Digital Tachograph

CPA Andorra

Certificate Policy

Version 1.00

May 16th 2022

Document versions history

Version	Author	Comments
1.00	Roman ZAICH Pascal MERLIN	Creation

Case followed by

Sylvain TRIQUET

Date of Approved Document:

Table of Contents

I. Introduction

I.1. Overall Presentation

Preliminary remark :
Please refer to subsection I.6 for terms and acronyms definition

I.1.1. Purpose of the document

This document forms the Certificate Policy of the Andorran Authority (named AND-CPA) which is integrated into the Public Key Infrastructure (PKI) of the european Smart Tachography System and which also covers symmetric master keys management. The Root Certification Authority and the symmetric master keys management is under the responsability of the ERCA (European Root Certification Authority).

This Certificate Policy (CP) is based on the ERCA Certificate Policy [6]. It describes the requirements that the Andorran Contracting Party Certification Autority (names AND-CPCA) is committed to respect in the execution of its digital signature and master keys distribution services to the other participants. Parties involved in the management of the life cycle of certificates, cards and applications of the Andorran Tachograph System shall also comply with the requirements described in this Certificate Policy.

I.1.2. Regulatory Context

The first-generation Tachograph system, called Digital Tachograph, has been introduced by Regulation (EU) No 3821/85 [1] of the European Parliament and of the Council.

The European Agreement concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR) (2] has been signed by 51 countries in Europe and Asia, with the aim of reducing obstacles to the international carriage of goods and passengers by road by harmonising the rules on driving and rest times, including the technical specifications of the tachograph. This multilateral agreement was drawn up under the aegis of the United Nations Economic Commission for Europe (UNECE).
In 2006, the EU introduced the digital tachograph as mandatory equipment for the control of driving times and rest periods as a replacement for the analogue tachograph used since 1985. Subsequently, the Contracting Parties to the AETR agreed to introduce from 2011 the same digital tachograph in their vehicles used in international transport. On that occasion, they agreed to insert into the AETR Agreement (2] a new Article 22a, which provides that tachograph specifications, although defined unilaterally by the EU without prior consultation of non-EU Contracting Parties when amending Annex 1B to Regulation (UE) No 3821/85 [1], are automatically applied by extension to all Contracting Parties.

In order for Andorra, contracting to the European Agreement (AETR), to benefit from ERCA's certification and master key distribution services, the present Policy covers the requirements defined by ERCA in the exclusive context of the first generation of the so-called Digital Tachograph. It therefore refers in particular to the various requirements of Appendice 1B (adaptation to the AETR agreement of the Annex 1B of the Regulation (EU) No 3821/85) of the European Agreement (AETR).

I.1.3. Public Key Infrastructure

A Public Key Infrastructure (PKI) has been designed to support the public-key cryptographic systems, while the symmetric cryptographic system relies on master keys that must be delivered to the relevant actors.
This infrastructure is composed of three hierarchical levels :

- Root Certification Authority (European Level)
- Sub-Certification Authority (Member State and/or Contracting Party Level)
- End Entities owner of equipement certificates (Member State and/or Contracting PartyLevel)

The European Root Certification Authority (ERCA) is responsible for the generation and management of root key-pairs (public-private keys) with associated certificates and of symmetric master keys. The ERCA issues certificates and distributes symmetric keys to Member State and/or Contracting Party Certification Authorities. MSCAs/CPCAs are responsible for issuing Digital Tachograph Equipment Certificates, as well as distributing symmetric master keys and other data derived from the master keys to be embedded in Digital Tachograph equipment.

I.1.4. Document Structure

This document follows the structure described in ETSI TS 319 411-1 [3] which sets out the general requirements of the international community for trusted electronic transactions.

It also follows the framework for Certificate Policy described in RFC 3647 [4]. The Policy on the Management of Symmetric Master Keys has been added to this document, while preserving the summary of RFC 3647 [5].
The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119 [5].

I.2. Document Name and Identification

This document is named « Digital Tachograph – CPA Andorra Certification Policy – v_1_00 ».
The curent version is 1.00
This Certificate Policy does not have an ASN.1 object identifier. The certificates issued by the Andorran CPCA (AND-CPCA) do not indeed contain a reference to this policy.

I.3. Participants

The architecture of the "Digital Tachograph" PKI is composed of an European Root Authority and of a sub-authority in each different Member State (MSCA) and/or Contracting Party (CPCA).
This hierarchy allows to create a chain of trust for the certificates issued by these MSCAs/CPCAs as well as for the master symmetric keys that are distributed by the ERCA.
In this context, at the Member State or Contracting Party level, different roles have been defined that can be split into one or more separate entities:

- Member State and/or Contracting Party Authority (MCA/CPA)
- Member State and/or Contracting Party Certification Authority (MSCA/CPCA)
- Card Issuing Cards
- Card Personalizer

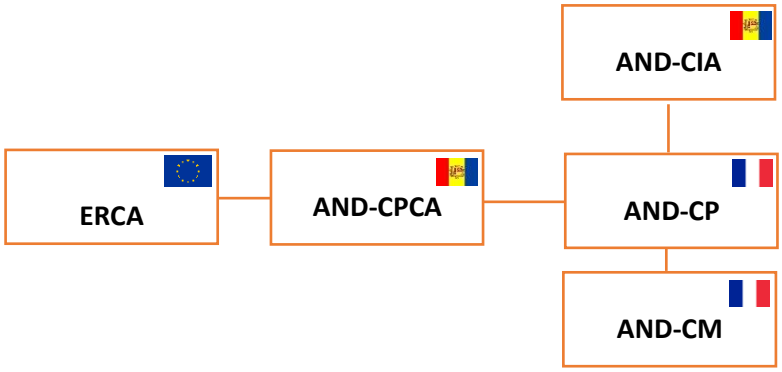
- Equipment Manufacturer (cards, VU and MoS)
- Equipment Users (tachograph cards, VU and Motion Sensor)

NB : VU and MoS manufacturers insert in these equipments derivated keys from symmetric master keys and use therefore, as such, the services of the CPCA.

In the specific Andorran context, the Digital Tachograph Participants (ERCA not included) are the following entities:

- The Andorran Contracting Party Authority (AND-CPA)
- The Andorran Contracting Party sub-Certification Authority (AND-CPCA)
- The Andorran Card Issuing Authority (AND-CIA)
- The Andorran Card Personalizer (AND-CP)
- The Andorran Manufacturer (AND-CM)
- Equipment Users

NB: only "card" type devices are concerned by this version of the PC. VU type equipment and related items do not fall within the scope of this version. No VU or MoS manufacturer is registered on the Andorran territory.



Schema 1: Relation between the different entities involved in the Andorran perimeter

The PKI of the AND-CPCA is operated by IN Groupe entity, itself designated MSCA for France. IN Groupe ensures therefore the role of Certification Operator (CO) on behalf of the AND-CPCA.

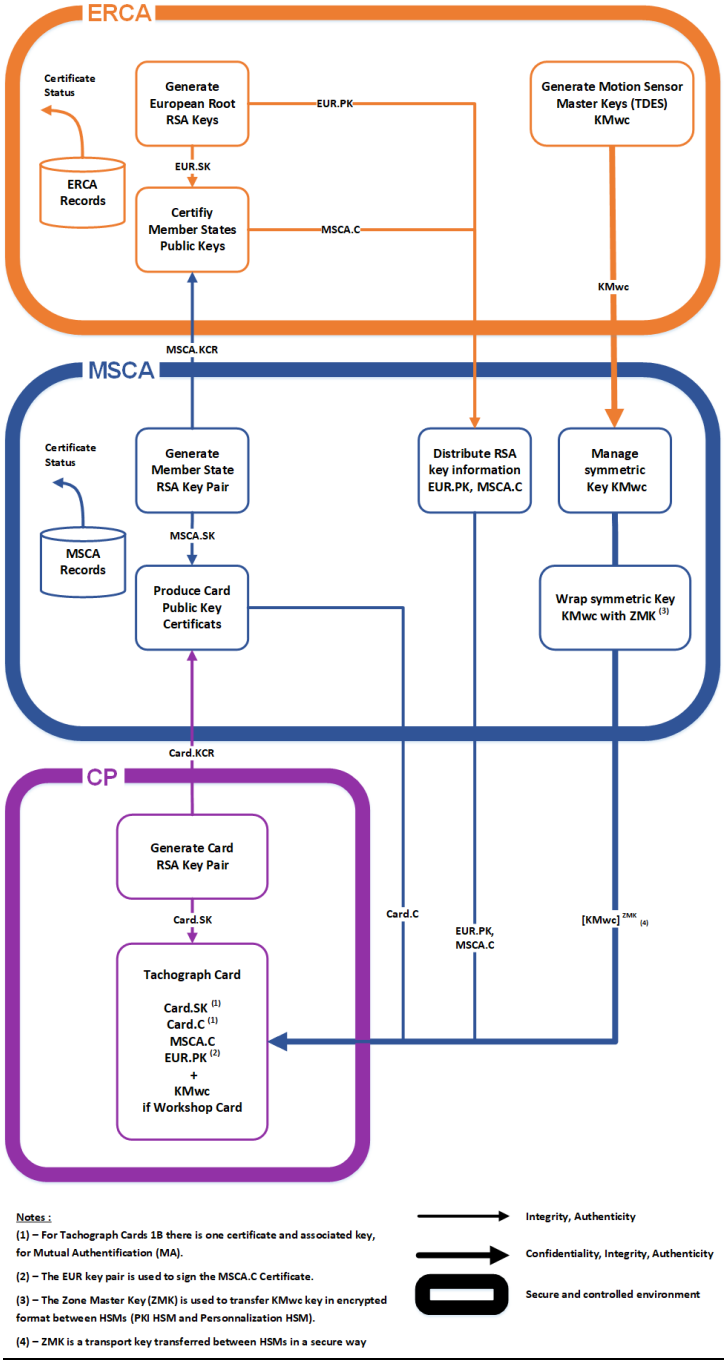
Note :

In the remainder of the document, unless otherwise indicated, operations related to the exploitation of the PKI of the AND-CPCA are implicitly performed by the IN-Groupe entity. However, when the AND-CPCA is mentioned and the CO is concerned, an indication is added in parentheses to clarify the involvement or responsibility of the CO.

AND-CPA also relies on the services of the F-CM and F-CP respectively for the manufacture and personalization of tachograph cards. The F-CM and F-CP are the manufacturer and the personalizer designated by the CPA France (F-CPA) in the context of the French tachograph system. However, for consistency purposes in the notation, this manufacturer and this personalizer are designated by the acronyms

AND-CM and **AND**-CP to specify the **AND**orran context of the tachograph system.

The following diagram shows the main participants (ERCA, AND-CPCA and AND-CP) in the specific Andorran context as well as the different exchanges that exist between them. This is the original ERCA scheme that has been adapted to the specific context of Andorra.



Schema 2: workflow inside Andorran PKI

I.3.1. Certification Authority

European Root Certification Authority (ERCA)

General context

The ERCA is the root Authority of the Digital Tachograph (Generation 1) and of the Smart Tachograph (Generation 2) systems PKI.
The ERCA generates the root key pairs and the corresponding public key certificates, as well as link certificates (exclusively for Generation 2) to create a chain of trust between the different root certificates generated.
It certifies the public keys of the Authorities of the different Member States (MSCA) and/or Contracting Parties (CPCA).

Andorran context (Digital Tachograph)

The ERCA provides the following services within the Smart Tachograph system PKI: registration service, certificate generation and dissemination service.
The ERCA also provides the following services within the Smart Tachograph System:
generation, management and distribution of symmetric master keys

In the context of Generation 1 of the tachograph system (Digital Tachograph), there are only two master keys: the Motion Sensor master key – VU part (KM-VU), the Motion Sensor master key – Workshop Card part (KM-WC).

