PUBLIC

OFFLINE CAS CERTIFICATION POLICY - CERTIFICATION PRACTICES STATEMENTS

AUTHOR(S) : F. Lesecq

DOCUMENT NO : WLM-TSP-F104
VERSION : 1.3
STATUS : Final
SOURCE : Worldline
DATE OF THE DOCUMENT : January 27, 2020
NUMBER OF PAGES : 52

DOCUMENT OWNER : Comité MediaCert

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2020-03-03 12:02:18

Role	Name	Signature	Date
Reviewer 1 – Head of TSP	Fanny Lesecq	Fanny Lesecq	27/01/2020
Reviewer 2 – ISSM	Thomas Belot	Thomas Belot	27/01/2020
Quality insurance function	Fanny Lesecq	Fanny Lesecq	27/01/2020
Document owner	Comité MediaCert	Guillaume Bailleul	27/01/2020
Approving – Resp. TSP	Guillaume Bailleul	Guillaume Bailleul	27/01/2020

Table of consents

List of changes

Version	Date	Description	Author(s)
0.1	31/11/2017	Initialization of the document	F. Da Silva N. Abrioux V. Dumond
1.0	29/03/2018	Validation of the document in Security Committee	MediaCert Committee
1.1	05/07/2018	Adding reasons for revocation in accordance with the update of 319 411-1 and 319 411-2	F. Da Silva
1.2	18/09/2018	Modification of the Intermediate CA Certificate Template	F. Da Silva
1.3	27/01/2020	Modification of the table headers defining the information retention period. Addition of the possibility of having a person equivalent to a judicial officer in the case of the creation of a root CA. Evolution of the versions of the standards of the reference system. Addition of CA Timestamping and Intermediate CA Mediacert Trust CA 2019.	F. Lesecq F. Poulain

1 Introduction

1.1 General presentation

The MediaCert *Trust Service Provider*, established by Worldline, provides a range of Trust Services and is therefore subject to the eIDAS Regulation No 910/2014 of the European Parliament and of the European Council on electronic identification and trust services for electronic transactions in the internal market.

This document describes the Certification Policy of four (4) CAs operated by MediaCert TSP:

- a Root CA named "Mediacert Root CA 2018", to issue Certificates to intermediate online or offline CAs, including the Time-stamping CA named "Mediacert Timestamp CA 2018" presented in this document and possibly to other trusted services;
- a Root CA named "Root CA – 2012", to issue à AC OTU 3 Certificate.
- a Time-stamping CA named "Mediacert Timestamp CA 2018", daughter of the Mediacert Root CA 2018, aimed at issuing sealing certificates exclusively to Time-stamping units, operated by the MediaCert TSP;
- an intermediate CA named "Mediacert Trust CA 2019", aiming to issue Certificates to online CAs, issuing signature certificates or electronic seal.

These four (4) CAs are part of MediaCert TSP's Trust Services as shown in the diagram below.

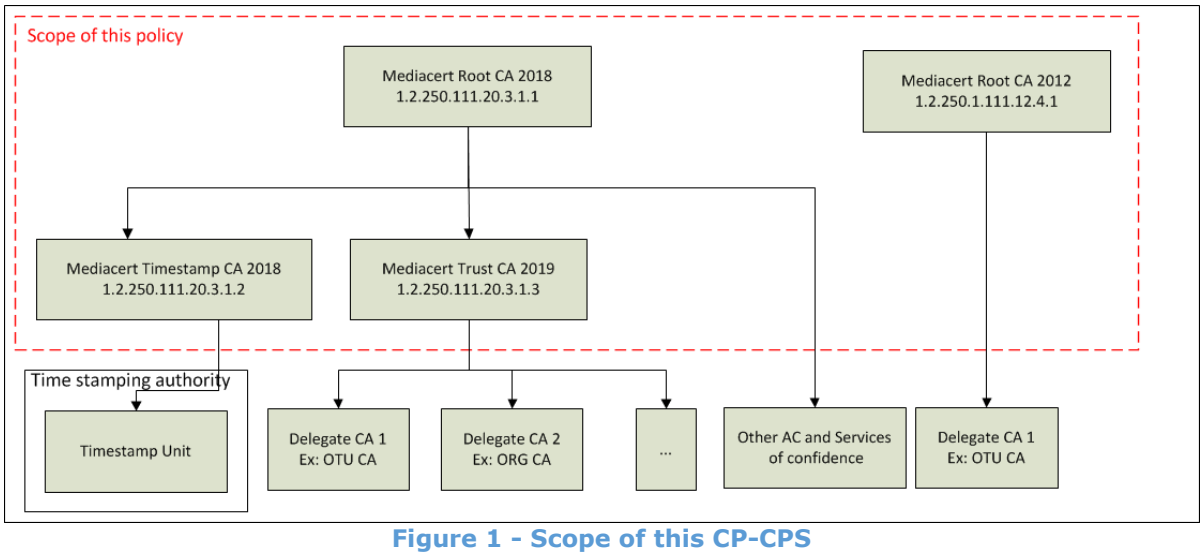

Figure 1 - Scope of this CP-CPS

In this context, this document presents:

- the requirements to which each of these offline CAs operated by the MediaCert TSP are subject;
- the organization set up to ensure the provision of services;

- the security measures applied.

In addition, as MediaCert TSP's Trust Services, all requirements and practices from the [GP] are, unless otherwise stated, applicable to the scope of these offline CAs.

These are both operated in an offline environment.

"MediaCert Timestamp CA 2018" and the "MediaCert Trust CA 2019" aim to comply with the requirements of standard [ETSI 319 411-2] for the QCP level.

"MediaCert Root CA 2018" and "MediaCert Root CA 2012" are operated under similar operating conditions but do not aim for specific compliance.

1.2 Document identification

This document is the certification policy of the offline CA.

Elements	Value
Title	Offline CAs Certification Policy - Certification Practices Statements
Document reference	WLM-TSP-F104
OID	1.2.250.1.111.12.4.1 for Root CA 2012 1.2.250.1.111.20.3.1.1 for MediaCert Root CA 2018 1.2.250.1.111.20.3.1.2 for the Time-stamping CA 1.2.250.1.111.20.3.1.3 for MediaCert Trust CA 2019
Version	1.3
Author	F. Lesecq

The OIDs in this document are based on the OID "**1.2.250.1.111.20.3**": 1.2.250.1.111.20.3**.z.w** where:

- z: major version of this policy (e. g. version 3.1 → 3);
- w: specification of the CAs concerned by this CP-CPS with:
    - MediaCert Root CA 2018 → w=1;
    - CA Time-stamping → w=2;
    - MediaCert Trust CA 2019 → w=3.

