, Relying Parties and Subcontractors with which EACP has agreements or other form of established relations;
- Inform all relevant trusted personnel;
- Revoke the all issued and valid certificates and Publish the last CRL in associated directories;
- Where practicable, make publicly available details of termination arrangements at least 3 months prior to termination;

6. TECHNICAL SECURITY CONTROLS

EACP CA shall ensure its CA and RA operations provide appropriate security protection of the core PKI components (Hardware Security Module, PKI Hardware and Software) and the PKI operator's credentials. Where a PIN or password is recorded, it shall be stored in a security container accessible only to authorised personnel.

Subscribers shall be obliged by the Subscriber Agreement to not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains private keys on a hard drive shall be physically secured or protected with an appropriate access control product.

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA key pairs shall be generated during a witnessed key signing ceremony in a physically secured environment. All private keys used by EACP that affect the status of issued Certificates or Certificate status information shall be generated securely under controlled procedures. Detail of such procedures shall be detailed in the CPS and/or in supporting documentation (Key Management Policy and Procedures).

Subscriber keys for use with an SSCD shall be generated and stored on the device under control of the Registration Authority. It shall not be possible to export any Private Key from the device and the device shall be appropriately secured during preparation, storage and distribution.

Within EACP, all key pairs shall be generated using an EACP PMA approved algorithm. Key pairs associated to each certificate class shall be generated in conformance to its own policy identified by an Object Identifier.

EACP CA keys shall be generated during a formally witnessed key ceremony, and shall be hosted in Hardware Security Modules. Therefore there is no need for procedures to deliver CA keys.

6.1.2 Private key delivery to subscriber

If the key pair is generated by the subscriber, either in software or hardware cryptographic token, then there is no need to deliver Private keys, and this section does not apply.

If the key pair is not generated by the subscriber, then the private key and associated certificate shall be either delivered to the subscriber in an on-line transaction in accordance with RFC 5280 Certificate Management Protocol, or via an equally secure manner approved by EACP PMA. In all cases, the following requirement shall apply

- During the delivery period, the private key shall be protected from compromise or modification
- For the online transaction delivery of the private key, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

- For hardware cryptographic token, EACP CA or RA shall maintain accountability for the location and state of all cryptographic tokens
- The subscriber shall acknowledge receipt of the cryptographic token;
- in both cases, mechanisms shall be in place to prevent usage of the token prior to its delivery to the subscriber;

Public-key certificates shall be individually accountable. Under no circumstances shall anyone other than the subscriber have access to private signing keys.

For cases where there are several subscribers acting in one capacity, (private key and certificate shared by multiple subscribers), the sharing of private key material shall not be accomplished through the sharing of the cryptographic token. In this specific case,

- The Security Officer (SO) shall be responsible for ensuring control of the private key, including maintaining a list of subscribers who have access to use of the private key, and accounting for which subscriber had control of the key at what time.
- that list of those holding the shared private key shall be provided to, and retained by, EACP CA and RA;

6.1.3 Public key delivery to certificate issuer

Where the subscribers or the RA generates key pairs, public keys shall be delivered to EACP CA for the certification purpose, via an online and secure transaction, or via an equally secure manner approved by EACP PMA, using a standard recognised protocol. Proof of possession is achieved using the mechanism defined in section 3.2.1.

6.1.4 CA public key delivery to relying parties

EACP and the relying parties shall work together to ensure the authenticated and integral delivery of EACP Root CA certificate. Acceptable mechanisms for Root CA certificate delivery include but are not limited to:

- CAs or RAs loading EACP Root CA certificate onto tokens delivered to subscribers via secure mechanisms;
- secure distribution of EACP Root CA certificate through secure out-of-band mechanisms;
- comparison of certificate hashes or fingerprints against EACP Root CA certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- loading EACP Root CA certificate from web sites secured with a currently valid EACP certificate of equal assurance level than the certificate being downloaded.

Systems shall store EACP Root CA certificate such that unauthorised alteration or replacement is readily detectable and preventable (i.e. does not succeed in replacing the existing Root CA certificate).

EACP enabled applications shall protect EACP Root CA certificate at all times. Applications conforming to EACP Policy shall store EACP Root CA certificate within the hardware token or in a software cryptographic module, or other protected certificate store. In all cases, the integrity of EACP Root CA certificate shall be maintained at all times.

6.1.5 Key sizes

The following asymmetric algorithms and key lengths in Table 2 shall be supported by the European Aviation EACP.

External parties unable to support the algorithms within this table will be unable to interoperate with EACP.