NB: only "card" type equipment is concerned by this version of the PC. VU-type equipment and related elements do not fall within the scope of this version. No actor (VU manufacturer) is registered on Andorran territory. The AND-CPCA is therefore only concerned by the "Card" part.

Andorran Contracting Party Certification Authority (AND-CPCA)

The AND-CPCA operates the Certification Authority subordinate to the Root CA under the responsibility of the Andorran Contracting Party Authority (AND-CPA).
The AND-CPCA is responsible for the Certification Authority subordinate to the Root CA (ERCA) on behalf of the Andorran Contracting Party Authority (AND-CPA).
The AND-CPCA certifies the public keys of the equipments. As a reminder, the scope of the equipment concerned in the context of Andorra is restricted to tachograph cards. Consequently, only the CPCA_Card certificate request is submitted to the ERCA. The private key associated with this certificate allows the AND-CPCA to certify the public keys of the tachograph cards.

The AND-CPCA can also submit to the ERCA a request for symmetric master keys $K_{M\text{-}WC}$ for tranmission to the Card Personalizer (AND-CP) on its own request.

The AND-CPCA only manages the certificates and symmetric keys respectively issued by and received from the ERCA. As a reminder, only first-generation Digital Tachograph system is supported by the AND-CPCA. This means that keys and certificates conforming to the specifications of the first-generation Digital Tachograph system are present in the PKI system of the AND-CPCA. These certificates and keys are referenced in Appendix 1B [2].

List of keys and certificates of the first-generation Digital Tachograph stored in the AND-CPCA PKI system:

- ERCA certificate (*ERCA.C*);
- CPCA_Card key pair (*CPCA_Card.PK* and *CPCA_Card.SK*);
- CPCA_Card certificate (*CPCA_Card.C*);
- $K_{M\text{-}WC}$ master key.

Exchange of symmetric keys between the ERCA and the AND-CPCA is carried out in a secure manner (encrypted with the RSA transport public key generated and transmitted by the AND-CPCA).

I.3.2. Certification Operator

The Certification Authority is operated by the IN Group entity, which therefore provides a "Certification Operator" service to the AND-CPCA.
This entity implements on behalf of the AND-CPCA an operational platform, functional, secure, in compliance with the requirements set out in this Certification Policy (CP) and the terms of which are detailed in the AND-CPCA Certification Practice Statement (CPS) whose writing is under its responsibility. This platform is implemented for:

- The management of the signature private keys of the AND-CPCA
- Management and dissemination of tachograph equipment certificates
- The management of symmetric master keys
- The distribution of its keys to tachograph equipment

I.3.3. Registration Authorities

A chain is set up as part of the registration and the validation of the certificate requests and the master keys distribution requests transmitted to the AND-CPCA.

AND-CP registration by the AND-CPCA
The AND-CP is designated by the AND-CPA. The AND-CPCA ensures that the Card Personaliser (AND-CP) is formally registered before processing the requests it issues. Information on the registration process is provided in the the AND-CPCA Certificate Practice Statement.
Authentication requirements are described in the « Identification and Authentication » section (see chapter III)

AND-CIA registration by the AND-CP
The AND-CIA is designated by the AND-CPA.
The Card Personalizer (AND-CP) ensures that the Card Issuer (AND-CIA) is formally registered before processing card personalization requests.
Authentication requirements are described in the section Identification and authentication (see chapter III).

Card applicants registration by the AND-CIA
Processing of certificate applications is delegated by the AND-CPCA to the Card Issuer (AND-CIA). The latter thus act as the Delegated Registration Authority (DRA) with the AND-CPCA in the context of the control and the processing of card applications that it receives from applicants. In particular, the AND-CIA is responsible of the identification of the applicant.

I.3.4. Tachograph Card Personalizer (AND-CP)

This is the organization that personalizes tachograph cards with cardholder identification data, keys and certificates.
The AND-CP (personalization system) transmits its requests for signing public keys to the AND-CPCA. The card personalization system is authenticated by the AND-CPCA in order to request a certificate. Authentication requirements are described in the section Identification and authentication (see chapter III).
The AND-CPCA also transmits the symmetric master key to the AND-CP which integrates it into the personalized cards.

I.3.5. Card Issuer (M-CIA)

The Role of the AND-CIA (Andorra) consits in:

- verifying whether all required documents were produced by card applicants and whether these documents are valid; In particular, the AND-CIA is responsible, when processing the applications, of the verification of:
    - the applicant identity (control of the ID card, passport, etc.)
    - the right of the applicant to request a card (for instance control of the validity of the driving licence for a driver card application)
- verifying whether all prerequisites for the issuing of a tachograph card subject to the AETR agreement [2] (in particular Appendix 1B), all other relevant legal provisions, the ERCA Certification Policy [6] and this AND-CPA Certificate Policy are fulfilled;
- verifying whether a tachograph card under validity was not already issued to the applicant in another EU-Member State or in another Contracting Party (non EU-Member); (via TACHOnet network)
- ensuring that the applications data is transmitted to the Card Personalizer (AND-CP) properly according to the produced documents and to the requirements of this policy;
- informing all users about the requirements of this policy in an appropriate manner;
- ensuring that the PIN code of the workshop card is handed over only to the intended bearer of the workshop card, ordered by the workshop in his name;
- immediately informing the AND-CPA and the AND-CPCA or one of its authorized agencies about all security-relevant incidents.

I.3.6. Applicants of certificates and master keys

Applicants to the ERCA
The AND-CPCA is acting as an applicant with ERCA. It can request signing its public keys as well as the distribution of the master keys of the Digital Tachograph system.

Applicants to the AND-CPCA
The only applicant for certificates and master keys to the AND-CPCA is the Card Personalizer (AND-CP). its requests are subsequent to the card personalization requests it receives from the Card Issuer (AND-CIA). The certificates and master keys transmitted by the AND-CPCA are inserted in the cards that the AND-CP personalizes on behalf of the Card Issuer (AND-CIA).

The Card Personalizer (AND-CP) is responsible of the personalization of driver cards, workshop cards, company cards and control cards.
For personalization of driver cardscompa and workshop cards, it ensures:

- generation of one key pair for mutual authentication;
- processing of the application to the AND-CPCA of public keys certification (with CPCA_Card certificate);
- processing of the application of K_{M-WC} master key (workshop cards only);
- availability of keys and certificates in the cards for mutual authentication and signature and MoS-VU pairing;

For personalization of company cards and control cards, it ensures:

- generation of the key pair for mutual authentication;
- processing of the application to the AND-CPCA of public key certification (with CPCA_Card certificate);
- availability of keys and certificates in the cards for mutual authentication and signature.

I.3.7. Other participants

In addition to the Card Personalizer (AND-CP) and the Card Issuer (AND-CIA), the other participants who rely on the AND-CPCA certification service are the drivers, the companies, the workshops and the controlers who use the certificates of the AND-CPCA to verify the equipement certificates, which in turn are used to verify the authenticity of the data downloaded from vehicle units and driver cards.

I.4. Keys and certificates usage

The root certificates of the ERCA are used to verify the certificates it issues to the AND-CPCA (CPCA_Card.C certificates). The ERCA certificate is the last link in the chain of certification. It is included, with the CPCA_Card.C certificates of the AND-CPCA, in cards issued by the Card Personalizer (AND-CP).

The AND-CPA and all PKI Participants (see chapter I.3) trust the ERCA certificates, provided they are published by the ERCA according to the requirements of the chapter II of this document.
The AND-CPCA uses the private key of the French Member State Authority (AND-CPA) only for:

- Signing the « cards » equipment certificates in compliance to Appendice 1B [2]
- Signing the Key Certification Request (KCR)

.
The master key (K_{M-WC}) is communicated by the AND-CPCA to the Card Personalizer (AND-CP) by appropriated secure means for the sole purpose for which the key is intended.

The K_{M-WC} master key is provided to the Card Personalizer (AND-CP) for installation in the workshop cards. K_{M-WC} is used by the VU with the K_{M-VU} key to generate the KM key while pairing the VU with the motion sensor.

The *CPCA_Card.C* Certificate is used to verify the cards certificates signed with the private key (*CPCA_Card.SK*) corresponding to the *CPCA_Card.C* certificate.
Card_MA.C certificates are used for mutual authentication and session key exchange between the VU and the card.

I.5. Certificate Policy administration

The main processes supported by this Certificate Policy are:

- The generation and the management of *CPCA_Card* keys (*CPCA_Card.PK* and *CPCA_Card.SK*) and certificates (CPCA_Card.C) of the AND-CPCA,
- The management and the dissemination of card keys and card certificates,
- Management and dissemination of $K_{M\text{-}WC}$ keys.

I.5.1. ERCA

The European Commission service responsible for implementing the Certificate Policy at the European level and for providing key certification and key distribution services to the Member States and the Contracting Parties is referred to hereinafter as the European Root Certification Authority (ERCA).

The contact address of the ERCA is :

Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Center (TP 580)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

This Certificate Policy has been written in French and translated into English. It has made available to the ERCA. The ERCA has reviewed this Policy to ensure compliance with the requirements of its own Certificate Policy. ERCA has archived the review report and the AND-CPA Certificate Policy for reference.
The AND-CPA is committed to answering to any comments made by ERCA and to making any updates to its Certificate Policy at the request of the ERCA in order to provide a level of security equivalent to the other Contracting Parties one.

Based on the guarantee of compliance of this document with the ERCA CP [6], the ERCA provides the AND-CPCA with the certification service and the distribution service for symmetric master keys. The provision of these services over time is subject to the periodic submission of audit reports (see Chapter VIII.1) demonstrating that the AND-CPCA continues to meet its obligations as defined in this ERCA approved Certiicate Policy.

I.5.2. Andorran Contracting Party Authority (AND-CPA)

The Contracting Party Authority for Andorra (AND-CPA), is responsible for the establishment and documentation of the Certificate Policy covered by this document. This Certificate Policy complies with the requirements applicable to CPCAs and described in the ERCA Certificate Policy [6].

After its approval by ERCA, this AND-CPA Certificate Policy is made available to :

- all relying parties, including in particular the AND-CPCA and the Card Personalizer (AND-CP) as well as the Card Issuer (AND-CIA),
- the Certification Operator (CO).

The contact address of the AND-CPA is:

Àrea de Transport Terrestre, Aeri i per Cable
Departament d'Empresa, Comerç, Desenvolupament, Seguretat i Qualitat Industrial, i Transport
Ministeri de Presidència, Economia i Empresa
Govern d'Andorra
Carrer Prat del Rull, 7, 3a planta
Edifici Prat del Rull
AD500 Andorra la Vella
Principat d'Andorra
Tel.: + 376 875 700

I.5.3. Contracting Party Certification Authority (AND-CPCA)

The AND-CPA has designated the entity that will implement this national Certificate Policy and provide the certification service and master keys distribution service to the Card Personalizer (AND-CP). This is the AND-CPCA which has itself designated the entity which will provide the Certification Operator services.
The Certification Operator (CO) describes its implementation of the AND-CPA Certificate Policy in the "Certification Practice Statement" (CPS) document. This CPS document identifies the practices (organization, operational procedures, technical and human resources) that the Certification Operator (CO) applies in providing its electronic certification service and master keys distribution service to the Card Personalizer (AND-CP) on behalf of the AND-CPCA and in accordance with the certificate policy(ies) to which it has committed itself. This CPS is therfore written by the Certification Operator (CO). Its distribution is restricted because it contains confidential technical and organizational information. The CO makes available the content of its Certification Practice Statement only on a need-to-know basis (see II.2.2).

The CO Certification Practice Statement is managed, reviewed and amended in accordance with the document control procedures.
The Certification Practice Statement is provided to the AND-CPA. It is the responsibility of the AND-CPA to ensure compliance of the Certification Practice Statement with the Certification Policy it has set itself.
The AND-CPCA maintains records of its operations as appropriate to demonstrate conformity with the AND-CPA Certificate Policy and shall make these records available to the AND-CPA and/or the ERCA on demand.