The number 1.2.250.1.111 has been assigned by AFNOR to Worldline as the OID root under which the OIDs of the various CAs are declined.

The Root CA 2012 OID is of the form 1.2.250.1.111.x.y.z where x, y and z are:

- x: year of creation of the Certification Authority: 2012 => 12;
- y: number assigned to the Certification Authority by Worldline after the year of creation;
- z: major version of the PC.

The OID assigned to this CA is: 1.2.250.1.111.12.4.1.

Further information is available in the General Policy [GP].

This document will be referred to as "CP-CPS" throughout the document.

Unless otherwise specified, the requirements of this document are applicable to these four (4) CAs.

The requirements applicable to a subset of ACs are preceded by the mention:

- [Root 2012] for MediaCert Root CA 2012 with the OID 1.2.250.1.111.12.4.1 ;
- [Root 2018] for MediaCert Root CA 2018 with the OID 1.2.250.1.111.20.3.1.1 ;
- [Time-stamping] for the Time-stamping CA with the OID 1.2.250.1.111.20.3.1.2;
- [Trust] for MediaCert Trust CA 2019 with the OID 1.2.250.1.111.20.3.1.3.

1.3 Entities involved in the PKI

1.3.1 Certification Authority

The CA is responsible for providing certificate management services throughout their life cycle (generation, distribution, renewal, revocation, etc.) and relies on a technical infrastructure for this purpose: a Key Management Infrastructure (PKI). The CA's services are the result of different functions that correspond to the different stages of the life cycle of Key pairs and Certificates. For the purposes of this document, we are only interested in CAs operated offline by MediaCert TSP. These authorities aim to provide Certificates to the other Trust Services operated by MediaCert TSP.

1.3.2 Registration Authority

The Registration Authority is the component of the PKI in charge of identifying Holders. For CAs within the scope of this CP-CPS, MediaCert TSP operates its own Registration Authority and will only register Trust Services operated by MediaCert TSP as Holders.

1.3.3 Certificate Holders

For the purposes of this CP-CPS, the Certificate Holder is:

- [Root 2012] [Root 2018] a trust service of the MediaCert TSP certified by the Root CA such as a Certification Authority dedicated to time-stamping or any other Intermediate Certification Authority;
- [Time-stamping] a Time-stamping Unit operated by the Time-stamping Service of the MediaCert TSP.
- [Trust] A Certification Authority operated by TSP MediaCert.

The Holder is not, in each case, a natural person. The Holder will be identified in the subject line of the Certificate through:

- the Trust Service name;

- [Root 2012][Root 2018] the name of the CA as a common name;
- [Timestamp] the name of the Time-stamping Unit;
- [Trust] name of delegate CA
- the organization that can only be "Worldline".

To carry out the request, the Certificate Holder will be represented by a natural person, the Certificate Manager, duly mandated.

1.3.4 Certificate Users

Users check the validity of the Certificate using:

- the information contained in the Certificate (validity date, etc.) ;
- additional information provided by the CA (Certificate revocation status).

1.3.5 Other participants

Not applicable.

1.4 Use of certificates

1.4.1 Applicable fields of application

The use of Certificates differs for each CA.

The Certificates described in this CP-CPS are intended exclusively for internal use by MediaCert TSP. Therefore, Test Certificates are not issued for third parties. MediaCert TSP does not plan to issue Test Certificates from production environments for offline CAs.

[Root 2012][Root 2018] Certificates issued by the Root CA are only intended to certify the Trust Services offered by MediaCert TSP or CAs offered by the TSP MediaCert.

[Time-stamping] Certificates issued by the Time-stamping CA of MediaCert TSP are only dedicated to Time-stamping Units operated by the Time-stamping Authority (TSA) of MediaCert TSP for sealing operations and issuing time-stamping tokens.

[Trust] The Certificates issued by this CA are only intended to certify CAs operated by the TSP MediaCert.

1.4.2 Areas of prohibited use

Any use other than that defined in the previous paragraph is prohibited by this CP-CPS. In addition, the Certificate must be used within the limits of the laws and regulations in force (see chapter 9.14).

1.5 CP management

1.5.1 Entity managing the policy

The entity managing this policy is indicated in the [GP].

1.5.2 Point of contact

The contact point is indicated in the [GP].

1.5.3 Entity determining the compliance of CP practices

This entity is described in the [GP].

1.5.4 Procedure for approving the conformity of the CP-CPS

The procedure for approving this CP-CPS is described in [GP].

1.6 Definition and abbreviations

1.6.1 Definitions of the terms

A list of the main definitions of the technical terms used in this CP-CPS is provided below:

Subscriber: an entity/organization that benefits from one or more Trusted Services provided by MediaCert TSP.

Key pair: pair composed of a private key (to be kept secret) and a public key, necessary for the implementation of a cryptography service based on asymmetric algorithms (RSA for example).

Certificate: X509 standard data element used to associate a public key with its holder. A Certificate contains data such as the identity of the holder, his public key, the identity of the organization that issued the Certificate, the validity period, a serial number, a *thumbprint* or the criteria for use. The whole is signed by the private key of the Certification Authority that issued the Certificate.

Certification Service: service that produces Certificates and, more generally, manages them (manufacturing, delivery, revocation, publication, logging, archiving) in accordance with a certification policy.

Trust Service: a trust service is an electronic service that consists of:

- the issuance of Certificates of electronic signature, electronic stamp and website authentication; or
- the validation of electronic signatures and stamps; or
- the storage of electronic signatures and electronic stamps;
- electronic time stamping;
- electronic registered mail.

Time-stamping Service: service that produces time-stamps and more generally ensures their management in accordance with a time-stamping policy.

Holder / Bearer: refers to an entity, a natural or legal person, for which the Certificate issued by one of the Certification Authorities governed by this policy is intended.

User: refers to an entity, whether a natural person or a legal entity, that uses Certificates issued by CAs governed by this CP-CPS to verify their validity and any link with the signed data.

1.6.2 Acronyms

A list of acronyms used in this CP-CPS is provided below:

- **CA:** Certification Authority;
- **ICA:** Intermediate Certification Authority;
- DCA : Delegate Certification Authority
- **AFNOR:** French Standards Association;
- **TSA:** Time-stamping Authority;
- **CSR:** Certificate Signing Request;
- **DN:** Distinguished Name;
- **TDGP:** Technical Documentation of General Practices;
- **EIDAS:** Electronic IDentification And Signature;
- **HSM:** Hardware Security Module;
- **PKI:** Public Key Infrastructure;
- **CRL:** List of Revoked Certificates;
- **OID:** Object IDentifier;
- **CP-CPS:** Certification Policy - Certification Practices Statements;
- **TP-TPS:** Time-stamping Policy - Declaration of Time-stamping Practices ;
- **BCP:** Continuity and Business Resumption Plan ;
- **GP:** General Policy of the MediaCert TSP;
- **ISP:** Worldline's Information Security Policy;
- **GDPR:** General Data Protection Regulations ;
- **SIEM:** Security Information & Event Management ;
- **SOC:** Security Operation Center ;
- **ISS**: Information Systems Security;
- **TSP**: Trust Service Provider ;
- **TSU**: Time Stamping Unit.