Symmetric key size	ECC key size	RSA/DSA key size	Protection to year
112	224	2048	2030
128	256	3072	2040
192	384	7680	2080
256	512	15360	2120

Table 4: Key size

6.1.6 Public key parameters generation and quality checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto algorithm in which the parameters are to be used; as such:

- ECDSA and ECDH keys shall be generated in accordance with FIPS 186-3. Curves from FIPS 186-3 shall be used.
- RSA keys shall be generated in accordance with FIPS 186-3 (except for certificates at the Basic or lower Assurance Levels). Public key parameters for use with the RSA algorithm shall be generated and checked in accordance with PKCS #1 see [16].

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The use of a specific key is determined by the key usage extension and, if applicable, the extended key usage extension in the X.509 Certificate. The Certificate Profiles in section 10 specify the allowable values for this extension for different types of Certificates issued by the European Aviation EACP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

EACP CA and RA cryptographic modules shall be certified compliant with the requirements of the FIPS PUB 140-2 level 3 or higher. Subscriber cryptographic modules shall be certified compliant with the requirements of the FIPS PUB 140-2 level 3, or validated, certified, or verified to requirements published by EACP PMA.

6.2.2 Private key (n out of m) multi-person control

EACP CA private keys shall be protected using a key protection mechanism implementing the m out of n scheme, i.e. CA private keys are protected by a set of hardware tokens. Each set consists of a number tokens, n, of which a smaller number, m, is required to authorize an action (create or restore a key in the Hardware Security Module). The required number m is known as the quorum.

End entity certificate private keys shall not implement the m/n scheme. In case end entity private keys shall be used by multi person, then the policy 6.1.2 described in this document shall applies.

6.2.3 Private key escrow

Private keys associated with encryption certificates shall be escrowed by EACP in support to data recovery of information encrypted by EACP applications. Recovery of escrowed encryption keys shall require the presence of 2 persons.

Key recovery shall be done at the request of subscriber who shall first be authenticated by EACP. The acceptable methods for authentication shall be defined in EACPCA CPS and the authentication information of the subscriber shall be recorded and archived by EACP.

CA private keys shall not be escrowed.

6.2.4 Private key backup

6.2.5 Backup of CA private Keys

The CA private keys shall be backed up under the same security controls as used to generate and protect the original CA private keys. At least three CA backups will be generated, the first backup shall be hosted in the primary site, the second backup shall be hosted in the secondary site, and the third one in a third backup location.

Procedures for backing up CA private keys shall be described EACP CPS and/or in supporting documentation.

6.2.6 Backup of Subscriber Private Key

Subscriber private keys whose corresponding public key is contained in a Certificate asserting the medium of high assurance level may be backed up or copied but must be held in the Subscriber’s control. The backup method must ensure the same security controls as the ones used during the creation of the original keys.

Subscriber private keys whose corresponding public key is contained in a Certificate asserting a low assurance level should not be backed up or copied.

6.2.7 Private key archival

Escrowed key material shall be retained for retention period as set forth by EACP Backup Policy after the expiry of the key material.

6.2.8 Private key transfer into or from a cryptographic module

Any CA Private Key transfer shall be done such that the Private Key is protected cryptographically in accordance with FIPS140-2 level 3, its equivalents and successors.

Subscriber keys are generated and stored on the Subscriber cryptographic device and are never transferred to or exported from their keystore.

6.2.9 Private key storage on cryptographic module

All cryptographic modules approved for use within EACP shall provide an adequate level of protection for the storage of the private key, commensurate with the certificate associated assurance level.

6.2.10 Method of activating private key

The subscriber shall be authenticated to the cryptographic module before the activation of the private key. The minimum authentication mechanism shall be in the form of a pin or password. Stronger authentication mechanisms may be required such as multifactor authentication (MFA) principles commensurate with the operational environment.

Repeated authentication failures shall invoke a security response mechanism. The number of incorrect authentication attempts shall be configurable and defined in EACP CPS but in no case shall be higher than 10 attempts.

6.2.11 Method of deactivating private key

When the cryptographic module is deactivated all cryptographic keys shall be cleared from general purpose memory before the memory is de-allocated. Any disk space where keys were stored shall be over-written before the space is released to the operating system.

When deactivated, private keys shall be protected by the hardware token from unauthorised access.

6.2.12 Method of destroying private key

Private keys shall be destroyed when they are no longer needed.

For the routine re-key of hardware tokens (i.e. the token remains in the possession of the same subscriber) the overwriting of the old private key with the new private key meets the requirement of this policy without zeroizing the hardware cryptographic token.

When all of a subscriber’s keys are no longer required (or are expired or revoked), the hardware cryptographic module shall be zeroized by the subscriber and the token returned to EACP CA or RA, as identified in the subscriber agreement. The authority receiving the returned token from the subscriber shall immediately verify that the token has been zeroized by the subscriber.