Upon request, AND-CPCA can provide ERCA with a version of the CO Certification Practice Statement. Documents referenced in the Certification Practice Statement giving information classified as "confidential" about procedures, technical means, etc. are not provided with the Certification Practice Statement.

The contact address of the AND-CPCA is :

Àrea de Transport Terrestre, Aeri i per Cable
Departament d'Empresa, Comerç, Desenvolupament, Seguretat i Qualitat Industrial, i Transport
Ministeri de Presidència, Economia i Empresa
Govern d'Andorra
Carrer Prat del Rull, 7, 3a planta
Edifici Prat del Rull
AD500 Andorra la Vella
Principat d'Andorra
Tel.: + 376 875 700

The contact address of the Certification Operator (CO) is:

IN Groupe
Direction des Programmes Tachygraphe
Rue des Frères Beaumont
59128 Flers-en-Escrebieux
FRANCE
Tél : +33 327937070

I.5.4. Card Personalizer (AND-CP)

The AND-CPA has also designated the Card Personalizer (AND-CP), which is the entity that will personalize the cards when requested by the Card Issuer (AND-CIA). The AND-CP is responsible of the cards key pair generation and of the public key certification request to the AND-CPCA. It has also the responsibility of securing the master keys transmitted by the AND-CPCA in order to be written to the cards.

The contact address of the AND-CP is:

IN Groupe
Direction des Programmes Tachygraphe
Rue des Frères Beaumont
59128 Flers-en-Escrebieux
FRANCE
Tél : +33 327937070

I.6. Definitions and acronyms

Acronyme	Définition
AES	Algorithm Encryption Standard
CA	Certification Authority
CIA	Card Issuing Authority
CO	Certification Operator
CP	Card Personalizer (NB: not used in this document, only Andorran CP refered as AND-CP is used)
CP	Certificate Policy
CPS	Certification Practice Statement
DRA	Delegated Registration Authority
EA	European Authority
EC	European Commission
EA	European Authority
EAL	Evaluation Assurance Level
AND-CIA	Andorran Card Issuing Authority
AND-CP	Andorran Card Personalizer
AND-CPA	Andorran Member State Authority

AND-CPCA	Andorran Member State Certification Authority
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ISMS	Information Security Management System
JRC	Joint Research Centre
KCR	Key Certification Request
KDR	Key Distribution Request
KDM	Key Distribution Message
KM	Motion Sensor Master Key
$K_{M\text{-}VU}$	VU (Vehicle Unit) part of KM (TDES Key)
$K_{M\text{-}WC}$	WC (Workshop Card) part of KM (TDES Key)
KID	Motion Sensor Key Identifier
KP	Motion Sensor Key Pairing
MA	Mutual Authentication
MoS	Motion Sensor
MSCA	Member State Certification Authority
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
TDES	Symmetric Algorithm Triple DES (Data Encryption Standard) [15]
VU	Vehicle Unit
ZMK	Zone Master Key (Key for secured key transfer between HSMs)
WC	Workshop Card
ENT.PK	Public Key of entity « *ENT* » e.g. Card_MA.PK is the public key of the card used for mutual authentication
ENT.SK	Private key of entity « *ENT* » e.g. CPCA_Card.SK is the private key of the AND-CPCA used for signing the cards certificates
ENT.C	Certificate of entity « *ENT* » e.g. EUR.C is the certificate of the ERCA

Table 1 – Definitions Acronyms

II. Publication and repository responsabilities

II.1. Repository

Equipment certificates issued by the AND-CPCA are recorded in the data base of the Certification Authority. No certificates repositoty is made public by the AND-CPCA.

II.2. Publication of Certification Practice Statement

II.2.1. Publication of Certificate Policy

This Certificate Policy is published by the AND-CPA on the Transport Andorra website at the following address:

https://www.transports.ad/ca/targetes-de-tacograf,

Certificates of the AND-CPCA (*CPCA_Card.C*) may be published by the ERCA (after issuance) and are accessible from a public server.

II.2.2. Publication of Certification Practice Statement (CPS)

The Certification Practice Statement is writen by the Certification Operator. The CPS shall be approved by the AND-CPA.
The Certification Practice Statement is not a public document but may be made available to the relying parties upon request (only on a need-to-know basis). In particular, the AND-CPA can ask the AND-CPCA to provide it with the CO CPS to ensure of its compliance against the CP it has itself writen.

II.3. Frequency of publication

Information relating to changes to this Certificate Policy shall be published in accordance with the schedule defined by the amendment procedures described in Chapter IX.12 of this document.
Similarly, information relating to changes to the OC Certification Practice Statement will be published according to the schedules defined by the amendment procedures as set out in the Certification Practice Statement.

III. Identification and authentication

This chapter describes the procedures in place to control the identity and/or attributes of applicants prior to issuing or renewing certificates or distributing symmetric master keys. In the context of AND-CPCA, these procedures cover the identification and authentication of the card personalization system.
The Card Personalizer (AND-CP) shall, for its part, identify and authenticate all card production orders before requesting the AND-CPCA the issuance of a card certificate.

III.1. Naming

III.1.1. Types of name

Certificate Issuer and Subject

The Certification Authority Reference and the Certificate Holder Reference identify respectively the issuer and the subject of a certificate. They shall conform to the format described in Appendix 1B Sub-appendix 11 [2] (CSM_017).

Key Distribution Request and Key Distribution Message

Key Distribution Requests and Key Distribution Messages contain a Key Identifier consisting in part of the number and name of the Contracting Party and the type of master key respectively requested by the AND-CPCA in the KDR and transmitted by the ERCA in the KDM.

III.1.2. Requirement of explicit names usage

N/A

III.1.3. Anonymisation and pseudonymisation

Certificates issued within the scope of the AND-CPCA do not contain any anonymous or pseudonymous identities.

III.1.4. Rules for interpreting the various types of name

No interprepation is made on the name of the certificates.

III.1.5. Uniqueness of names

All the names of certificate and all key certification requests (KCRs) shall be unique.

III.1.6. Identification, authentication and role of registred trademarks

N/A

III.2. Initial identity validation

III.2.1. Method to prove possession of the private key

Certificate Request from AND-CPCA to ERCA

When submitting key certification requests (KCR), the AND-CPCA proves the ownership of the corresponding private key through an internal signature generated with this private key(as described in the ERCA PC, Annex A [6]). This signature is verified by the ERCA.
Further proof of integrity, authenticity and trust must be provided by checking the hash calculated over the KCR transmitted by the AND-CPA, upon receipt by the ERCA (as described in the ERCA PC [6]).

Certificate Request from Card Personalizer to AND-CPCA

When submitting key certification request (KCR), the Card Personalizer (AND-CP) proves the ownership of the corresponding private key by an internal signature generated with this private key. The AND-CPCA verifies the signature before issuing the certificate.

III.2.2. Validation of entity's identity

All requests for certificate issuance should only be processed when received from a formally authenticated entity. The AND-CPCA therefore authenticates the Card Personalizer (AND-CP). The Card Personalization System can then send card certificate issuance requests.
Mutual authentication shall be performed by the AND-CPCA PKI when processing requests issued by the card personalization system. The AND-CPCA PKI rejects all requests if the mutual authentication has failed.

III.2.3. Validation of requester's authority

In the context of the AND-CPA, the Card Personalization System is expected to identify and authenticate other parties using the AND-CPCA. The Card Personalizer verifies the authenticity of their identity and applies all the prerequisites to be recognized as a trusted entity by the AND-CPCA.

III.2.4. Unverified requester's informatIons

Unverified information from an applicant is rejected by the Certification Authority (AND-CPCA) and cannot therefore be included in the certificates.

III.2.5. Validation of requester's authority

The CPCAs shall define a procedure for the validation of the applicant's authority. In the context of AND-CPCA, this procedure shall be referenced in its Certification Practice Statement.

III.2.6. Criteria for interoperability

The AND-CPCA shall not rely on any external certification authority, with the exception of the ERCA for the certificate signing and key distribution services it provides to the Digital Tachograph system.
If the AND-CPCA must rely on an external PKI for any other service or function, it shall review and approve

the Certificate Policy and/or Certification Practice statement of this external certification service provider before relying on its services.

III.3. Identification and Authentication for re-key request

III.3.1. I&A for re-key request, AND-CPCA

The identification and authentication of a key renewal application for the AND-CPCA shall respect the ERCA Certificate Policy [6]

III.3.2. I&A for re-key request, Card Personalizer (AND-CP)

The renewal of the key of the equipment (cards) is not considered within the scope of the Digital Tachograph system. This means that for a given card it is not possible to replace the key pair and the associated certificate.

III.4. Identification and Authentication for revocation request

Certificate revocation lists are not managed by the AND-CPCA.

IV. Life-Cycle Operational Requirements for Certificates and Master Keys

This chapter describes message formats, cryptographic mechanisms and procedures for the processing and distribution of certificates and symmetric keys for cards, and equipment data encryption services between AND-CPCA and the Card Personalizer (AND-CP), as well as for the processing and distribution of AND-CPCA Certificates (*CPCA_Card.C*) and master keys between the ERCA and the AND-CPCA.

IV.1. Certificates application and issuance

IV.1.1. Certificate Request (Key Certification Request)

Key Certification Requests issued to the ERCA by the AND-CPCA

Key Certification Requests (KCRs) can only be submitted by the AND-CPCA if it has been appointed by the AND-CPA as CPCA to the ERCA. The European Authority is responsible for the recognition of the AND-CPA.

KCR issued by the AND-CPCA shall comply with the following format:

Field	Bytes	Explanation
Certificate Content	164	See below
Signature of Certificate Content	128	See below

Table 2 – Format of the KCR issued by the AND-CPCA

Field	Format	Bytes	Explanation
CPI	Integer	1	Certificate Profile Identifier '01'
CAR	Octet String	8	Certification Authority Reference
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC web-site) 'FD' (253) = European Community
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website) '45 43 20' = "EC "
keySerialNumber	Integer	1	'00'
additionalInfo	Octet String	2	'FF FF' Production Certificate '54 4B' Test Certificate
caIdentifier	Octet String	1	'01'
CHA	Octet String	7	Certificate Holder Authorization
tachographApplicationID	Octet String	6	'FF 54 41 43 48 4F'
equipmentType	Integer	1	'00'
EOV	TimeReal	4	Certificate End Of Validity 'FF' padded if not used.
CHR	Octet String	8	Certificate Holder Reference
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC web-site) '03' = Andorra
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website) '41 4E 44'= "AND"
keySerialNumber	Integer	1	Unique serial number
additionalInfo	Octet String	2	'FF FF' Production Certificate '54 4B' Test Certificate
caIdentifier	Octet String	1	'01'
Public Key			
n	Octet String	128	Public Key modulus
e	Octet String	8	Public Key public exponent

Table 2.a – Format of *Certificate Content*

Public key modulus submitted to the ERCA (via a KCR) shall be unique in the domain of the AND-CPCA.
The KCR is signed with the private key (*CPCA_Card.SK*) associated to the public key (*CPCA_Card.PK*) submitted by the AND-CPCA to ERCA. The signature of the Certificate Content is the primitive signature RSASP1 (PKCS#1) [14]with the card private key (*Card.SK*).

Field	Bytes	Explanation
Fixed value	1	'4B'
Fixed value	58	58 x 'BB'
Fixed value	1	'BA'
Hash	20	SHA-1(CC)
Hash	20	SHA-1(SHA-1(CC))
Fixed value	1	'BC'

Table 2.b – Format of *Signature of Certificate Content*

Key Certification Requests issued to the AND-CPCA by the Card Personalizer

The AND-CPCA issues certificates only if an appropriate request is submitted to the responsible authority and if all the requirements of AETR agreement [2] and all other legal provisions and associated agreements have been fulfilled at the time of application.