1.7 References

1.7.1 Regulations and regulations

Reference	Description
[CNIL]	Law n°78-17 of 6 January 1978 relating to data processing, files and freedoms, amended by law n°2004-801 of 6 August 2004 Note: These regulations will be replaced in 2018 by [GDPR].
[EIDAS]	REGULATION (EU) No 910 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[GDPR]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

1.7.2 Technical regulatory references

Reference	Description
[ETSI 119 312]	ETSI TS 119 312 v1.2 (2018-09) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI 319 411-1]	ETSI EN 319 411-1 v1.2.2 (2018-04) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI 319 411-2]	ETSI EN 319 411-2 v2.2.2 (2018-04) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ISO 27001 : 2013]	ISO/IEC 27001 : 2013 Information technology - Security techniques - Information security management systems - Requirements
[ISO 27002 : 2013]	ISO/IEC 27002 : 2013 Code of good practice for safety management of information
[RFC 3647]	Network Working Group - November 2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RGS B1]	General Safety Standard v2.0 - Appendix B1 (2014-02) National Agency for Information Systems Security (ANSSI) Cryptographic mechanisms: rules and recommendations for the selection and sizing of cryptographic mechanisms

1.7.3 MediaCert TSP repository

Reference	Description
[GP]	General Policy of the MediaCert TSP MediaCert TSP Reference: WLM-TSP-F094 OID: 1.2.250.1.111.20.1.1

2 Responsibilities for the provision of information to be published

2.1 Entity responsible for making information available

The entity described in the [GP] document in the corresponding chapter is the entity responsible for making available the information to be published described in chapter 2.2 of this document. The publication site is described in the [GP].

2.2 Information to be made available

Within the scope of this document, the information published is as follows:

- this CP-CPS;
- the List of Certificates of Certification Authority Revoked (LAR) by the Root CA;
- the List of Certificates Revoked (LCR) by each CA;
- the valid CA Certificate for each CA;

This CP-CPS is published in PDF/A format.

2.3 Publication deadlines and frequencies

All requirements and practices described in the [GP] in the corresponding chapter apply. The specific additional requirements and practices of this section also apply.

Certification policies are updated and published in the event of major changes and at least every two (2) years.
Root CA Certificates are released or put online prior to any release of Intermediate CA Certificates or LARs.
Time-stamping CA Certificates are issued or posted online prior to any issuance of Time-stamping Unit Certificates or CRL.

2.4 Access control to published information

All requirements and practices described in the [GP] in the corresponding chapter apply.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The names used in a Certificate are described according to [ISO/IEC 9594] *(Distinguished Name*), each Holder having a distinct name (DN).

3.1.2 Need to use explicit names

The names to distinguish the Holders are explicit. The distinctive name is in the form of a string of type UTF8string of type name X.501.

The profiles of the Certificates are described in chapter 7.1.

3.1.3 Anonymization or pseudonymization of bearers

The Certificates covered by this CP-CPS may under no circumstances be anonymous. The names provided for the issuance of a Certificate may under no circumstances be pseudonyms.

3.1.4 Rules for the interpretation of the different forms of names

The name of the CA is defined by the MediaCert Committee.

3.1.5 Uniqueness of names

An added distinctive code ensures the uniqueness of the DN in case of homonymy. This code corresponds to the year in which the CA Certificate begins to be valid.

In the case of a CA Certificate to be generated with the same valid-from date, a unique additional index is added (2018-1, 2018-2 for example).

[Time-stamping] A unique identifier ensures the uniqueness of the CN of the Certificate of Time-stamping Units.

3.1.6 Identification, authentication and role of trademarks

For trademarks, company names or other distinctive signs, MediaCert TSP does not carry out any prior art searches or other verifications. It is the responsibility of the applicant or the Holder to verify that the requested name does not infringe the property rights of third parties.

3.2 Initial validation of identity

The registration of a future Holder is done directly with the RA by a natural person.

The request is made in accordance with the definition in chapter 4.1.

3.2.1 Method for proving possession of the private key

[Root 2012][Root 2018] The applicant submits a signed CSR with the private key of the relevant Intermediary CA or Trusted Service concerned.

[Time-stamping] The requester submits a signed CSR with the private key of the TSU concerned.

[Trust] The requester presents a CSR signed with the private key of the relevant delegate CA.

3.2.2 Validation of the identity of an organization

As defined in chapter 3.2.5 only the MediaCert TSP is the recipient of Certificates issued under this CP-CPS.

3.2.3 Validation of an individual's identity

The identity of an individual authorized to make a Certificate creation request under this CP-CPS is ensured by the fact that he/she operates one of the following trusted roles within MediaCert TSP:

- Head of the TSP;
- Deputy Head of the TSP.

The identity of the applicant is verified in particular when the Certificate application is submitted via a physical face-to-face meeting (see chapter 4.1.2).

[Root] The validation of the applicant's identity is carried out during the preparation phase of the Intermediate CA key ceremony.

[Time-stamping] The validation of the applicant's identity is carried out during the preparation phase of the TSU key ceremony.

[Trust] The validation of the identity of the applicant is carried out during the preparation phase of the delegate CA key ceremony.

3.2.4 Unaudited information of the holder

This CP-CPS does not make any specific requirements on this subject.

3.2.5 Validation of the applicant's authority

[Root 2012][Root 2018] This version of the CP-CPS only contemplates the issuance of Certificates to Intermediate CAs operated by MediaCert TSP. As a result, no particular verification is made. Only the MediaCert TSP is authorized to apply for an Intermediate CA Certificate.

[Time-stamping] This version of the CP-CPS only envisages the issuance of Certificates to TSUs operated by MediaCert TSP. As a result, no particular verification is made. Only the MediaCert TSP is authorized to apply for a TSU Certificate.

[Trust] This version of the CP-CPS only envisages issuing Certificates to CA Daughters operated by the TSP MediaCert. Therefore, no particular verification is made. Only the TSP MediaCert is authorized to apply for a CA Delegate Certificate.

3.2.6 CA Cross Certification

Not applicable.

3.3 Identification and validation of a key renewal request

A new Certificate cannot be provided without renewal of the corresponding key pair. The renewal then results in a new Certificate application and benefits from the same procedures as for an initial application (see chapter 3.2 this CP-CPS).