The physical destruction of hardware should not be required to zeroize non-personalised cryptographic modules.

For software cryptographic modules, destroying private key can be done by overwriting the data.

6.2.13 Cryptographic Module Rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

EACP CA shall archive public key certificates based on the requirements of 5.5, as part of the certificate archival.

6.3.2 Certificate operational periods and key pair usage periods

Table 3 summarises the maximum validity period of EACP CA's certificate, and the maximum lifetime of the associated key (used for certificate signature), separated by a slash (i.e. Signing Life Years/Verification Life Years).

	Algorithm	Hashing Algorithm	Key Size	Private Key	Certificate
Entity Root CAs	ECC/ RSA	SHA-512	521/4096	20 years	20 years
Entity Sub CAs	ECC/ RSA	SHA-384/SHA-256	521/4096	10 years	13 years
End Entity	ECC/ RSA	SHA-256	256/2048	3 years	≤ 3 years

Table 5: Key pairs and associated Certificates usage Period

6.4 Activation data

6.4.1 Activation data generation and installation

Any activation data creation shall be unique and unpredictable. The activation data, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected, and shall meet the applicable security policy requirements of the crypto module used to store the keys.

6.4.2 Subscriber Cryptographic Module Activation Data

Where pin or passwords are used, a subscriber shall have the capability to change them at any time.

As a minimum, cryptographic module activation codes shall be 10 characters in length. One time initialisation data shall be 14 characters in length as a minimum. The selected length for activation data, its complexity, and maximum lifespan shall be defined in EACP CPS and in the Password Policy.

6.4.3 Activation Data for Initial Keying of Cryptographic Module

One time activation data required for initial keying/certifying of the cryptographic module shall be managed by EACP or RA and distributed securely (e.g. out of band) to the subscriber. These mechanisms shall be documented in EACP and RA CPS.

6.4.4 Activation data protection

Data used for subscriber initialisation and activation shall be protected from unauthorised use by a combination of cryptographic and physical access control mechanisms. The level of protection shall be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism shall include a facility to temporarily lock the account after a predetermined number of login attempts.

6.4.5 Other aspects of activation data

Subscribers and Sponsors shall not share, write down or otherwise store copies of EACP cryptographic module activation codes.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Each EACP CA servers and RA workstations shall include, as a minimum, the following functionality as applicable:

- identification and authentication of EACP roles and associated identities;
- access control to EACPCA/RA services and EACP roles;
- enforced separation of duties for EACP roles;
- use of cryptography for session communication and database security;
- archival of EACPCA/RA and subscriber history and audit data;
- audit of security related events;
- self-test of security related EACP CA/RA services (check integrity of audit logs);
- trusted path for identification of EACP roles and associated identities;
- recovery mechanisms for keys and EACPCA/RA system;

- Boundary protection device protecting EACP element from the general purpose network.

This functionality may be provided by the operating system, or through a combination of operating system, EACPCA/RA software, and physical safeguards.

Software which provides additional security functionality to EACP such as IDS and Antivirus software should be considered as long as the additional software does not interfere with the evaluated configuration of EACP product. Any software which interferes with the evaluate configuration or does not increase security functionality to EACP shall not be installed on EACPCA or RA systems.

6.5.2 Computer security rating

No stipulation

6.6 Life cycle technical controls

6.6.1 System development controls

Equipment (hardware and software) procured to operate EACP shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with. The selected equipment for EACP infrastructure shall be developed in a controlled environment and the system development controls for EACP software and hardware are as follows:

- Software shall be designed and developed under a formal, documented development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with.
- Hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not parts of the PKI operation.
- Actions shall be taken to prevent malicious software from being loaded onto the PKI equipment. Applications required to perform the PKI operations shall be obtained from trusted sources.
- PKI hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed and be installed by trusted and trained personnel in a formal, documented change procedure.
- The design and development process shall be supported by third party verification of process

compliance and ongoing Risk Assessments to influence security safeguard design and minimise residual risk.

6.6.2 Security management controls

The configuration of EACP system, as well as any modifications and upgrades, shall be documented and implemented in a controlled way. EACP shall not have installed applications or software components, which are not part of EACP configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of EACP systems. There shall be a mechanism for detecting unauthorised modifications to EACP system software or configuration.

A formal configuration management methodology shall be used for installation and ongoing maintenance of EACP system. EACP software, when first loaded, shall implement a mechanism for EACP to verify that the software on the system:

- originated from the software developer;
- has not been modified prior to installation; and
- is the version intended for use.