Field	Bytes	Explanation
Certificate Content	164	See below
Signature of Certificate Content	128	See below

Table 3 – Format of the KCR issued by the Card Personalizer

Field	Format	Bytes	Explanation
CPI	Integer	1	Certificate Profile Identifier '01'
CAR	Octet String	8	Certification Authority Reference
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC website) '03' = Andorra
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website) '41 4E 44' = "AND"
keySerialNumber	Integer	1	Serial number to distinguish the different keys of the Certification Authority in the case keys are changed.
additionalInfo	Octet String	2	'FF FF' Production Certificate '54 4B' Test Certificate
caIdentifier	Octet String	1	'01'
CHA	Octet String	7	Certificate Holder Authorisation
tachographApplicationID	Octet String	6	'FF 54 41 43 48 4F'
equipmentType	Integer	1	1 = Driver card 2 = Workshop card 3 = Control card 4 = Company card
EOV	TimeReal	4	Certificate End Of Validity 'FF' padded if not used.
CHR	Octet String	8	Certificate Holder Reference
serialNumber	Integer	4	Serial number for the equipment, unique for the manufacturer, the equipment's type and the month and year below.
monthYear	BCDString	2	Identification of the month and the year of manufacturing (or of serial number assignment).
type	Integer	1	1 = Driver card 2 = Workshop card 3 = Control card 4 = Company card
manufacturerCode	Integer	1	'50' (80) = IN Groupe
Public Key			
n	Octet String	128	Public Key modulus
e	Octet String	8	Public Key public exponent

Table 3.a – Format of *Certificate Content*

Signature of Certificate Content is the RSASP1 signature primitive (PKCS#1) [14] with the Card Private key (*Card.SK*) over.

Field	Bytes	Explination
Fixed value	1	'4B'
Fixed value	85	85 x 'BB'
Fixed value	1	'BA'
Hash	20	SHA-1(CC)
Hash	20	SHA-1(SHA-1(CC))
Fixed value	1	'BC'

Table 3.b - Format of *Signature of Content Certificate*

IV.1.2. Certificate Application Processing

The AND-CPCA shall ensure that the Key Certification Request issued from the Card Personalizer System (AND-CP) is complete, accurate and duly authorized to process it.
The AND-CPCA shall only accept valid tachograph card certificate applications as described in Appendice 1B [2].

For each tachograph card, a unique key pair (Card_MA.PK, Card_MA.SK) used for mutual authentication shall be generated.
This task of generating tachograph cards key pairs is given to the Card Personalizer (AND-CP). Each time a key pair card is generated, the part generating this key pair shall send the public part (public key) to the AND-CPCA in order to obtain the corresponding certificate. The private key shall only be used by the tachograph card. Key Certification Requests based on the transfer of private keys are not allowed.

Approval or rejection of requests

All key certification requests received from the Card Personalizer (AND-CP) after authentication are approved. Requests that do not have the ad hoc structure, and that therefore can not be processed, are rejected.

Time to process requests

Certificate requests issued by the Card Personalizer system are processed by the AND-CPCA in a synchronous manner without delay, provided that the Card Personalizer system has been duly authenticated.

IV.1.3. Certificate issuance

If all checks are done successfully, the AND-CPCA signs et issues the certificate.

The cryptographic operations (signature of the certificate with the private key *CPCA_Card.SK*) are performed within a secure cryptographic module (HSM). Once the certificate is generated for the device (card), it can be transferred synchronously to the Card Personalizer (AND-CP).

The Certification Authority shall ensure, within the scope of its competences, that the responsible Authority is duly registered before issuing a certificate to the Card Personalizer (AND-CP).
Since the key pair is not generated by the Certification Authority, the latter issues a certificate to the Card Personalizer only if it has proof that the Personalizer is in possession of the corresponding private key. The

private key shall not leave the secure environment of the Card Personalizer during the processing of the certificate request.
The consistency and accuracy checks, as well as the signature checks of the request are performed automatically by the Certification Authority.

Certificate validity period

The validity period of a mutual authentication certificate (*Card_MA.C*) shall be as follows:

- for driver cards : 5 years
- for company cards : 5 years
- for controller cards : 5 years
- for workshop cards : 1 year

The effective date of the certificate shall indicate the date and time of the beginning of the validity period of the certificate. This will be the date and time of the certificate issuance by the Certification Authority.
The validity period for the *Card_MA.SK* private keys shall be the same as for the corresponding certificates (*Card_MA.C*).

IV.1.4. Exchange of requests and responses

Exchange of requests and responses with the ERCA

For transporting certificate requests and generated certificates, a removable storage medium shall be used. This support can only be a CD-R 12 cm medium in single-session mode (ISO 9660: 1988 [11] format).
Other means of transport may be used with the prior consent of the ERCA. For testing purposes, the ERCA accepts and distributes KCRs and certificates via e-mail.
The AND-CPCA shall write three copies of each Certificate Certification Request to the transport medium for the ERCA. These copies shall be in ASCII hexadecimal format (.txt file), Base64 (.pem file) and binary (.bin file) respectively.
Other means of transport may be used with the prior agreement of the ERCA. For testing purposes, the ERCA accepts and distributes KCRs and certificates via e-mail.
The ERCA writes three copies of each certificate on the transport medium for handing over to the AND-CPCA. These copies are in hexadecimal ASCII format (.txt file), Base64 (.pem file) and binary (.bin file) respectively.
Each certificate application and certificate shall be accompanied by a hard copy of the data, formatted according to a template defined in the ERCA Certification Practice Statement. Another paper copy of the data shall be kept by the ERCA or the AND-CPCA, respectively.
For KCRs and also certificates, transport media and prints are exchanged between an the ERCA employee and the AND-CPCA courier in an ERCA controlled space.

Exchange of requests and responses with the AND-CPCA

The connection to the PKI system of the AND-CPCA shall be secure: mutual authentication and guarantee of confidentiality of exchanges.
The requests and responses exchanged between the AND-CPCA PKI system and the Card Personalizer (AND-CP) personalization system as part of the certification service contain respectively the following information:

- Key Certification Request (KCR):

- Descriptive data of the card:
  - Type of equipment
  - Country Code
  - Card number
  - Extended serial number
  - End date: date of end of validity of the card
- Response:
  - Certificates
    - Generation 1 card certificate

IV.1.5. Certificate Acceptance

Certificate acceptance, AND-CPCA

The courier signs the receipt of the AND-CPCA certificate at the ERCA premises.
Upon receipt of the certificate at the AND-CPCA premises, the AND-CPCA shall control that:

- the transport medium is readable, that is, undamaged or corrupt;
- the format of the certificate complies with the table 7 in Chapter VII.1 ;
- all certificate field values match the values requested in the KCR;
- the signature of the certificate can be verified using the ERCA root public key indicated in the CAR field.

If any of these checks fail, the AND-CPCA shall abort the process and contact the ERCA. The certificate rejection is managed according to the certificate revocation procedure.

Certificate Acceptance, Card Personalizer (AND-CP)

Acceptance of the certificate by the Card Personalizer (AND-CP) may be implicit, provided it has the guarantee of the origin of this certificate (it is issued by the AND-CPCA).
However, in case of card personalization problem (graphic and/or electrical personalization), the Card Personalizer shall inform the AND-CPCA.
The blacklist contains a list of certificates that are considered invalid and can no longer be used in the Digital Tachograph system.

IV.1.6. Key pair and certificate usage

Key pair and certificate usage, AND-CPCA

The AND-CPCA shall use key pairs and corresponding certificates in accordance with Chapter VI.2.

Key pair and certificate usage, Card Personalizer

The Card Personalizer (AND-CP) shall use the key pair and the corresponding certificates in accordance with Chapter VI.2.

The size of the card key is set to 128 bytes (1024 bits).
A tachograph card shall use its key pair (*Card_MA.SK*, *Card_MA.PK*), exclusively to perform mutual authentication and session key exchange with the VUs, as specified in Appendix 1B – Sub-appendix 11 [2].
Key pairs, symmetric keys and PINs shall be generated and stored in a secure dedicated device that:

- is certified at EAL 4 or higher level in accordance with ISO / IEC 15408 [8]; or at ITSEC E3 level or higher; or at equivalent security criteria. Assessments should be conducted according to an appropriate protection profile or security target; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [9]; or
- meets the requirements identified in FIPS PUB 140-2 (or FIPS 140-1) Level 3 or higher [10]; or
- demonstrates an equivalent level of security.

The most common secure device used within a PKI (PKI) is the Hardware Security Module (HSM).

Operations on private keys shall be performed in the HSM that stores these keys.
Private keys should only be used in a physically secure environment by personnel in trusted roles. Private keys shall not be exploited outside the HSM without performing ad-hoc encryption. All private key usage events shall be logged in the event logs.
Key pairs and corresponding certificates of a given tachograph card shall not be replaced or renewed once the card has been issued

When issued, tachograph cards shall contain the following keys and certificates:

- The private key *Card_MA.SK* and the corresponding certificate *Card_MA.C*;
- The *CPCA_Card.C* public key (*CPCA_Card.PK*) certificate of the AND-CPCA used for the verification of the *Card_MA.C* certificate;
- The *ERCA EUR.C* public key (*EUR.PK*) certificate used for the verification of the AND-CPCA *CPCA_Card.C* certificate;
- $K_{M\text{-}WC}$ symmetric master key for workshop cards.

IV.1.7. Certificate renewal

NOTE: In the context of this Certificate Policy, the term "renewal" of a certificate reflects the action of regenerating the certificate by modifying only the validity period (conservation of the identifiers and the value of the public key).

Certificate renewal, AND-CPCA

The renewal of an existing AND-CPCA certificate (that is the extension of the validity period, with conservation of the key pair) is not allowed by the ERCA Certificate Policy [6].

Certificate renewal, Card Personalizer (AND-CP)

The renewal of an existing certificate (that is, the extension of the validity period, with the conservation of the key pair) is not authorized by this Certificate Policy.

IV.1.8. Key pair renewal

Key pair renewal, AND-CPCA

Renewal of the key pair means the signing of a new AND-CPCA certificate, replacing an existing certificate. Renewal of a key pair is done for one of these two cases:

- approaching the end of the use period of the private key. In this case, the key pair shall be renewed in time to allow the AND-CPCA to continue its certification activities after the end of this period.
- following the revocation of the certificate.

The application, the processing, the issue, the acceptance and the publication of the certificate are carried out in the same way as the initial certificate.
AND-CPCA key pairs can be changed regularly. The ERCA does not impose any limit on the number of AND-CPCA certificates it will sign. The AND-CPCA is authorized to request several certificates of the same type, if its activity justifies it, with overlapping validity periods.
The generation of new Contracting Party Key Pairs shall take into account the one month turnaround time required for certification by the ERCA.

Key pair renewal, Card Personalizer (AND-CP)

Renewal of the key pair of a tachograph card certificate (*Card_MA.C*) is not allowed. At the end of validity of the certificates and at the end of the use period of the corresponding key pair, a new tachograph card shall be created.

IV.1.9. Certificate modification

Certificate Modification, AND-CPCA

Modification of an AND-CPCA certificate is not allowed by the ERCA Certificate Policy [6].

Certificate modification, Card Personalizer (AND-CP)

Modification of a tachograph card certificate is not allowed by this Certificate Policy. Any request for a certificate modification received by the AND-CPCA will be rejected and not processed.

IV.1.10. Certificate revocation and suspension

Circumstances for certificate revocation

Revocation and suspension of a certificate, AND-CPCA

AND-CPCA certificates shall be revoked in the following cases:

- rejection by the AND-CPCA of a newly certificate issued by the ERCA;
- compromise or suspicion of compromise of the private key associated with the AND-CPCA certificate;
- loss of the private key associated with the AND-CPCA certificate;
- AND-CPCA termination;

- AND-CPA, AND-CPCA or CO failure to comply with the obligations required by the Regulation and the ERCA Certificate Policy [6].