3.3.1 Identification and validation for a current renewal

The procedure is identical to an initial request.

3.3.2 Identification and validation for renewal after revocation

The procedure is identical to an initial request.

3.3.3 Identification of a revocation request

[Root 2012][Root 2018] The request for key revocation for an Intermediate CA signed by the Root CA can only be made by an authorized person and is formally validated before taking into account. The Root CA Certificate being a self-signed Certificate, it cannot be revoked. In the event of compromise of the private key corresponding to the Root CA Certificate, the MediaCert TSP will carry out all the actions planned in the event of compromise (see chapter 5.7.3).

[Time-stamping][Trust] The request for key revocation can’t only be made by an authorised person and is formally validated before it is taken into account (see chapter 4.9).

4 Operational requirements for the certificate life cycle

4.1 Certificate request

4.1.1 Origin of a certificate request

The Certificate applicant is the MediaCert TSP, represented by the Head of the MediaCert TSP or one of his deputies (see chapter 3.2.3).

4.1.2 Process and responsibilities for preparing a certificate application

The establishment of a Certificate application must be established by the future Holder. This request must contain the Certificate creation request form, signed by the applicant and submitted face-to-face to MediaCert TSP.

4.2 Processing a certificate request

4.2.1 Execution of the identification and validation processes of the request

The identification and validation of the request is processed during the preparation phase of the Key Ceremony by the Head of the MediaCert TSP or one of his deputies (see chapter 3.2.3). This person cannot be the same person as the one who made the request.

The identification and validation of the request is carried out as follows:

- the physical identity of the applicant and his authority shall be verified in accordance with the requirements of chapter 3.2;
- the addressee of the request (see paragraph above) checks that the application file (see chapter 4.1.2) is complete. In particular, the Terms and Conditions in effect at the time of the request are signed by the MediaCert TSP.

The RA then keeps a record of the Certificate applications submitted (see chapter 5.4.1).

4.2.2 Acceptance or rejection of the request

If the application is rejected, the person who processed the application shall inform the applicant and give reasons.

4.2.3 Duration of the certificate preparation

The CA shall endeavour to process the Certificate application within a reasonable time. However, there are no restrictions on the maximum or minimum processing time.

4.3 Issuance of the certificate

4.3.1 Actions by the CA regarding the issuance of the certificate

The validation of the request triggers the technical operation of generating the Certificate. This contains the following actions:

- verification that the Certificate request comes from a trusted member of the MediaCert TSP authorized by this CP-CPS to make a Certificate request;
- generation of the CSR;
- technical verification of the CSR;
- submission of the CSR to the CA and generation of the Certificate;
- verification of the Certificate;
- issuance of the Certificate.

4.3.2 Notification by the CA of the issuance of the Bearer Certificate to the holder

The Certificate Holder is notified via an internal Worldline application.

4.4 Acceptance of the certificate

4.4.1 Procedure for accepting the certificate

The acceptance of the Certificate signed by the CA is recorded on the minutes of the key ceremony.

4.4.2 Publication of the certificate

The Certificate is published on the publication site (see chapter 2.2) before any use in production of the associated private key.

4.4.3 Notification by the CA to other entities of the issuance of the certificate

Not applicable.

4.5 Use of the key pair and certificate

4.5.1 Use of the private key

4.5.1.1 CA Private Key

[Root 2012][Root 2018] The private key of the Root CA is used for:

- sign its own Root CA Certificate (self-signed certificate);
- sign Intermediate CA Certificates or other Trust Services;
- sign the list of revoked Intermediate CAs (LARs).

[Time-stamping] The private key of the Time-stamping CAs is used for:

- sign the TSU Certificates;
- sign the list of revoked TSUs (CRL).

[Trust] The CA private key is used to:

- sign the CA delegate Certificates;
- sign the list of CA delegate revoked (LAR).

These uses are explicitly defined in the certificate extensions.

4.5.1.2 Private key of the holders

[Root 2012][Root 2018] The intermediate CA private key, associated with a Certificate issued by the Root CA, is intended for :

- sign the Certificates of the final Holders;
- sign the list of revoked Certificates (CRL), if applicable;
- sign OCSP Responder Certificates, if applicable.

[Time-stamping] The TSU private key, associated with a Certificate issued by the Time-stamping CA, is intended to sign Time-stamps. These uses are explicitly defined in the certificate extensions.

[Trust] The delegate CA private key, associated with a Certificate issued by the Intermediate CA is intended for:

- sign the Certificates of final holders;
- sign the list of revoked certificates (CRL), if applicable;
- sign OCSP Responder Certificates, if applicable.

4.5.2 Use of public key and certificate

4.5.2.1 Public Key and CA Certificate

[Root 2012][Root 2018] The Root CA Certificate is used for:

- verify the integrity of the Root CA public key (self-signed certificate);
- verify the origin and integrity of Intermediate CA Certificates;
- verify the origin and integrity of the LARs issued;

[Time-stamping] The Time-stamping CA Certificate is used for:

- verify the origin and integrity of TSU Certificates;
- verify the origin and integrity of the list of revoked TSUs (CRUs);

[Trust] The Intermediate CA Certificate is used to:

- verify the origin and integrity of the Certificates of the delegate CAs;
- verify the origin and integrity of the LARs issued;

4.5.2.2 Holders' certificates

[Root 2012][Root 2018] The Intermediate CA Certificates issued by Root CAs are intended for:

- validate the Certificates of the final Holders;
- validate the list of revoked Certificates (CRL), if applicable;
- validate OCSP Answering Machine Certificates, if applicable.

[Time-stamping] TSU Certificates, issued by the Time-stamping CA, are intended to validate the time-stamps produced by TSUs.

[Trust] The delegate CA Certificates issued by the 2019 AC Mediacert Trust CA are intended for:

- validate the certificates of final holders;
- validate the list of revoked certificates (LCR), if applicable;
- validate the OCSP responder certificates, if applicable.

4.6 Renewal of a certificate

The notion of renewal of a Certificate, within the meaning of [RFC 3647], corresponding only to the modification of validity dates, is not permitted by this CP-CPS. Only the issuance of a new Certificate following a change of the key pair is authorized.

4.6.1 Possible reasons for renewing a certificate

Not applicable.

4.6.2 Origin of a renewal request

Not applicable.

4.6.3 Procedure for processing a renewal request

Not applicable.

4.6.4 Notification to the bearer of the establishment of the new certificate

Not applicable.

4.6.5 Acceptance procedure for the new certificate

Not applicable.

4.6.6 Publication of the new certificate

Not applicable.

4.6.7 Notification by the CA to other entities of the issuance of the new certificate

Not applicable.