EACP shall provide a mechanism to periodically verify the integrity of the software. EACP shall also have mechanisms and policies in place to control and monitor the configuration of EACP system. Upon installation, the integrity of EACP system shall be validated.

6.6.3 Life cycle security controls

Equipment updates shall be purchased or developed in the same manner as original equipment and be installed by trusted and trained personnel in a defined manner.

6.7 Network security controls

EACP Root CA equipment shall in an offline way configuration. The Root CA certificates and associated CRL shall be transported manually to EACP repositories.

The online EACP servers shall be protected from attack through any open or general-purpose network with which they connected. Such protection shall be provided to prevent EACP from Intrusion attacks or against denial of services. As a minimum through the installation of a boundary protection device configured to allow only the protocols and commands required for the operation of EACP services.

6.8 Time-stamping

Where implemented, a secure time-stamping service shall meet the same system security and availability requirements as the CA. Specifically, the time-stamping service shall have the same redundancy and system security requirements as a CA. The hardware cryptographic module for the OCSP responder shall meet the standards as defined for the CA hardware cryptographic module.

7. Certificate, CARL / CRL, And OCSP profiles Format

7.1 CERTIFICATE PROFILE

7.1.1 Version

The version field indicates the X.509 version of the certificate format.

EACP certificates shall be compliant with version 3 of the rfc 5280 [2], allowing for certificate extensions.

7.1.2 Serial Number

The field serial number specifies the unique, numerical identifier of the certificate within all public-key certificates issued by the same CA.

EACP CA shall assign a unique serial number to every EACP certificate.

7.1.3 Signature

The signature field determines the cryptographic algorithm used by EACP CA to sign a certificate. The algorithm identifier, which is a number registered with an internationally recognized standards organization, specifies both the public-key algorithm and the hashing algorithm used by the CA to sign certificates.

The signature algorithm used by EACP CAs to sign EACP certificates shall be:

ecdsa-with-Sha256 = {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsawith-Specified(3) ecdsa-with-Sha256 (2)}

RSA with SHA2 (256)= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.

7.1.4 Issuer

The Issuer field identifies the certification authority that has signed and issued the certificate. Issuer is structured as a “Distinguished Name”, that is a hierarchically structured name, composed of attributes, most of which are standardised in the X.500 attributes.

The Distinguished Name associated with EACP Root CA is made of the following attribute:

CN=European Aviation Root CA, OU=EACP, O=EUROCONTROL

CN=European Aviation Safety Critical CA, OU=EACP, O=EUROCONTROL

CN=European Aviation Administrator CA, OU=EACP, O=EUROCONTROL

7.1.5 Validity

The validity field indicates the time interval during which EACP certificates are valid, and over which the issuing CA maintains certificate status information.

The validity period should be interpreted as the period when, before and after which the certificate should not be trusted.

The validity period is expressed in two fields: not before and not after.

- Not before: expresses the date on which the certificate validity period begins, and
- Not after: expresses the date on which the certificate validity period ends.

The validity period of EACP Root CA certificate shall be 30 years.

The validity period of EACP subordinate CA certificates shall be 20 years.

The validity period of EACP end entity certificates shall be 1, 2 or 3 years depending on certificate classes.

7.1.6 Subject

The Subject field identifies the subject holding the private key corresponding to the public key published in the certificate. Subject is structured as a set of attributes, defined in the X.500 attributes, with the attribute type as further described in RFC3280.

The subject of EACP certificates shall be as follows:

CN= Subject or Device common name, OU=EACP, O=EUROCONTROL

7.1.7 Subject Public Key Info

The Subject Public Key Info field is used to carry the public key being certified and identify the algorithms with which the key has been generated.

7.2 Certificate Extensions

CA and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

Details of the extensions will be given once the use cases task has been completed.

7.2.1 Key usage

The Key Usage extension field specifies the purpose of the key contained in the certificate.

The possible key purposes identified by the X.509v3 standard are the following:

a) digital signature,

b) non-repudiation,

c) key encipherment,

d) data encipherment,

e) key agreement,

f) key certificate signing,

g) CRL signing,

h) encipher only,

i) decipher only.

In all EACP CA certificates, the following flags are asserted:

- Key certificate signing
- CRL signing

7.2.2 Basic constraints

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-user. If the subject may act as a CA, it may also specify the maximum acceptable length of valid certification path that includes this certificate. This extension should always be marked as critical; otherwise some implementations will ignore it and allow a non-CA certificate to be used as a CA certificate.

In all EACP certificates:

For Root CA: the Subject Type value is set to “CA”, with a Path Length constraint of “None”, and this extension shall be marked critical.

For Subordinate CA: the Subject Type value is set to “CA”, with a Path Length constraint of “0”, and this extension shall be marked critical.