If necessary, on the appreciation of the AND-CPCA, in the event of termination of the CO with impossibility of reversibility, the certificates of AND-CPCA may be revoked.

Revocation and Suspension of a Certificate, Card Personalizer (AND-CP)

Revocation of tachograph card certificates is not provided in this Certificate Policy. In case of receipt of a revocation request, this will not be accepted or processed by the AND-CPCA.

Who can request certificate revocation

Certificate revocation, AND-CPCA

The ERCA only accepts applications for the revocation of an AND-CPCA certificate if it comes from one of the following entities:

- the European Authority (EA)
- the AND-CPA
- the AND-CPCA

The European Authority is authorized to request the revocation of CPCA certificates as well as MSCA ones.
The AND-CPA is authorized to request the revocation of certificates issued for the AND-CPCA that is designated by this Certificate Policy.
The AND-CPCA is authorized to request the revocation of a certificate that the ERCA issued to it.
The ERCA rejects any request from any other entity.

Certificate Revocation, Card Personalizer (AND-CP)

N / A

Grace period to make the revocation request

Grace period to make the revocation request, AND-CPCA

The grace period to make the revocation request is 5 working days from the knowledge of one of the effective causes of revocation.

Grace period to make the revocation request, Card Personalizer (AND-CP)
N / A

Grace period to process the revocation request

Grace period to process the revocation request, AND-CPCA

The ERCA shall process any correct, complete and authorized request for revocation within 3 working days of receipt.

Grace period to process the revocation request, Card Personalizer (AND-CP)

N / A

Requirement to verify revocation by certificate users

Requirement to verify revocation by certificate users, AND-CPCA

The AND-CPCA is responsible for checking the status of the certificates published on the ERCA website.

Requirement to verify revocation by certificate users, Card Personalizer(M-CP)

N / A

Frequency of publication of revocation information

Frequency of publication of revocation information, AND-CPCA

Information on the status of the ERCA and AND-CPCA certificates is available online at:
https://dtc.jrc.europa.eu
ERCA maintains the integrity of the revocation information it publishes.

Frequency of publication of revocation information, Card Personalizer (AND-CP)

N / A

Grace period to publish the CRL

N/A

Requirements for online verification of the revocation and the status of certificates

No stipulation

Specific requirements concerning key compromise

Specific requirements concerning key compromise, AND-CPCA

Key compromise is a security incident that shall be considered and addressed.
In the event of compromise or suspicion of compromise of an AND-CPCA key, the AND-CPCA shall report the incident to the ERCA and to the AND-CPA. The follow-up survey and potential actions should be conducted by the AND-CPA. The findings of the AND-CPCA investigation should be reported to the ERCA.
If a compromise is confirmed or can not be excluded, the affected key shall be destroyed. Likewise, all copies of the compromised key will be destroyed.

Specific requirements concerning key compromise, Card Personalizer (AND-CP)

The compromise of a private key or symmetric master key is a security incident that shall be considered and addressed.
In the event of compromise or suspicion of compromise of a private key or a symmetric master key, the Card Personalizer (AND-CP) shall notify the AND-CPCA without delay. In its notification to the AND-CPCA, the Card Personalizer will indicate the circumstances in which the compromise occurred.

Certificate suspension

Certificate suspension, AND-CPCA

AND-CPCA certificates issued by the ERCA can not be suspended.

Certificate Suspension, Card Personalizer (AND-CP)

The Card Personalizer certificates issued by the AND-CPCA can not be suspended.

IV.1.11. Certificates status service

Information on the status of tachograph card certificates is managed by the AND-CPCA. This information is not published but is made available to parties which request it. This request is however subject to the assessment of the AND-CPCA which will study the legitimacy.

IV.1.12. End of subscription

End of subscription, AND-CPCA

The AND-CPCA subscription to the ERCA certification services ends when the AND-CPA decides for CPA termination. Such a change is notified to the ERCA by the AND-CPA as a modification of the AND-CPA national Policy.
In the event of subscription ending, the decision to submit a revocation request for all valid AND-CPCA certificates or to authorize their use until they expire is under the responsibility of the AND-CPA.

End of subscription, Card Personalizer (AND-CP)

The subscription to the AND-CPCA certification service ends when the Card Personalizer or the AND-CPA decides to terminate the service. In this case, all certificates of tachograph cards issued remain valid until they expire (i.e. validity end date is reached).
The Card Personalizer (AND-CP) shall notify the end of the service to the AND-CPA and the AND-CPCA.

IV.1.13. Keys escrow and recovery

Card private keys (*Card_MA.SK*) is expressly forbidden, meaning that once the cards are personalized these keys shall not be kept or stored in a system other than the concerned card.

IV.2. Master Key application et distribution

IV.2.1. Key Distribution Request (KDR)

Key Distribution Request, ERCA

Key Distribution Requests (KDRs) may be submitted by the AND-CPCA, subject to its recognition by the AND-CPA via its registration to the ERCA.

The format of the $K_{M\text{-}WC}$ distribution request is the following:

Field	Bytes	Explanation
Key request Content	164	See below
Signature of Key request Content	128	See below

Table 4 – Key Distribution Request format

Field	Format	Bytes	Explanation
CPI	Integer	1	Certificate Profile Identifier '01'
CAR	Octet String	8	Certification Authority Reference
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC website) 'FD' (253) = European Community
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website) '45 43 20' = "EC "
keySerialNumber	Integer	1	'00'
additionaInfo	Octet String	2	'FF FF' Production '54 4B' Test
caIdentifier	Octet String	1	'01'
MRA	Octet String	7	Message Recipient Authorisation
tachographApplicationID	Octet String	6	'FF 54 41 43 48 4F'
type	Integer	1	'27' (corresponds to the $K_{M\text{-}WC}$ key type. cf. EquipmentType values defined in Appendix 1B)
EOV	TimeReal	4	End Of Validity 'FF FF FF FF'
KID	Octet String	8	Key Identifier
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC website)
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website)
keySerialNumber	Integer	1	Serial number to identify the KDR
additionaInfo	Octet String	2	'FF FF' Production '54 4B' Test
type	Integer	1	'27' (corresponds to the $K_{M\text{-}WC}$key type)
Public Key			Ephemeral Public key used for master key encryption.
n	Octet String	128	Public Key modulus
e	Octet String	8	Public Key public exponent

Table 4.a – Format of *Key request Content*

The KDR signature is the primitive RSAP1 (PKCS#1) [14] with the ephemeral private key of the AND-CPCA.

Field	Bytes	Explanation
Fixed value	1	'4B'
Fixed value	58	58 x 'BB'
Fixed value	1	'BA'
Hash	20	SHA-1(Key request)
Hash	20	SHA-1(SHA-1(Key request))
Fixed value	1	'BC'

Table 4.b – Format of *Signature of Key request Content*

Key Distribution Request, AND-CPCA

Key Distribution Requests may be submitted by the Card Personalizer (AND-CP) to the AND-CPCA.

IV.2.2. Master keys application processing

Master keys application processing, ERCA

The ERCA ensures that the KDR issued by the AND-CPCA is complete, accurate and duly authorized.
The ERCA will only create the Key Distribution Message (KDM) if these conditions are met. Checks are done manually by the the ERCA officers and/or automated by the the ERCA registration service. If the message is complete and correct, the officers can authorize the generation of the Key Distribution Message (KDM) by the key distribution service.

Master key application processing, AND-CPCA

The key distribution request issued by the AND-CP to the AND-CPCA follows a different workflow than that presented in the ERCA schema (see chapter I.3). However, the security level of this workflow shall be at least equivalent to that of the process described in the ERCA Certification Polic [6].

IV.2.3. Confidentiality and integrity protection of master keys

Transfer from the ERCA to the AND-CPCA

Confidentiality and authenticity of the symmetric keys distributed by the ERCA to the AND-CPCA shall be ensured by RSA encryption using a transport key-pair generated by the AND-CPCA. This encryption and a hash calculation allow security of the symmetric master key during the distribution process. This process is detailed in is detailed in Appendix 1B – Sub-appendice 11 [2].

Transfer from the AND-CPCA to the Card Personalizer (AND-CP)

Confidentiality and authenticity of the symmetric keys distributed by the AND-CPCA to the Card Personalizer (AND-CP) are ensured by a secure transfer process between the two entities: direct transfer between the cryptographic hardware of the AND-CPCA and the cryptographic hardware of the AND-CP, secured with a transport key (ZMK) shared between the two HSMs. The security level of this process shall meet the requirements of the ERCA.

IV.2.4. Key Distribution Message (KDM)

Key Distribution Message, ERCA

After processing the KDR, the ERCA shall build a distribution message of the master key.
The following table shows the expected format of the KDM.

Field	Bytes	Explanation
KID	8	See below
Encrypted Labeled Master Key	128	RSA encryption scheme RSA-PKCS1-v2_0-ENCRYPT with CPCA Ephemeral Public Key

Table 5 – Format of the Key Distribution Message

Field	Format	Bytes	Explanation
KID	Octet String	8	
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC web-site)
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC web-site)
keySerialNumber	Integer	1	Serial number to identify the KDR
additionalInfo	Octet String	2	'44 4B' Production (='DK' for DES Key) '54 4B' Test (='TK' for Test Key)
type	Integer	1	'27' (corresponds to the $K_{M\text{-}WC}$ key type)
KM	Octet String	16	Certification Authority Reference

Table 5.a – Format of *Labeled Master Key*

Key Distribution Message, AND-CPCA

The keys are exported on the AND-CPCA side in encrypted form and then imported on the Card Personalizer (AND-CP) side. The message consists of a file containing the master key $K_{M\text{-}WC}$ encrypted by a ZMK transport key (256-bit AES key) shared by the two entities. The confidentiality and integrity of this key shall be guaranteed by both entities (AND-CPCA and Card Personalizer).

IV.2.5. Exchange of requests (KDR) and responses (KDM)

Exchange of KDR and KDM between the ERCA and the AND-CPCA

The KDR and KDM are transported on a removable storage medium (only CD-R is accepted).

The KDR is hand delivered by the AND-CPCA to the ERCA officiers in the form of 3 copies (3 different formats) on removable storage medium. The ERCA shall contact the AND-CPCA to ensure that the hash calculated on the received KDR matches that calculated and recorded by the AND-CPCA.

After KDR processing, the KDM is provided by the ERCA to the AND-CPCA in the form of 3 copies (3 different formats) on removable storage media.

Each KDR and KDM shall be accompanied by a paper copy of the data, formatted according to a model defined

in the ERCA Certification Policy [6]. Another paper copy of the data shall be kept by the ERCA or the AND-CPCA, respectively.

During the creation of the KDR by the AND-CPCA, the generation of a ephemeral key pair is performed. The ERCA ensures that it has not already certified the public key transmitted in the request or that this key has not been used in a previous KDR.

IV.2.6. Master Key acceptance

Acceptance by the AND-CPCA

The courier (representative of the AND-CPA) signs the delivery of the KDM on the premises of the ERCA. Upon receipt of the KDR by the AND-CPCA on the premises of the CO, the AND-CPCA verifies that:

- the removable storage medium is readable, that is, undamaged or corrupt;
- the format of the message is in accordance with Table 4;
- the message is authentic. To achieve this, the AND-CPCA contacts the ERCA as described in the ERCA CPS and verifies that the received KDM hash matches the KDM hash sent by the ERCA;
- The type and version of the master key in the message correspond to the requested type and version;
- the public point specified in the message is on the curve specified by the KDR sent by the AND-CPCA to the ERCA.

If any of these checks fails, the AND-CPCA should abort the process and contact the ERCA.

Acceptance by the Card Personalizer (AND-CP)

The Card Personalizer (AND-CP) system shall check the consistency and integrity of the symmetric master keys which are transmitted to it. Acceptance of a key by the Card Personalizer shall be explicit.