4.7 Issuance of a new Certificate following the change of the key pair

In accordance with [RFC 3647], this chapter deals with the issuance of a new Bearer Certificate related to the generation of a new Key pair.

4.7.1 Possible causes for changing a key pair

The keys must be periodically renewed in order to minimize the possibility of cryptographic attacks.

In addition, a Key pair and a Certificate may be renewed in advance, following the revocation of the Holder's Certificate (see chapter 4.9, in particular chapter 4.9.1 for the various possible reasons for revocation).

[Root 2012][Root 2018] The corresponding ICA Key pairs and Certificates will be renewed at least every ten (10) years.

[Time-stamping] The TSU key pairs will be renewed at least every year.

[Trust] The AC delegate Bi-keys will be renewed at least every ten (10) years.

4.7.2 Origin of a request for a new certificate

[Root 2012][Root 2018] The request for a new Certificate is at the initiative of the Intermediate CA.

[Time-stamping] The request for a new Certificate is at the initiative of the TSA.

[Trust] The request for a new Certificate is at the initiative of the delegate CA.

4.7.3 Procedure for processing an application for a new certificate

The procedure is identical to the initial request. The identification and validation of a request for a new Certificate is specified in chapter 4.2 above. For CA actions, refer to chapter 4.3.1.

4.7.4 Notification to the bearer of the establishment of the new certificate

The procedure is identical to the initial request (see chapter 4.3.2).

4.7.5 Acceptance procedure for the new certificate

The procedure is identical to the initial request (see chapter 4.4.1).

4.7.6 Publication of the new certificate

The procedure is identical to the initial request (see chapter 4.4.2).

4.7.7 Notification by the CA to other entities of the issuance of the new certificate

The procedure is identical to the initial request (see chapter 4.4.3).

4.8 Amendment of the certificate

This CP-CPS does not authorize the modification of a Certificate. The said Certificate will have to be revoked and then reapplied to the CA.

4.8.1 Possible reasons for modifying a certificate

Not applicable.

4.8.2 Origin of a request to modify a certificate

Not applicable.

4.8.3 Procedure for processing a request to amend a certificate

Not applicable.

4.8.4 Notification to the holder of the establishment of the amended Certificate

Not applicable.

4.8.5 Acceptance procedure for the amended Certificate

Not applicable.

4.8.6 Publication of the amended Certificate

Not applicable.

4.8.7 Notification by the CA to other entities of the issuance of the amended Certificate

Not applicable.

4.9 Revocation and suspension of certificates

4.9.1 Possible causes for revocation

[Root 2012][Root 2018] There may be several reasons for revoking a Certificate from an Intermediate CA:

- the information of an ICA contained in its Certificate is no longer correct;
- the Certificate no longer complies with the CP-CPS to which it is subject;
- the ICA has not complied with the applicable terms and conditions for use of the Certificate;
- the ICA has not met its obligations under this CP-CPS;
- an error (intentional or unintentional) has been detected in the ICA registration file;
- the private key of the ICA is suspected of being compromised, compromised, lost or stolen (possibly the associated activation data);
- the ICA explicitly requests the revocation of the Certificate (in particular in the case of destruction or alteration of the holder's private key and/or its carrier);
- the cryptography used no longer ensures the connection between the subject and the public key;
- termination of ICA activities;
- termination of this CA.

[Time-stamping] There may be several reasons for revoking a TSU's Certificate:

- the information of a TSU contained in its Certificate is no longer correct;
- the Certificate no longer complies with the CP-CPS to which it is subject;
- the ICA has not complied with the applicable terms and conditions for use of the Certificate;
- the ICA has not complied with its obligations under this CP-CPS;
- an error (intentional or unintentional) has been detected in the TSA registration file;
- the TSU private key is suspected of being compromised, compromised, lost or stolen (possibly the associated activation data);
- the ICA explicitly requests the revocation of the Certificate (in particular in the case of destruction or alteration of the TSU's private key and/or its carrier);
- the cryptography used no longer ensures the connection between the subject and the public key;
- termination of the ICA's activities;
- termination of this CA.

[Trust] There can be several causes for the revocation of a delegate’s CA Certificate:

- the information of an DCA appearing in its Certificate is no longer correct;
- the Certificate no longer conforms to the CP-CPS to which it is subject;
- the DCA has not complied with the applicable conditions for using the Certificate;
- DCA has not complied with its obligations arising from this PC-DPC;
- an error (intentional or not) was detected in the DCA registration file;
- the DCA private key is suspected of being compromised, is compromised, is lost or is stolen (possibly the associated activation data);
- the DCA explicitly requests the revocation of the Certificate (in particular in the case of destruction or alteration of the bearer's private key and / or its medium);
- the cryptography used no longer ensures the link between the subject and the public key;
- cessation of DCA activity;
- cessation of activity of this CA.

For all CAs governed by this CP-CPS, when one of the above circumstances occurs and the CA concerned becomes aware of it (it is informed or obtains the information during one of its audits, in particular when a new Certificate is issued), the relevant Certificate must be revoked.

4.9.2 Origin of a revocation request

[Root 2012][Root 2018][Trust] A request for revocation of an ICA Certificate can only be made by:

- the person in charge of the MediaCert TSP or one of his deputies;
- a legal representative of the entity operating the CA, or a person mandated by it;
- by the judicial authorities through a court decision.

[Time-stamping] A request for revocation of a TSU Certificate can only be made:

- the person in charge of the MediaCert TSP or one of his deputies;
- a legal representative of the entity operating the ICA, or a person authorised by it;
- by the judicial authorities through a court decision.

4.9.3 Procedure for processing a revocation request

A Certificate revocation request received by the CA must contain at least the following information:

- the serial number of the Certificate to be revoked;
- the name associated with the Certificate to be revoked (full DN);
- the name and capacity of the applicant for revocation;

- the cause of revocation.

The request is then, upon receipt, authenticated and controlled by the CA. The CA then forwards the corresponding request to the revocation management function, which then proceeds with the revocation and communicates this new status to the Certificate status information function.

4.9.4 Period allowed to the holder to formulate the request for revocation

As soon as the Holder becomes aware that one of the possible causes of revocation referred to in chapter 4.9.1 is effective, he or she must formulate the revocation request without delay.

4.9.5 Time for the CA to process a revocation request

The maximum processing time for a request to revoke a Certificate is 24 hours.

4.9.6 Requirements for verification of revocation by certificate users

The user of a Certificate is required to check, before use, the status of the corresponding Certificate chain up to the Root CA Certificate. For this purpose, it may use the last published revocation status.

4.9.7 Frequency of LAR/LCR establishment

[Root 2012][Root 2018][Trust] LARs are generated every six (6) months. They are valid for one (1) year.

[Time-stamping] CRLs are pre-generated every year. They are published every twenty-four (24) hours. They are valid for seven (7) days.