For End entity certificate: the Subject Type value is set to “End Entity”, with a Path Length constraint of “-”, and this extension shall NOT marked critical.

7.2.3 CRL Distribution Point

The CRL Distribution Points extension identifies the CRL distribution point or points to which a certificate user should refer to ascertain if the certificate has been revoked. A certificate user can obtain a CRL from an applicable distribution point or it may be able to obtain a current complete CRL from the authority directory entry.

The status of EACP certificates can be obtained from an http location identified by the following URLs:

- For Root CA

<u>The Root CA Certificate location</u>:

URL=http://repository. common-pki.eacp.int /root-ca.crt

The Root CRL location:

URL=http://repository.common-pki.eacp.int/root-ca.crl

URI=ldap://ldap.common-pki.eacp.int/cn=EuropeanAviationRoot CA,ou=EACP,o=EUROCONTROL?certificateRevocationList?base

- For Subordinate CA:

The Safety Critical CA certificate location:

URL=http://repository.common-pki.eacp.int/safetycritical-ca.crt

The Safety Critical CRL location:

URL=http://repository.common-pki.eacp.int/safetycritical-ca.crl

URI=ldap://ldap.common-pki.eacp.int/cn=EuropeanAviationSafetyCritical CA,ou=EACP,o=EUROCONTROL?certificateRevocationList?base

In URL=http://repository.common-pki.eacp.int/admin-ca.crl

URI=ldap://ldap.common-pki.eacp.int/cn=EuropeanAviationAdministrator CA,ou=EACP,o=EUROCONTROL?certificateRevocationList?base

7.2.4 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

- sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- ecdsa-with-Sha256: {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsawith-Specified(3) ecdsa-with-Sha256 (2)}
- ecdsa-with-Sha384: iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}
- ecdsa-with-Sha512: {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-Sha512(4)}

Certificates under this CP use the following OIDs for identifying the algorithm for which the subject key shall be generated:

- id-ecc256-Key: {iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) prime256v1(7)}
- secp384r1: {iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}
- RsaEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
- Dhpublicnumber: {iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
- id-keyExchangeAlgorithm: {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

7.2.5 Name Forms

The subject and issuer fields of the base certificate shall be populated with a unique X.500 Distinguished Name, with the attribute types as further constrained by RFC 5280. DNs shall be encoded as printable strings if possible. If that is not possible, the only acceptable alternative is UTF8. In all cases the CA DN and name space for name constraints shall be encoded as a printable string.

7.2.6 Name Constraints

Principal CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in Section 10 subject to the requirements above. The Issuer CA may obscure an End Entity Subject name to meet local privacy regulations as long as such name is unique and traceable to a corresponding unobscured name. Issuer names may not be obscured. Issuer CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.2.7 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to each certificate is set forth in Section 1.2. The Certificate Policies extension in each certificate is populated in accordance with Section 1.2.

7.2.8 Usage of Policy Constraints Extension

EACP CAs shall adhere to the Certificate Formats described in this CP.

7.2.9 Policy Qualifiers Syntax & Semantics

Certificates issued under this CP shall not contain policy qualifiers

7.2.10 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used by the CA conforms to X.509 certification path processing rules.

7.3 CRL PROFILE

7.3.1 Version Numbers

EACP CAs shall issue version 2 CRLs.

7.3.2 CRL and CRL Entry Extensions

The CRL and CRL entry extensions comply with the CRL profile specified in [2].

7.4 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 6960.

7.4.1 Version Number

The version number for request and responses shall be v1.

7.4.2 OCSP Extensions

The ExtendedKeyUsage extension of the OCSP certificate shall have the OCSP flag asserted.

Responses shall support the nonce extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

All EACP CAs, Pursuant to EACP Certificate Policy, shall demonstrates to the satisfaction of EACP PMA that they fully comply with the requirements of this policy prior to initial generation of EACP hierarchy of certificates. The online EACP CAs shall be inspected at least once every 2 years. The offline EACP Root CA shall be inspected at least once every 5 years.

EACP shall certify bi-annually to EACP PMA that they have at all times during the period in question complied with the requirements of this policy.

EACP CA shall also provide to EACP PMA reasons for which EACP has not complied with its Certificate Policy and state any periods of non-compliance.

The inspection body shall hold the applicable Security Clearance of at least or equivalent to NATO secret.

EACP PMA shall certify to any external PMA with whom it interoperates (cross-certification, Bridge Certification or Certificate Trust List (CTL)) that it fully complies with the requirements of EACP Certificate Policy and shall receive a similar certification from the external PMA that the external PKI complies with EACP Certificate Policy. The above reciprocal certifications shall be provided prior to initial interoperability with EACP, and on a schedule agreed upon in the cross-certification agreement. The compatibility of Certificate Policies shall be addressed as part of the cross-certification agreement and is subject to approval by both EACP PMA and the external PMA.