IV.2.7. Master key usage

Master key usage, AND-CPCA

The AND-CPCA shall use the master keys it received in accordance with Chapter VI.2

Master key usage, Card Personalizer (AND-CP)

The Card Personalizer (AND-CP) shall use master keys it received in accordance with Chapter VI.2

IV.2.8. KDM renewal

KDM renewal, AND-CPCA

Renewal o the KDM means issuing a copy of an existing KDM without changing the transport RSA public key or any other information contained in the KDM.
Renewal of the KDM can only be performed if the original removable storage medium received by the AND-CPCA is damaged or corrupt. Damage or corruption of the transport medium is a security incident that shall be reported to the AND-CPA and the ERCA. Following this report, the AND-CPCA may send an application for

KDM renewal to the ERCA, with reference to the original KDR.
The ERCA only accepts KDM renewal applications approved by the AND-CPA.

Note:
If the AND-CPCA needs to send a request to redistribute a master key that has been previously successfully distributed, it will generate a new KDR using a new transport RSA key pair. Such a request may lead the ERCA to investigate the possible compromise of the master key.

Renewal KDM, Card Personalizer (AND-CP)

The renewal of the request for a master key by the Card Personalizer (AND-CP) can only be performed in the exceptional case of:

- loss of the content (or compromise of its integrity) of the cryptographic hardware (malfunction, failure, etc.);
- involuntary erasure of a cryptographic object.

The AND-CPCA will be able to transfer again the master key from the cryptographic hardware (the OC one) to the Card Personalizer one (according to the initial process) by checking that the origin of the incident is not likely to compromise the master key. The AND-CPCA will nevertheless inform the AND-CPA of this incident.
The AND-CP request must be forwarded to the AND-CPCA.
If the CO is the recipient of the request, the latter must necessarily forward it to the AND-CPCA. Only the AND-CPCA can decide to transfer the master key again to the AND-CP.

IV.2.9. Master key renewal

Master key renewal, AND-CPCA

If the ERCA generates a new master key version, the availability of this new version is published on the ERCA website, specifying its version number and length.
To obtain this new version, the AND-CPCA shall submit a new KDR. The request for a new master key shall be made in due course so that the key can be taken into account quickly in the new cards issued by the Card Personalizer (AND-CP).
The key request, processing, distribution and acceptance processes are the same as for the initial master key.

Master key renewal, Card Personalzer (AND-CP)

The AND-CPCA shall inform the Card Personalizer (AND-CP) of the availability of a new master key version, without delay, as soon as they have been obtained.
The transfer of this new master key version from the cryptographic material of the AND-CPCA (more precisely from the CO one) to the AND-CP one is perfomed according to the initial process (see 0 paragraph KDM, AND-CPCA).

IV.2.10. Master key revocation

Notification of master key compromise, AND-CPCA

If the AND-CPCA detects or is notified of the compromise or suspicion of compromise of a master key, it shall

inform the ERCA and the AND-CPA without delay and at least within 5 days of such detection/notification. The AND-CPCA will indicate in its notification the circumstances in which the compromise occurred.
The ERCA processes the incident according to a defined security incident handling procedure and immediately informs the European Authority (EA).

Any investigation and potential action by the AND-CPA and/or the AND-CPCA shall be performed in accordance with the AND-CPA policy. The conclusions of the AND-CPA investigations shall be transmitted to the ERCA.

Notification of master key compromise, Card Personalizer (AND-CP)

If the Card Personalizer (AND-CP) detects or is notified of the compromise or suspicion of compromise of a master key, it shall inform the AND-CPCA and the AND-CPA without delay. In its notification, the Card Personalizer will indicate the circumstances in which the compromise occurred.

IV.2.11. Master key status service

The status of the master keys is exclusively managed by the ERCA. It shall be retrieved online at the following address:
https://dtc.jrc.ec.europa.eu/
Information on the status of master keys published by the ERCA is updated on the first working day of each week. The availability of the website mentioned above is ensured during business hours.

IV.2.12. End of subscription

End of subscription, AND-CPCA

The ERCA Master Key Distribution Services subscription ends when the AND-CPA decides for CPA termination. This change is notified to the ERCA by the AND-CPA as a modification of the national policy.
In the event of end of subscription, the AND-CPCA shall securely destroy all copies of any symmetric master key in its possession and keep proof of such destruction that may be made available to the AND-CPA or the ERCA. Thus, it must notify the CO and participate with the latter in this destruction.

End of subscription, Card Personalizer (AND-CP)

The Card Personalizer (AND-CP) may decide to terminate its subscription to the master key distribution service. Its decision shall be notified to the AND-CPCA.
In the event of end of subscription, the Card Personalizer shall securely destroy all copies of the master key in its possession.

IV.2.13. Master keys escrow and recovery

Master Keys escrow, AND-CPCA
The escrow of master keys is expressly prohibited, meaning that they shall not be exported or stored in a system other than the AND-CPCA production and backup systems (OC cryptographic hardware).

Master keys escrow, Card Personalizer (AND-CP)

The escrow of the master keys is expressly prohibited, which means that they shall not be exported or stored in a system other than the AND-CP production and backup systems (cryptographic hardware).

V. Facility, management and operational controls

V.1. Physical controls

V.1.1. AND-CPCA

Key and certificate generation services shall be hosted in a secure area, protected by a defined security perimeter, with appropriate security barriers and access controls to prevent unauthorized access, damage, and interference.
Storage media for confidential information, such as hard drives, smart cards, and HSMs, shall be protected from unauthorized or unintentional use, access, disclosure, or damage by persons or other threats (e.g. fire, flood).
Storage media destruction procedures shall be implemented to prevent unauthorized use, access or disclosure of confidential data.
Procedures for the disposal of waste shall be implemented in order to avoid unauthorised use, access, or disclosure of confidential data.
Off-site backup for the AND-CPCA critical data, especially for its private keys, shall be implemented.

V.1.2. Card Personalizer (AND-CP)

Key generation services shall be hosted in a secure area, protected by a defined security perimeter, with appropriate security barriers and access controls to prevent unauthorized access, damage, and interference.
Storage media for confidential information, such as hard drives, smart cards, and HSMs, shall be protected from unauthorized or unintentional use, access, disclosure, or damage by persons or other threats (eg fire, flood).
Storage media destruction procedures shall be implemented to prevent unauthorized use, access or disclosure of confidential data.

V.2. Procedural controls

Procedural controls shall be implemented to ensure the security of operations. In particular, the segregation of duties shall be enforced by the implementation of multi-person control for critical tasks.
Access to the AND-CPCA systems (ownership of the CO) and to the Card Personalizer (AND-CP) ones shall be restricted to individuals who are duly authorized and on need-to-know basis. In particular, the following access control measures shall be implemented:

- Confidential data shall be protected in order to preserve their integrity and confidentiality during storage;
- Confidential data shall be protected in order to preserve their integrity and confidentiality when they are exchanged over unsecure networks;
- The deleted confidential data shall be permanently destroyed, for example by re-writing the storage medium several times with random data;

- the AND-CPCA and the Card Personalizer (AND-CP) systems shall ensure efficient user administration and access management;
- The AND-CPCA and the Card Personalizer (AND-CP) systems shall ensure that access to information and functions of the application system is restricted to authorized staff and provide sufficient computer security controls to separate trusted roles. In particular, the use of system utility programs shall be restricted and strictly controlled. Access shall be restricted, allowing only access to the resources necessary to perform the role assigned to a user;
- The staff working on behalf of the AND-CPCA (including the CO staff) and the Card Personalizer staff shall be identified and authenticated before using their respective systems;
- The staff working on behalf of the AND-CPCA (including the CO staff) and the Card Personalizer (AND-CP) staff is accountable for their activities which shall be recorded in the event logs, as described in Section V.4;

The AND-CPCA (more precisely the CO) and the Card Personalizer (AND-CP) shall set up an Information Security Management System (ISMS) based on a risk assessment for all relevant operations. The AND-CPCA (more precisely the CO) and the Card Personalizer (AND-CP) shall ensure that their ISMS policy addresses staff training, roles and permissions. The implementation of the ISMS by the AND-CPCA (more precisely the CO) and the Card Personalizer (AND-CP) should conform to the best practices described in ISO/IEC 27001 [12] and ISO/IEC 27005 [13].

V.3. Personnel controls

V.3.1. Security measures relative to AND-CPCA personnel

The responsibilities of the AND-CPCA may be outsourced to a specialized company, or a contractor's personnel may be employed to perform them. In particular, the responsibility for issuing certificates and distributing master keys is subcontracted to the Certification Operator designated by the AND-CPCA.
All personnel involved in the AND-CPCA activities shall be properly trained and possess the knowledge, experience and qualifications required for the services offered and in line with the function performed. This concerns staff directly employed by the AND-CPCA, staff of a specialized company for which tasks have been subcontracted or staff of a contractor. In particular, the CO staff is concerned.
Staff training should be managed according to a training plan. In particular, a training plan shall be detailled in the CO Certification Practice Statement (CPS).
Staff appointment to trusted roles shall be managed in accordance with a selection procedure outlined in the CO CPS.
The trusted roles, on which the security of the operation depends, shall be clearly identified in the CO CPS. These roles and associated responsibilities shall be documented in job descriptions. These job descriptions shall be made from the point of view of segregation of duties and least privilege. No one should be allowed to run simultaneously multiple trusted roles.

V.3.2. Security measures relative to Card Personaliser (AND-CP) personnel

All personnel involved in the Card Personalization (AND-CP) activities shall be properly trained and shall possess the knowledge, experience and qualifications required for the services offered and adapted to the function performed. This concerns personnel employed directly by the Card Personalizer (AND-CP), the personnel of a specialized company for which tasks have been subcontracted or the personnel of contractors.

V.4. Audit logging procedures

V.4.1. Audit logging procedures, AND-CPCA

All significant security events generated by the AND-CPCA software (more precisely by the CO software) shall be automatically time-stamped and recorded in the system logs. These include at least the following:

- Successful and failed attempts to create, update, delete or retrieve information about personnel accounts, and create or revoke privileges of an account;
- attempts, successful and unsuccessful, to define or modify the authentication method (password, biometric or cryptographic certificate, for example) of a user account;
- Attempts, successful and failed, login and logout to an account;
- Successful and failed attempts to modify the software configuration;
- Starting and stopping software;
- Software updates;
- System start-up and shutdown;
- Successful and unsuccessful attempts to add or remove an entity from the subscribers register for which the AND-CPCA provides (through the CO) key certification services, or to modify the information of any subscribers or to retrieve information from this register;
- Successful and failed attempts to process a Key Certification Request (KCR) or Key Distribution Request (KDR);
- Successful and failed attempts to sign a certificate (ENT.C) or to generate a key distribution message (KDM);
- Successful and failed interactions with the database(s) containing information about the (status of) issued certificates, including logon attempts and read, write, update or removal operations;
- Attempts, successful or failed, to connect or disconnect from an HSM;
- Successful or failed attempts to authenticate a user to an HSM;
- Successful and failed attempts to generate or destroy a key pair or symmetric key within an HSM;
- Attempts, successful and failed, to import or export a key to or from an HSM;
- Attempts, successful and failed, to change the life cycle state of any key pair or any symmetric key;
- Attempts, successful and failed, to use a private or symmetric key inside an HSM for any purpose.

In order to investigate security incidents, the system log shall include, if possible, information to identify the person or account that performed the system tasks.
The integrity of the system event logs shall be ensured and the event logs shall be protected from unauthorized inspection, modification, deletion or destruction. System event logs shall be backed up and stored internally.

V.4.2. Audit logging procedures, Card Personalizer (AND-CP)

All significant security events generated by the Card Personalizer (AND-CP) software shall be automatically time stamped and recorded in the system event logs.
In order to investigate security incidents, the system log shall include, if possible, information to identify the person or account that performed the system tasks.

The integrity of the system event logs shall be ensured and the event logs shall be protected from unauthorized inspection, modification, deletion or destruction. The system event logs shall be backed up and stored internally.