4.9.8 Maximum time limit for publication of LAR/LCRs

The LARs and CRLs shall be published as soon as possible after the date of establishment. The maximum publication time for CRLs will be sixty (60) minutes.

4.9.9 Availability of an online system for checking the revocation and status of certificates

Not applicable.

4.9.10 Online verification requirements for certificate revocation by certificate users

Not applicable.

4.9.11 Other available means of information on revocations

Not applicable.

4.9.12 Specific requirements in the event of compromise of the private key

For Certificates issued, in addition to the requirements of chapter 4.9.3, revocation following a compromise of the private key shall be notified to the inspection body within twenty-four (24) hours in accordance with the requirements of [eIDAS].

4.9.13 Possible causes of a suspension

Suspension of Certificates is not permitted in this CP-CPS.

4.9.14 Origin of a request for suspension.

Not applicable.

4.9.15 Procedure for processing a request for suspension

Not applicable.

4.9.16 Limits on the period of suspension of a certificate

Not applicable.

4.10 Revocation and suspension of certificates

4.10.1 Operational characteristics

The MediaCert TSP provides Certificate users with information to verify and validate, prior to its use, the status of a Certificate and the entire corresponding certification chain (up to and including the Root CA), i.e. to also verify the signatures of the chain's Certificates, signatures guaranteeing the origin and integrity of the CRL/LARs and the status of the Root CA Certificate.

CRL/LARs are published at the address specified in the [GP]. This address is available in particular within the Certificates issued.

[Time-stamping] A CRL contains a list of revoked Time-stamping Unit Certificates, whether expired or not. It contains in particular the date of its issue and the date of issue of the next CRL.

4.10.2 Availability of the function

The Certificate status information function is available 24 hours a day, 7 days a week. This function has a maximum downtime of eight (8) hours due to a service interruption (failure or maintenance).

4.10.3 Optional devices

This CP-CPS does not make any specific requirements on this subject.

4.11 End of the relationship between the holder and the CA

In the event of termination of the contractual/hierarchical/regulatory relationship between the issuing CA and the holder prior to the expiry of the certificate, for any reason, the certificate must be revoked.

4.12 Key escrow and recovery

The private keys of the porters are not sequestered by the CA.

4.12.1 Key escrow collection policy and practices

Not applicable.

4.12.2 Session key encapsulation recovery policy and practices

Not applicable.

5 Non-technical security measures

5.1 Physical security measures

5.1.1 Geographical location and site construction

All requirements and practices described in the [GP] apply.

In particular, all premises hosting systems involved in the generation and revocation of Certificates are operated in an environment that physically protects services from threats of compromise due to unauthorized access to systems or data. The perimeter of the secure area is clearly identified and cannot be accessed by unauthorized personnel or third party organizations.

5.1.2 Physical access

All requirements and practices described in the [GP] apply.

5.1.3 Power supply and air conditioning

All requirements and practices described in the [GP] apply.

5.1.4 Vulnerability to water damage

All requirements and practices described in the [GP] apply.

5.1.5 Fire prevention and protection

All requirements and practices described in the [GP] apply.

5.1.6 Conservation of the supports

All requirements and practices described in the [GP] apply.

5.1.7 Decommissioning of supports

All requirements and practices described in the [GP] apply.

5.1.8 Off-site backups

All requirements and practices described in the [GP] apply.

5.2 Procedural security measures

5.2.1 Trusted roles

All requirements and practices described in the [GP] apply.

5.2.2 Number of people required per task

All requirements and practices described in the [GP] apply.

5.2.3 Identification and authentication for each role

All requirements and practices described in the [GP] apply.

5.2.4 Roles requiring segregation of duties

All requirements and practices described in the [GP] apply.

5.3 Security measures for staff

5.3.1 Required qualifications, skills and authorizations

All requirements and practices described in the [GP] apply.

5.3.2 Background check procedures

All requirements and practices described in the [GP] apply.

5.3.3 Initial training requirements

All requirements and practices described in the [GP] apply.

5.3.4 Continuing education requirements and frequency

All requirements and practices described in the [GP] apply.

5.3.5 Frequency and sequence of rotation between different allocations

All requirements and practices described in the [GP] apply.

5.3.6 Sanctions in the event of unauthorized actions

All requirements and practices described in the [GP] apply.

5.3.7 Requirements for the staff of external service providers

All requirements and practices described in the [GP] apply.

5.3.8 Documentation provided to staff

All requirements and practices described in the [GP] apply.

5.4 Procedure for compiling audit data

5.4.1 Type of events to be recorded

All requirements and practices described in the [GP] apply.

In addition to the events described in the |GP], this policy requires CAs within its scope to collect the following audit data:

- all security-related events, in particular:
    - changes in system security policy;
    - system starts and stops;
    - hardware and software failures;
    - attempts to access systems.
- all events relating to the registration of holders, in particular:
    - receipt of a Certificate application (initial and renewal);
    - validation / rejection of a Certificate request;
    - events related to signature keys and CA Certificates (generation (key ceremony), backup / recovery, revocation, renewal, destruction, etc.) ;
    - generation of Certificates for Holders;
    - publication and updating of CA-related information (CP-CPS, CA certificates, general conditions of use, etc.);
    - receipt of a revocation request;
    - validation / rejection of a revocation request;
    - generation and publication of LAR and LCR.

Regarding the registration procedure, the CA also keeps:

- the identity of the person in a trusted role who applied for the Certificate;
- the original of the Certificate application form;
- the identity of the person in a trusted role who made the recording.

As the CA is operated off-line, the requirements on the activity of network elements are only applicable to the publication function.

As the registration file contains the Holder's personal data, storage is subject to security measures in accordance with chapter 9.4 this document.

5.4.2 Frequency of event log processing

CA event logs are not processed because they are offline.

5.4.3 Event log retention period

Event logs intended to be kept are archived. The archiving period for this information is specified in chapter 5.5.2 this document.

5.4.4 Protection of event logs

Event logs are protected under the same conditions as those defined in chapter 5.5.3 this document.

5.4.5 Procedure for saving event logs

The procedure for backing up CA event logs is internal and specified in the TDCP document.

5.4.6 Event log collection system

The collection system for CA event logs is internal and specified in the TDCP document.

5.4.7 Notification of the recording of an event to the event manager

All requirements and practices described in the [GP] apply.

5.4.8 Vulnerability assessment

Vulnerabilities are assessed during a risk analysis (see chapter on risk analysis in the [GP]). The control of functional event logs is carried out on demand in the event of a dispute, or for analysis of the PKI's behaviour.

5.5 Data Archiving

Archiving arrangements are put in place by the CA. This archiving ensures the durability of the journals compiled by the various components of the PKI.