8.2 Identity/qualifications of assessor

Any person or organisation undertaking a compliance inspection shall possess significant experience with PKI and cryptographic technologies as well as the operation of relevant EACP software and hardware. EACP PMA is responsible for ensuring that the compliance inspection is performed by an appropriate person or organisation.

The inspector or the organisation that will carry out assessments must be independent from the contractor operating EACP or EACP members and must be formally accredited or recognized for the applicable scheme. In particular. The inspector conducting ETSI audits must be accredited against ISO/IEC 17065 and ETSI EN 319 403 for audits against ETSI EN 319 411 standards series;

8.3 Assessor's relationship to assessed entity

The inspector shall be independent from the contractor operating EACP or EACP members and their affiliated companies, as well as sub-contractors operating for them.

8.4 Topics covered by assessment

The compliance inspection shall follow the inspection guidelines instituted by EACP PMA. This shall include as a minimum whether EACP implements and complies with the technical, procedural and personnel policies and practices defined in EACP CP and CPS.

8.5 Actions taken as a result of deficiency

If irregularities are found, inspectors shall submit a report to EACP PMA as to any action EACP will take in response to the inspection report. EACP PMA shall make a choice to;

- acknowledge the irregularities, but allow EACP to continue operations until the next programmed inspection;
- allow EACP to continue operations for a maximum of thirty days pending correction of any problems prior to revocation;
- or revoke EACP CA's certificate.

The inspection results for external PKI systems, with whom EACP has interoperated, shall be submitted to EACP PMA. Where the PMA of an interoperated PKI fails to take appropriate action to correct irregularities, EACP PMA may revoke the external PKI’s cross-certificate with EACP. Any decision regarding which of these actions to take will be based on the severity of the irregularities.

8.6 Communication of results

The inspection results of EACP shall be provided to EACP PMA. External PKIs that has interoperated with EACP shall provide EACP PMA with a copy of the results of the compliance inspection. EACP PMA shall provide EACP compliance audit results to the external PMA of interoperated PKIs if required by the Interoperability Agreement. These results shall not be made public. The method and detail of notification of inspection results to CAs that are interoperable with EACP shall be defined within the Interoperability Agreement between the two parties.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

EACP certificates are chargeable. EACP shall charge the subscribers depending on the certificate classes or the PKI services provided.

9.1.2 Certificate access fees

EACP shall decide on any fees related to EACP services.

There shall be no fees for Relying Parties accessing EACP certificates.

9.1.3 Revocation or status information access fees

EACP shall decide on any fees related to EACP OCSP and SCVP based validation services.

9.1.4 Fees for other services

EACP shall decide on any fees for other EACP services.

9.1.5 Refund policy

No Stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

EACP shall maintain reasonable levels of insurance coverage as required by Aviation regulations.

9.2.2 Other assets

EACP shall maintain sufficient financial resources to maintain and sustain the PKI services.

9.2.3 Insurance or warranty coverage for end-entities

No Stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

By nature, information contained in a digital certificate is public and is deemed not private. In addition, CRL files, OCSP request and responses, SCVP request and responses and other information's published in EACP directories are not considered private or confidential.

Other business information which does not appear in the items cited above and that are used in connection with this CP shall be classified and shall not be disclosed.

As a minimum the following information shall be protected:

- All applications made by potential subscribers (whether accepted or not)
- Personal information supplied during registration
- Private keys
- Records relating to the management of certificates
- PKI documentations (System and Network design, Specifications, Key Management Policy and Procedures, Key ceremony scripts, etc.)
- Audit data, records and reports
- Contingency planning, disaster recovery plans and security measures.

9.3.2 Information not within the scope of confidential information

The following information shall not be regarded as confidential, and shall not therefore contain any confidential information

- Certificates
- CRLs
- This certificate policy, the associated CPS and set of policy agreements.

9.3.3 Responsibility to protect confidential information

All EACP participants shall have a duty to protect business information in their possession, custody, or control.

Business information shall be classified and labelled. Business information that is labelled as confidential shall be treated with the same degree of care and security as the CA treats its own most confidential information.

Any request for the disclosure of confidential information shall be made in writing, signed and delivered to EACP PMA.

9.4 Privacy of personal information

9.4.1 Privacy plan

Certificates and CRLs published in public directories shall not contain sensitive personal subscriber information or classified information.

Sensitive personal subscriber information shall not be disclosed without the prior consent of the subscriber, unless required by applicable laws and regulations.