V.5. Records archival

An overview of the events to be archived shall be described in the internal procedures and shall comply with the rules and regulations in force. The AND-CPCA (more precisely the CO) and the Card Personalizer (AND-CP) implement appropriate record archival procedures. Measures shall be taken to ensure the integrity, authenticity and confidentiality of the records.
For all archived information, archiving periods are indeterminate.
Measures shall be taken to ensure that records are kept without reasonable risk of loss.
The events mentioned in section V.4 shall be periodically checked for integrity. These inspections take place annually as part of periodic security audits.

V.6. Key changeover

The AND-CPCA shall generate a new key pair (*CPCA_Card.PK* and *CPCA_Card.SK*) according to its needs. Once the AND-CPCA has generated a new key pair, it shall submit a Key Certification Request (KCR).
The AND-CPCA shall ensure that replacement keys are generated in a controlled manner and in accordance with the procedures defined in this Certificate Policy.

V.7. Compromise and disaster recovery

V.7.1. Compromise and disaster recovery, AND-CPCA

The AND-CPCA shall define (jointly with the CO) the security incidents and the processing procedures for compromise through a Security Incident Processing Procedure, which shall be published for administrators and auditors.
The AND-CPCA shall maintain (jointly with the CO) a Business Continuity Plan detailing how it will maintain its services in the event of an incident affecting normal operations. When detecting an incident, operations shall be suspended until the level of compromise is established. The CO further assumes that technological advances will render its computer systems obsolete over time and shall therefore define the measures to manage obsolescence.
The procedures for backup and restore of all relevant data shall be described in a backup and recovery plan.
The following incidents are considered as disasters :

- compromise or theft of a (AND-CPCA) private key and/or a master key;
- loss of a (AND-CPCA) private key;
- failure of computer equipment.

The loss of a master key by the AND-CPCA (i.e. by the CO) does not constitute a disaster, the ERCA ensuring the conservation of the master keys it generates (existence of multiple copies subject to periodic checks).
Protection against computer equipment failure is ensured by the redundancy of the equipment.

V.7.2. Compromise and disaster recovery, Card Personalizer (AND-CP)

The Card Personalizer (AND-CP) shall write a plan for handling security incidents and compromises of private keys and/or master keys.

V.8. Termination of activity

V.8.1. Termination of activity, AND-CPCA

In the event of the termination of AND-CPCA activity by the appointed organization, the AND-CPA shall inform the EA and the ERCA, indicating the newly appointed AND-CPCA. The AND-CPA shall ensure that at least one AND-CPCA is operational at all times.
If necessary, the contract with the CO may be transferred between the entity ceasing the AND-CPCA activity and the new designated entity.

V.8.2. Termination of activity, Certification Operator (CO)

In the event of the termination of CO activity to operate the AND-CPCA PKI, the CO shall inform the AND-CPCA. The AND-CPCA will search for another CO which could operate its PKI.
The AND-CPA is accountable to the ERCA for the correct management of the activities transfer/termination.

V.8.3. Termination of activity, Card Personalizer (AND-CP)

If the Card Personalizer (AND-CP) terminates its activities, the AND-CPCA and the AND-CPA shall be informed. The AND-CPA shall inform the European Authority (EA) and the ERCA of this termination of activity. It shall also indicate to the AND-CPCA, the EA and the ERCA the newly appointed Card Personalizer.
The AND-CPA shall ensure that at least one Card Personalizer is operational at all times within the perimeter of Andorra.

VI. Technical security controls

VI.1. Key pairs generation and installation

VI.1.1. Key pairs of the AND-CPCA

The AND-CPCA shall generate its private keys in accordance with Appendix 1B [2]. Key pairs generation shall be performed in a physically secure environment by staff in trusted roles under at least dual person control. The key ceremony shall be documented.
The AND-CPCA system (more precisely the CO system) shall be able to issue key certification requests (KCRs) and master key distribution requests (KDR) to the ERCA according to the processes described in Chapters IV.1.1 and IV.1.2.
The CO should have an AND-CPCA test environment for interoperability testing, in accordance with the Regulations (see Specifications for Equipment Interoperability Testing [7]). If present, the AND-CPCA test environment shall be a separate environment and shall have its own AND-CPCA private keys and its own master keys.
The AND-CPCA test environment shall be able to issue to the ERCA test certificates signing and test keys distribution requests according the processes described in Chapters IV.1 and IV.2.

The AND-CPCA test environment shall also be able to sign equipement (cards) test certificates and to distribute the test master key on request of the AND-CP.

VI.2. Private and symmetric keys protection and cryptographic module technical controls

The AND-CPCA (through the CO) and the Card Personalizer (AND-CP) shall maintain the confidentiality, integrity and availability of private keys and master keys, as described below.
Private keys and master keys shall be generated and used in a secure device that:

- is certified at EAL 4 or higher level in accordance with ISO / IEC 15408 [8]; or at ITSEC E3 level or higher; or at equivalent security criteria. Assessments should be conducted according to an appropriate protection profile or security target; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [9]; or
- meets the requirements identified in FIPS PUB 140-2 (or FIPS 140-1) Level 3 or higher [10]; or
- demonstrates an equivalent level of security.

The most common secure device for use within a PKI is the Hardware Security Module (HSM). Other implementations using different devices are also possible, provided that the implemented devices meet one of the security requirements listed above. In addition to these security requirements, this AND-CPA Certificate Policy contains additional functional requirements for the hardware security module used in the CO system dedicated to the AND-CPCA. Note that if a different device is used in place of an HSM, all these functional requirements shall also be satisfied. The term "HSM" is used generically in the document as an abbreviation for the requirements mentioned above.

Private key operations and master key operations shall be performed in the HSM that stores these keys.
The private keys and master keys of the AND-CPCA and Card Personalizer (AND-CP) shall only be used in a physically secure environment by staff in trusted roles under at least dual person control. All events related to the use of private keys and the use of symmetric master keys shall be logged.
The private keys of the AND-CPCA and the Card Personalizer (AND-CP) as well as the master keys may only be saved, stored and recovered by personnel in trusted roles and under at least dual person control in a physical secured environment.
The backup copies of the AND-CPCA and AND-CP private keys as well as the master keys shall be subject to the same level of security controls as the keys in use.
A backup copy of the AND-CPCA private key (*CPCA_Card.SK*) and a copy of each master key shall be kept off-site.
Private keys import and export shall occur only for backup and restore purposes.
Master key import and export is allowed for backup and restore.
Export of the master key $K_{M\text{-}WC}$ in encrypted form is allowed to respond to a valid key distribution request from the Card Personalizer (AND-CP) by staff in trusted roles and under at least dual person control.
At the end of use period of a AND-CPCA or Card Personalizer (AND-CP) private key, all copies of the concerned key shall be destroyed in such a way that this key cannot be recovered.
Similarly, at the end of use period of a symmetric master key (as specified in Appendix 1B [2]), the AND-CPCA and the Card Personalizer (AND-CP) shall destroy all copies of the key in their possession in such a way this key cannot be recovered. Otherwise, if this private key is kept, its holder shall prevent any use of the latter.

Private keys and master keys shall be deactived and destroyed in case of compromise or suspicion of compromise. The keys shall be destroyed after investigating their compromise and taking the decision to deactivate these keys.
Destroying of private keys and master keys shall be done using the HSM destroy key function. Similarly, backup copies of compromised keys shall be destroyed.

VI.3. Other aspects of key pairs management

The AND-CPCA certificates and therefore the associated public keys shall be archived indefinitely.
The validity periods of all AND-CPCA certificates shall be in accordance with Appendix 1B [2].
The ERCA, by default, sets the end of validity of AND-CPCA public key certificates for tachograph cards at 7 years from the issuing date.
The ERCA will use the End-of-validity information specified by the AND-CPCA in the KCR if it does not exceed the 7-year limit.
In accordance with the ERCA Policy, the period of use of the AND-CPCA private keys must be a maximum of two years. The periods of use of the private keys must begin on the effective date indicated in the corresponding certificate.
The AND-CPCA shall not operate a private key after the end of its period of use.

VI.4. Activation data

The AND-CPCA private keys and/or the symmetric master keys stored in the HSM shall be activated only if all the persons controlling the keys have been authenticated on the HSM. Authentication shall be performed

using appropriate means (eg, passphrases, authentication tokens).
The duration of an authentication session shall not be unlimited. A new authentication of the users shall be performed if a reactivation of the key(s) is necessary.
For the activation of the AND-CPCA software (more precisely the CO software), the authentication of the user shall be performed using appropriate means (for example by a passphrase).

VI.5. Computer security controls

The AND-CPCA (more précisely the CO) and the Card Personalizer (AND-CP) shall specify and approve specific technical security procedures and measures for the management of its computer systems. These procedures shall ensure that the required level of security is always achieved. Technical security procedures and measures should be described in internal documentation and/or security concepts. Computer systems shall be designed and managed in accordance with these procedures, the procedures specified in the security concepts and best practices for trustworthy and confident computing.

VI.6. Computer life cycle security controls

The AND-CPCA (more précisely the CO) and the Card Personalizer (AND-CP) shall perform a security requirements analysis during the design and specification phase to ensure that security is taken into account in their systems.
A separation between the Acceptance (or pre-production) and Production systems shall be maintained. Change procedures and security management procedures shall ensure that the required level of security is maintained in the Production system.
Change control procedures shall be documented and used for releases, changes, and (emergency) software fixes for all operational software.

VI.7. Network security controls

The AND-CPCA (more precisely the CO) shall design and implement a network architecture in such a way that access from the Internet to its internal network and from the internal network to the Certification Authority systems can be effectively controlled.
In particular, the complete offline implementation of the Certification Authority signature system (disconnection from the network) shall be considered.

VI.8. Time stamping and dating system

The date and time of an event shall be included in each record of the audit trail. The CO Certification Practice Statement (CPS) and the Card Personalizer (AND-CP) Policy shall describe how time is synchronized and verified.

VII.Certificates, CRL and OCSP profile

VII.1. AND-CPCA Certificate profile

AND-CPCA certificate (*CPCA_Card.C*) shall have the following profile as specified in Appendix 1B [2]:

Field	Bytes	Explanation
Signature	128	RSASP1 signature primitive (PKCS#1) [14] with the ERCA RSA Private Key (*EUR.SK*) of below fields
Fixed value	1	'6A'
C_r	106	First 106 bytes of the Certificate Content as supplied in the KCR
Hash	20	SHA-1(CC)
Fixed value	1	'BC'
C_n	58	Last 58 bytes of the Certificate Content as supplied in the KCR
CAR	8	See Request

Table 6 – AND-CPCA Certificate profile

VII.2. Card certificates format

Card certificates (*Card.C*) issued by the AND-CPCA shall have the following profile as specified in Appendix 1B [2]:

Field	Bytes	Explanation
Signature	128	RSASP1 signature primitive (PKCS#1) [14] with the AND-CPCA RSA Private Key (*CPCA_Card.SK*) of below fields
Fixed value	1	'6A'
C_r	106	First 106 bytes of the Certificate Content as supplied in the KCR
Hash	20	SHA-1(CC)
Fixed value	1	'BC'
C_n	58	Last 58 bytes of the Certificate Content as supplied in the KCR
CAR	8	See Request

Table 7 – Card certificate format

VII.3. CRLs profile

The status of certificates issued by the ERCA (i.e. CPCA certificates) can be found on the website: https://dtc.jrc.ec.europa.eu/

No CRL (Certificate Revocation List) is issued by the AND-CPCA.

VII.4. OCSP Profile

No OCSP service shall be implemented.