5.5.1 Types of data to be archived

The data to be archived are as follows:

- software (executable) and configuration files of computer equipment;
- CP-CPSs;
- TDCPs;
- registration files;
- the Certificates issued;
- LARs and CRLs issued or published;

- the various commitments signed by the MediaCert Committee;
- the event logs of the different PKI entities (see chapter 5.4.1).

5.5.2 Archive retention period

The minimum retention periods are as follows:

Retention period	Data
5 years after the end of the CA's life	• software (executable) and configuration files of computer equipment; • CP-CPSs; • TDCPs; • the Certificates issued; • LARs and CRLs issued or published; • the various commitments signed by the MediaCert Committee.
7 years after the expiry of the associated Certificate	• registration files; • the elements of the Certificate life cycle (generation, revocation,...).
10 years after their generation	Other audit data (e.g. system start-ups and shutdowns)

5.5.3 Protection of archives

The means of archive protection implemented by MediaCert TSP as part of its offline CAs differ according to the type of data.

Digital archives are protected by secure physical systems such as safes or strong cabinets whose accesses are controlled and protected in the same way as the activation data of CA private keys (see chapter 6.4.2).

Digital documentary archives are protected by a digital safe whose access is controlled by MediaCert TSP.

Handwritten archives are protected by secure physical systems such as safes or strong cabinets, access to which is controlled by MediaCert TSP.

5.5.4 Archive backup procedure

Archive backup procedures are internal and are specified in the TDCP document.

5.5.5 Data time stamping requirements

The clock of the CA systems is synchronized with a defined time source within the TDCP. This synchronization is performed before each use of these systems.

5.5.6 Archive collection system

The CA event archive collection system is internal and is specified in the TDCP document.

5.5.7 Procedures for retrieving and verifying archives

The procedure for retrieving CA archives is internal and is specified in the TDCP document. Access to the archives is subject to restrictions (see chapter 6.4.2).

The archives will be made available in case of judicial requisition.

5.6 CA key change

The CA may not generate a Certificate with an end date later than the expiry date of the corresponding CA Certificate. For this purpose, the period of validity of the CA Certificate must be longer than that of the Certificates it signs.

With regard to the expiry date of this Certificate, its renewal will be requested within a period at least equal to the lifetime of the Certificates signed by the corresponding private key.

As soon as a new CA key pair is generated, only the new private key will be used to sign Certificates.

The previous Certificate remains usable to validate Certificates issued under this key until all Certificates signed with the corresponding private key have expired.

5.7 Recovery from compromise and disaster

5.7.1 Procedures for reporting and handling incidents and compromises

All requirements and practices described in the [GP] apply.

In the case of a major incident, such as loss, suspicion of compromise, compromise, theft of the CA private key, the triggering event is the recognition of this incident at the PKI level. The person in charge of the MediaCert TSP must be informed immediately. He will then have to ensure that the anomaly is treated. If he considers that the incident is of a serious nature, he will request an immediate revocation of the Certificate. If this occurs, it will publish the information of revocation of the Certificate in the greatest urgency, or even immediately. It will do so via the MediaCert TSP public website and/or via e-mail notification to all customers. If any of the algorithms, or associated parameters, used by the CA or its bearers become insufficient for its remaining intended use, then the Head of the MediaCert TSP will publish the information via the public site and notify all of its affected customers by email. All relevant Certificates will then be revoked.

5.7.2 Recovery procedures in case of corruption of IT resources (hardware, software and/or data)

MediaCert TSP has a business continuity plan (see chapter 5.7.4) to meet the availability requirements of the various PKI functions arising from this CP-CPS, the CA's commitments in its own CP-CPS, in particular with regard to functions related to the publication and/or revocation of certificates. This plan is tested at least once every two (2) years.

5.7.3 Recovery procedures in case of compromise of a component's private key

The compromise of an infrastructure or component control key is treated as a disaster in the component's continuity plan (see chapter 4.7.2).

In the event of compromise of an Intermediate CA or TSU key, the corresponding Certificate will be immediately revoked: see chapter 4.9.
In the event of a compromise of the Root CA key, the MediaCert TSP will publicly indicate that Certificates and revocation information issued using that key may no longer be valid. The relevant Certificate will be immediately revoked: see chapter 4.9.

5.7.4 Business continuity capabilities following a disaster

All requirements and practices described in the [GP] apply.

5.8 Termination of activity affecting the CA

The cessation of activity may be total or partial (for example: cessation of activity for a given family of Certificates only).

The partial cessation of activity shall be progressive so that only the obligations referred to below are to be performed by the CA, or a third party entity that takes over the activities, upon expiry of the last Certificate issued.

In the event of a total cessation of activity, the CA or, in the event of impossibility, any entity that would be substituted for it by virtue of a law, regulation, court decision or agreement previously concluded with such entity, shall ensure the revocation of the Certificates and the publication of the LAR / LCR in accordance with the commitments made in its CP-CPS. A cessation of activity plan is then applied by the CA concerned. This plan is regularly updated and includes the actions listed below.

The CA shall make the following arrangements in the event of separation:

- notification of affected entities;
- the transfer of its obligations to Worldline;
- managing the revocation status for unexpired Certificates that have been issued.

When the service is stopped, the CA will take the following measures:

- inform (for example by receipt) all holders of revoked or to be revoked Certificates, as well as their connecting entities if applicable;
- refrain from transmitting the private key that enabled him to issue Certificates;
- revoke its Certificate;
- revoke all the Certificates it has signed and which are still valid;
- take all necessary measures to destroy it or render it inoperative (the nominal key and any backups).

6 Technical security measures

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

6.1.1.1 CA Key

All requirements and practices described in the [GP] apply.

The specific additional requirements and practices of this section also apply.

Key ceremony

[Root 2012][Root 2018] The ceremony of generation of the keys of AC Racine is carried out in the presence of a judicial officer or a trusted person independent of the management of TSP MediaCert.

Cryptographic module

CA signature keys are generated and implemented in a cryptographic module that has been security evaluated as defined in chapter 6.2.11 this document.

6.1.1.2 Carrier key

[Time-stamping][Trust] The keys associated with Certificates issued by the CA must be generated and used in a cryptographic module that has undergone a security assessment at least EAL4 of the common criteria repository (ISO/IEC 15408) and has been qualified at the level reinforced by the ANSSI.

6.1.2 Transmission of the private key to its owner

Not applicable.

6.1.3 Transmission of the public key to the CA

The public key is transmitted internally by the trusted operator who generated it during a key ceremony.