EACP shall commit to process the registration data and any other personal data shared in a lawful, fair and transparent manner and in observance with the principles set out by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data regulation (also called 'GDPR' see [16]) and for EUROCONTROL in the EUROCONTROL Regulation on Personal Data Protection and its Implementing Rules..

Inspection information shall be appropriately classified and shall not be disclosed to anyone for any purpose other than inspection and system security purposes.

Subscribers must be given access and the ability to correct or modify their personal or organisation information upon appropriate request to EACP Issuing CA.

9.4.2 Information treated as private

Information required to establish the binding between the user and the certificate is collected as part of the certification process. Information beyond the items defined in 9.4.3 below shall be treated as private unless it is identified within the CA CPS and deemed not private by EACP PMA.

9.4.3 Information not deemed private

Certificates will contain personal information which is relevant and necessary to implement secure transactions using the certificate. Such information may include the following information concerning the subscriber;

- Subscriber name
- Subscriber organisation
- Subscriber e-mail address

This information, while personal in nature is not deemed to be private.

9.4.4 Responsibility to protect private information

Information pertaining to EACP CA's management of a subscriber's certificate may only be disclosed to the subscriber. Any requests for the disclosure of information shall be signed and delivered to EACP and approved by EACP PMA.

9.4.5 Notice and consent to use private information

Private information collected for the purposes of establishing a binding between a user and their certificate shall only be used for the purpose of establishing this binding, and for the audit of this activity. Acceptance of a certificate from EACP shall be deemed to be consent for the use of this private information by EACP.

9.4.6 Disclosure pursuant to judicial or administrative process

Information pertaining to EACP's management of a subscriber's certificate may only be disclosed to the subscriber. Any requests for the disclosure of information shall be signed and delivered to EACP.

9.4.7 Other information disclosure circumstances

No Stipulation

9.5 Intellectual property rights

EACP shall maintain ownership rights of any PKI services it is running unless otherwise it has explicitly transferred or released to a third party.

In the case of interoperability using cross certification, bridge or CTL, key pair and certified certificate shall be the property of the certified party.

9.6 Representations and warranties

9.6.1 CA representations and warranties

An Issuing EACP shall ensure that its PKI services and repository are in accordance with this Certificate Policy. EACP shall also ensure that all RAs and subscribers follow the requirements of this policy when dealing with any of EACP services. EACP CAs and RAs shall ensure that their authentication and validation procedures are implemented as set forth in this policy.

9.6.2 RA representations and warranties

When an RA submits subscriber information to EACP, it shall certify that it has authenticated the identity of that subscriber in accordance with EACP Certificate Policy. Acceptance and delivery of a signed certificate request to EACP CA for the signature purpose constitutes notice of such verification.

RA personnel shall inform subscribers about all relevant information pertaining to the rights and obligations of EACP CA, RA and subscriber. This information is contained in EACP Certificate Policy, the subscriber agreement, and any other relevant document outlining the terms and conditions of use.

Records of all actions carried out in performance of RA duties shall identify the individual who performed the particular duty.

RA personnel shall be individually accountable for actions performed on behalf of EACP CAs. Within this policy, individually accountable requires that there shall be evidence that attributes an action to the person performing the action.

9.6.3 Subscriber representations and warranties

Any information required to be submitted to EACP PMA, EACP CA, or RA in connection with a certificate shall be complete and accurate. It is the responsibility of subscribers to verify the completeness and accuracy of the submitted information prior to completing the key management process (registration, rekey, or revocation.)

Any error or misrepresentation of information discovered after the completion of the key management process is basis for the revocation of all EACP subscriber's certificates.

9.6.4 Relying party representations and warranties

The rights and obligations of a relying party who is relying on a certificate managed by EACP are covered in this policy. The rights and obligations of a relying party belonging to another PKI shall be addressed in the cross-certification agreement or Memorandum of Agreement between the two PKIs.

9.6.5 Representations and warranties of other participants

No Stipulation

9.7 Disclaimers of warranties

European Aviation EACP assumes no liability whatsoever in relation to the use of EACP certificates or associated public/private key pairs for any use other than in accordance with EACP Certificate Policy.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No Stipulation.

9.10 Term and termination

9.10.1 Term

This CP becomes effective once it is approved by EACP PMA and is published in the appropriate directory.

Amendments of this CP shall become effective upon acceptance and execution by EACP PMA. This certificate policy shall remain effective until it is superseded by EACP PMA, or until the end of the archive period for the last expired or revoked certificate which asserts a policy OID from this certificate policy.

9.10.2 Termination

This CP may only be terminated or withdrawn by EACP PMA. All entities and PKI stakeholders shall be notified 6 (six) months prior to the effective termination of this CP.