VIII. Compliance audit and other assessments

VIII.1. Frequency and/or circumstances of assessments

VIII.1.1. Audit of the AND-CPCA

A full and formal audit of the AND-CPCA and CO activity shall be performed by order of the AND-CPA. The audit of respectively the AND-CPCA and the CO shall establish whether respectively the AND-CPCA and the CO requirements described in this Certificate Policy are met. The AND-CPA shall perform the first audit within 12 months of the start of the operations covered by this Certification Policy.
If no evidence of non-compliance is found during the audit, the next audit shall be perfomed within 24 months. If not, the next audit shall be performed within 12 months to ensure that non-compliances have been solved.
The AND-CPA shall report the results of the audit and provide the audit report, in English, to the ERCA. This report shall define all the corrective actions required to fulfill the obligations of the AND-CPA. It also includes a timetable for implementing these corrective actions.

VIII.1.2. Audit of the Card Personalizer (M-CP)

An audit of the Card Personalizer (AND-CP) activity shall also be performed by order of the AND-CPA. This audit shall establish that the Card Personalizer (AND-CP) practices meet the requirements of this Certification Policy.
The Card Personalizer (AND-CP) shall undergo at least the same audit scheme as the AND-CPCA and the CO, as it is reponsible for private key (*Card*.*SK*) and symmetric master key it writes down to the cards.
Before the begining of the operations covered by this certificate policy, the AND-CPA shall carry out a pre-operational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements in the AND-CPA certificate policy.
In order the AND-CP can access the AND-CPCA service, the card manufacturer (AND-CM) shall demonstrate that the equipment (card) it provides to the AND-CP has received the ad hoc certifications.

VIII.1.3. Audit of the Card Issuer (AND-CIA)

The AND-CPCA may, if it wishes, audit or have the Issuer of Cards (AND-CIA) audited to ensure that the practices of the latter comply with the requirements of this Certification Policy, in particular with regard to its Delegated Registration Authority role.
The frequency and number of these audits are not fixed by this CP.

VIII.2. Identity and qualification of assessors

The audit shall be performed by an independent auditor specialized in Information Technologies.
Any person selected or proposed to perform a compliance audit of the AND-CPCA or of the Card Personalizer (AND-CP) shall be first approved by the AND-CPA.
The names of the auditors who will perform the audits shall be registered by the AND-CPA. Such auditors shall comply with the following requirements:

- Ethical behavior - trustworthiness, uniformity and confidentiality regarding their relationship to the audited Certication Authority and when handling its information and data;
- Fair presentation – findings, conclusions and reports from the audit are true and precisely describe all the activities carried out during the audit;
- Professional approach – has a high level of expertise and professional competency and makes effective use of its experience gained through good and deep-rooted practice in information technologies, PKI and the related technical norms and standards.

The auditor shall possess significant knowledge of, and preferably be accredited for:

- Information system security audits;
- PKI and cryptographic technologies;
- The operation of PKI software;
- The relevant European Commission policies and regulations.

VIII.3. Relations between assessors ans assessed entities

The auditor shall be independent and not related to the audited entity, i.e. the AND-CPCA or the CO. He shall not suffer any conflict of interest with the AND-CPCA or the CO.

VIII.4. Topics covered by the assessments

The audit of the AND-CPCA, the CO and the Card Personalizer (AND-CP) shall cover compliance to this Certification Policy, the CO Certification Practice Statement as well as the related procedures and techniques written by the AND-CPCA and/or the CO.
The purpose of the compliance audit shall be the implementation of the technical, procedural and organizational practices described in these documents.
The areas of intervention of the audits are as follows:

- identification and authentication;
- operational functions / services;
- physical, procedural and personnel security controls;
- technical security checks;
- security incident handling procedures.

Audit log analysis allows to determine if the security of the AND-CPCA systems (more precisely the CO systems) is weak. These potential weaknesses shall be reduced by appropriate measures. The analysis and any weaknesses shall be recorded.

In the event of an exceptional audit triggered by a serious security incident, the audit shall focus on the processes and technical measures related to the security incident.

VIII.5. Actions taken after the conclusions of the assessment

VIII.5.1. Audit of the AND-CPCA and the CO

If non-compliances are discovered by the auditor, corrective actions shall be taken immediately by the concerned entity (the AND-CPCA or the CO). Once the corrective measures have been implemented, a follow-up audit shall be carried out within 12 months.

VIII.5.2. Audit of the Card Personalizer (AND-CP)

If non-compliances are discovered by the auditor, corrective actions shall be taken immediately by the AND-CP. Once the corrective measures have been implemented, a follow-up audit shall be carried out within 12 months.

VIII.5.3. Audit of the Card issuer (AND-CIA)

If non-compliances are discovered by the auditor, corrective actions shall be taken immediately by the Card Issuer (AND-CIA). The AND-CPCA may, if it wishes, carry out a follow-up audit. This CP does not impose a deadline for this audit.

VIII.6. Communication of the results

VIII.6.1. Audit of the AND-CPCA and the CO

The independent auditor shall report the full results of the compliance audit of the AND-CPCA and the CO to the AND-CPA, the audit sponsor. The AND-CPA shall send an audit report covering the relevant results of the audit to the ERCA. This report shall include at least the number of deviations found and the nature of each deviation. The audit report reception date shall be published on the ERCA website. If requested by the ERCA, the AND-CPA shall send it the full results of the compliance audit.

VIII.6.2. Audit of the Card Personalizer (AND-CP)

The results and compliance audit report of the Card Personalizer (AND-CP) shall be communicated to the AND-CPA, the audit sponsor. This report shall include at least the number of deviations found and the nature of each deviation.

VIII.6.3. Audit of the Card Issuer (AND-CIA)

The results and the compliance audit report of the Card Issuer (AND-CIA) shall be communicated to the AND-CPCA, the audit sponsor. This report shall include at least the number of deviation found and the nature of each deviation.

IX. Other business and legal issues

IX.1. Fees

The M-CPCA has signed a service contract with the "IN Groupe" entity. These services cover:

- CO services
- AND-CP services
- AND-CM services

These services are invoiced to the AND-CPCA according to the terms of the contract signed between the parties.

IX.2. Financial responsability

No stipulation

IX.3. Confidentiality of business information

Confidential data shall comprehend at least:

- Personal data (e.g. from AND-CPCA, CO, Card Perzonaliser employees, or ERCA representatives);
- Private keys;
- Symmetric master keys;
- Reasons for certificate revocation;
- Audit logs (unless access is required by court décision, by regulations or by the provisions of the CP or the CPS);
- Detailed documentation ralting to the PKI management;
- Audit reports (internal or external).

Confidential information shall not be released, unless a legal obligation exists to do so.

IX.4. Privacy of personal information

The only personal data processed or stored in the AND-CPCA and/or CO system is those of ERCA, AND-CPCA and AND-CP representatives.
This data shall be treated according to the General Data Protection Regulation 2016/679 (GDPR).

IX.5. Intellectual et industrial property rights

The AND-CPCA does not own the software that the CO implements under the operation of the PKI of the Digital Tachograph system.

IX.6. Representations and warranties

The AND-CPCA and the CO shall operate according the ERCA Certificate Policy [6], this Certificate Policy and, also for the CO, according to its own Certification Practice Statement (CPS) it wrote.

IX.7. Warranty limits

The AND-CPA and the AND-CPCA disclaims all commercial warranties and obligations of any type. They and further disclaims any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

IX.8. Limitations of liability

It is expressly understood that neither the AND-CPA nor the AND-CPCA can be held responsible for any damage resulting from a fault or negligence of a subscriber, nor from damage caused by an external fact, especially in case of:

- Use of a certificate for an application other than the applications defined in Chapter I.4 of this CP;
- Fraudulent or negligent use of a certificate or status information of a certificate issued by the AND-CPCA (via the CO) ;
- Use of a certificate to guarantee another object than the identity of the equipment (card) for which the certificate was issued ;
- Use of a certificate beyond its validity limit ;
- Non-compliance by the entities concerned with their obligations as defined in this CP;
- Facts external to the certificate issuance such as a failure of the application or equipment (card) for which it was issued ;
- Force majeure as defined by the French courts.

Subscribers and relying parties using the AND-CPA services are not eligible for compensation claims for losses resulting from inappro-priate or fraudulent use of the key management system of the AND-CPCA.
The AND-CPCA or the CO responsibility can only be held liable if it is shown that it has operated in a manner inconsistent with this certificate policy and, only for the CO, with the CPS it wrote.

IX.9. Indemnities

No stipulation

IX.10. Term and termination of the CP

This certification policy is valid as soon as it is approved by the AND-CPA and the JRC. It shall be valid until further notice.

The validity of this CP ends when the AND-CPA stops operating or when the AND-CPA announces this CP is no longer valid, e.g. because a new version of the CP becomes effective.

IX.11. Individual Notices and communications with Participants

Official notices and communications with participants in the Digital Tachograph key management system shall be in written form, and subject to the registration procedures for correspondence in force within the Andorran Transport.
Notice of severance or merger may result in changes to the scope, management and/or operation of the AND-CPCA. In such an event, this Certificate Policy and the CO Certification Practice Statement (CPS) may require modification as well. Changes to these documents shall be made in a manner consistent with the administrative requirements stipulated in section IX.12 of this document.

IX.12. Amendments to the CP

This CP is issued under responsibility of the AND-CPA. The AND-CPA may revise this CP if it deems this necessary.
The procedure for change propositions and approvals of this CP shall be as follows:

1. Comments or requests for changes to the CP shall be addressed by the AND-CPCA or the AND-CP to the AND-CPA. Such communication shall include a description of the comment or requested change, a rationale, and contact information for the person submitting the comments or requesting the change.
2. The AND-CPA shall accept, accept with modifications, or reject the comment or proposed change after completion of the comment period (fixed appropriately by the AND-CPA). AND-CPCA or AND-CP disposition of proposed changes are reviewed by the AND-CPA. Decisions with respect to the proposed changes are at the discretion of the AND-CPA.
3. A new version of this Certificate Policy will be published on the AND-CPA website and distributed to the ERCA, the AND-CPCA, the CO, the AND-CP and the AND-CIA.

Every change to this CP shall be accompanied by an increase in the version number of the document. The only changes that may be made to the CP and CPS with no change to the document version number are editorial or typographical corrections.
The AND-CPCA may change the contact information in section I.5 with notification to the AND-CPA and the ERCA, but without change to the document version number. All other changes to the CP shall be made according to the amendment procedure outlined in this section.

IX.13. Dispute resolution procedures

Any dispute related to master keys and certificates management for the Digital Tachograph system between the AND-CPCA and an organization or individual outside of the AND-CPCA or the CO shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible. A

dispute not settled by negotiation should be resolved through arbitration by the AND-CPA.

IX.14. Compliance with laws and regulations

This Certificate Policy is compliant with AETR agreement [2]. In case discrepancies exist between this document and the Regulation, the latter shall prevail.

IX.15. Miscellaneous dispositions

No stipulation

IX.16. Other dispositions

No stipulation

X. Annex A: List of schemas

Schema 1: Relation between the different entities involved in the Andorran perimeter
Schema 2: workflow inside Andorran PKI

XI. Annex B: List of tables

XII. Annex: References

1. Regulation (EU) No 3821/85. Official Journal of the European Union L60.
2. European agreement concerning the work of crews of vehicles engaged in international road transport (AETR), dated July the 1st 1970
3. ETSI EN 319 411–1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, version 1.1.1, 2016-02
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
6. JRC, Digital Tachograph - ERCA Certification Policy, version 2.1
7. JRC, Smart Tachograph - Equipment Interoperability Test Specification, version 1.0
8. ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security
9. CEN Workshop Agreement 14167-2 : Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2 Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)
10. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
11. ISO/IEC 9660:1988, Informatin processing – Volume and file structure of CD-ROM for information interchange
12. ISO/IEC 27001:2018, Information technology – Security techniques – Information security risk management systems -- Requitrements
13. ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management
14. PKCS#1 v2.0 : RSA Cryptography Standard, RSA Laboratories, 1er Octobre 1998
15. TDES : National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. 19999 Draft Standard project