9.10.3 Effect of termination and survival

Once terminated, no further certificates may be issued under this certificate policy. The provisions of sections 9.3, 9.4, 9.5, 9.8, and 9.9 of this CP and any related agreements shall survive termination of this certificate policy.

9.11 Individual notices and communications with participants

No Stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

Written and signed comments on proposed changes to EACP Certificate Policy shall be directed to EACP PMA. Decisions with respect to the proposed changes are at the sole discretion of EACP PMA.

Prior to publishing any changes to this Certificate Policy, EACP PMA shall notify EACP CAs, and all external CAs that are directly cross-certified with EACP CA.

Following approval by EACP PMA, public notification of amendments shall be made.

9.12.2 Notification mechanism and period

All changes to this Certificate Policy are subject to the notification requirement. However, spelling errors or typographical corrections which do not change the meaning of the Certificate Policy shall be allowed without notification.

EACP PMA shall notify, in writing, all CAs that are directly cross-certified with EACP of any proposed changes to this Certificate Policy. The notification shall contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. EACP subscribers may also be notified by the proposed changes. EACP PMA shall also post a notice of the proposal on EACP PMA Web site.

The review/comment period shall be 30 days unless otherwise specified. The comment period shall be defined in the notification.

9.12.3 Circumstances under which OID must be changed

If an amendment is determined by EACP PMA to warrant the issuance of a new policy, EACP PMA may assign a new Object Identifier (OID) for the amended or the new policy.

9.13 Dispute resolution provisions

A dispute related to key and certificate management, and PKI services within EACP shall be resolved pursuant to provisions in the applicable agreements between parties.

A dispute related to key and certificate management, and PKI services related to an external CA or a cross-certified CA shall be resolved using an appropriate dispute settlement mechanism in accordance with the dispute resolution procedures documented within the cross-certification agreement.

9.14 Governing law

EACP CA shall ensure that any agreements by that EACP CA shall be governed by the rules and regulations of European Aviation Agency concerning the enforceability, interpretation and validity of this Certificate Policy.

9.15 Compliance with applicable law

The Relationships between EACP and its PKI Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. Dispute between a PKI Participants and EACP is dealt with under Belgian laws, with the exception of the rules applicable to data protection where the obligations of the Parties shall be determined in accordance with the laws applicable to each Party.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No Stipulation

9.16.2 Assignment

EACP and the European Aviation stakeholders implementing this certificate policy reserve the right to assign this certificate policy, in whole or in part, to another European Aviation stakeholder, or representative European Aviation members. In such a case, EACP shall notify EACP PMA accordingly in writing. EACP shall remain responsible for its obligations under this certificate policy and for the actions of the new stakeholder or its representative to which this certificate policy may be assigned.

9.16.3 Severability

If any provision of this Certificate Policy, including limitation of liability clauses, is found to be invalid or unenforceable, the other provisions shall remain in effect until the CP is updated. The process for updating EACP CP is described in section 9.12.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation

9.16.5 Force Majeure

EACP PMA and EACP shall not be held liable for a termination of the Agreement for default if the failure to perform to the terms of the Agreement arises out of causes beyond the control and without the fault or negligence of EACP and EACP PMA. Such causes may include, but are not restricted to, acts of God, or act of civil or military authority, acts of the public enemy, acts of the subscriber in its contractual capacity, acts of sovereign governments that was not reasonably anticipated, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the failure to perform must be beyond the control and without the fault or negligence of EACP and EACP PMA.

9.16.6 Other provisions

No Stipulation.

10. References

1. RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework

2. RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List Profile.

3. RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

4. RFC 5055: Server-Based Certificate Validation Protocol - SCVP

5. RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.

6. RFC 4210: Internet X.509 Public Key Infrastructure - Certificate Management Protocol (CMP)

7. ETSI TS 102 042 V1.1.1 (2002-04): Electronic Signatures and Infrastructures (ESI) - Policy requirements for certification authorities issuing public key certificates

8. ETSI TS 101 456 v1.4.3 (2007-05): Electronic Signatures and Infrastructures (ESI) - Policy requirements for certification authorities issuing qualified certificates

9. ETSI EN 319 412-2 V2.2.1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

10. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

11. Trust Service Principles and Criteria for Certification Authorities – Version 2.

12. European Aviation – EACP Governance Model

13. RFC 8017: PKCS #1: RSA Cryptography Specifications - Version 2.2

14. RFC 2986: PKCS #10: Certification Request Syntax Specification - Version 1.7

15. GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

16. PKCS #1 v2.2: RSA Cryptography Standard: October 2012. Republished as RFC 8017

17. EACP Criteria and Methodology for Interoperability