6.1.4 Transmission of the CA public key to certificate users

[Root 2012][Root 2018] The Root CA public key is wrapped in a self-signed Root Certificate. Its distribution is accompanied by the digital fingerprint of the Certificate as well as a statement that it is indeed a public key of the Root CA. The public key of the Root CA, as well as the corresponding information (certificate, fingerprints, declaration of membership) can easily be retrieved by Certificate users via the MediaCert TSP's website (see chapter2.2).

[Time-stamping][Trust] The public key of the CA is certified by the Root CA. It is published on the MediaCert TSP's website (see chapter 2.2).

6.1.5 Key sizes

All requirements and practices described in the [GP] apply.

The specific additional requirements and practices defined below also apply.

6.1.5.1 CA key size

Scope of consolidation	Hash function	Algorithm	Size
Root CA "Mediacert Root CA 2018"	SHA256	RSA	4096 bits
AC Root « Root CA 2012 »	SHA256	RSA	4096 bits
Time-stamping CA	SHA256	RSA	4096 bits
AC intermediate « Mediacert Trust CA 2019 »	SHA256	RSA	4096 bits

6.1.5.2 Carrier key size

Scope of consolidation	Hash function	Algorithm	Size
Intermediate CA	SHA256	RSA	4096 bits
Delegate CA	SHA256	RSA	4096 bits
TSU	SHA256	RSA	2048 bits

6.1.6 Verification of the generation of key pair parameters and their quality

The Key pair generation equipment used to generate CA Key pair parameters is a cryptographic module configured to meet these requirements. The Key pairs can only be generated on a module that complies with this requirement, or at a higher cryptographic and security level.

6.1.7 Objectives of the key use

The use of a Root CA and ICA private key and the associated Certificate is strictly limited to the signing of Certificates, CRLs / LARs (see chapter 1.4).

6.2 Security measures for private key protection and cryptographic modules

6.2.1 Standards and security measures for cryptographic modules

6.2.1.1 Standards for cryptographic modules

CA signature keys are generated and implemented in a secure cryptographic module that meets the qualification level defined in chapter 6.2.11 of this document.

6.2.1.2 Security measures for cryptographic modules

MediaCert TSP ensures the physical and software security of the cryptographic modules used. In particular, it hosts this equipment in controlled access areas and offline. MediaCert TSP ensures the security of cryptographic modules throughout their lifecycle, in particular, during their installation, key ceremonies and use, until their end of life.

6.2.2 Private key control by several people

All requirements and practices described in the [GP] apply.

In addition, the CA's private signing keys are controlled by trusted personnel (PKI secret holders) and through a tool implementing secret sharing.

6.2.3 Private key escrow

All requirements and practices described in the [GP] apply.

6.2.4 Backup copy of the private key

All requirements and practices described in the [GP] apply.

In addition, as the private keys of CAs governed by this CP-CPS are not permanently activated within the cryptographic module, these private keys are backed up outside a cryptographic module. This backup copy is made in encrypted form and with an integrity control mechanism. The encryption used provides a level of security equivalent to or greater than the storage within the cryptographic module and, in particular, is based on an algorithm, key length and operating mode capable of resisting cryptanalytic attacks for at least the lifetime of the key thus protected. Encryption and decryption operations are performed within the cryptographic module in such a way that CA private keys are at no time in clear text outside the cryptographic module. The storage media for backup copies are stored in a safe. The control of encryption/decryption operations complies with the requirements of chapter 6.2.2.

6.2.5 Archiving the private key

All requirements and practices described in the [GP] apply.

6.2.6 Transfer of the private key to / from the cryptographic module

The transfer to / from the cryptographic module is only done for the generation of backup copies. This is done in numerical form, in accordance with the requirements of chapter 6.2.4

6.2.7 Storage of the private key in a cryptographic module

The storage of private keys of CAs governed by this CP-CPS is carried out in the same way as the storage of backup keys (see chapter 6.2.4).

6.2.8 Method of activating the private key

The activation of CA private keys is done in a cryptographic module and is controlled via activation data (see chapter 6.4). Since the private key is deactivated after each cryptographic

operation (see chapter 6.2.9), a quorum of secret holders must be present in order to activate the key before each operation.

6.2.9 Method of activating the private key

The CA private key is disabled after each cryptographic operation by resetting the cryptographic module.

6.2.10 Method of destroying private keys

The permanent destruction of a CA private key is achieved by destroying the means of restoring the private key:

- the destruction of the private key and all backup copies, and
- the destruction of the means of activating the private key.

6.2.11 Qualification level of the cryptographic module and signature creation devices

The cryptographic module used by the Root CA governed by this CP-CPS has undergone a security evaluation at FIPS 140-2 level 3.

[Time-stamping] In addition, the cryptographic module used by the Time-stamping Service must be subject to a security evaluation of at least EAL4 level of the common criteria reference system (ISO/IEC 15408) and qualified by the ANSSI.

6.3 Other aspects of key pair management

6.3.1 Public key archiving

CA public keys and public keys included in Certificates issued are archived for the period specified in 5.5.2.

6.3.2 Lifetimes of key pairs and certificates

6.3.2.1 Lifetimes of CA key pairs and certificates

[Root 2012][Root 2018] The Root CA key and associated Certificate have a lifetime of twenty (20) years.

[Time-stamping][Trust] The CA key and the associated Certificate have a lifetime of ten (10) years.

6.3.2.2 Life expectancy of key pairs and bearer certificates

The end of validity of a CA Certificate must be after the end of the life of the Certificates it issues.

[Root 2012][Root 2018] Intermediate CA keys and Certificates issued by the Root CA have a maximum life of ten (10) years.

[Time-stamping] The TSU keys have a lifetime of 1 year. The associated Certificates have a lifetime of 3 years.

[Trust] Delegate CA keys and CA Trust Certificates have a maximum life of three (3) years.

6.4 Activation data

6.4.1 Generation and installation of activation data

All requirements and practices described in the [GP] apply.

6.4.2 Activation data protection

All requirements and practices described in the [GP] apply.

6.4.3 Other aspects related to activation data

Not applicable.

6.5 Computer system security measures

6.5.1 Technical security requirements specific to computer systems

All requirements and practices described in the [GP] apply.

In addition, since the CAs within the scope of this document are operated off-line, certain security measures from the [GP] are applicable only to certain specific CA functions. For example, network security measures are applicable to the publication function but not to the Certificate generation function.

6.5.2 Qualification level of computer systems

Not applicable.

6.6 Security measures related to system development

6.6.1 Measures related to safety management

All developments carried out by the MediaCert TSP and impacting the PKI are documented and carried out via a process in order to ensure their quality. The system configuration of the PKI components and any modifications and upgrades are documented and controlled. In addition, MediaCert TSP operates a partitioning between development, testing, pre-production and production environments. This ensures a quality production start.

6.6.2 Level of security assessment of the life cycle of systems

Any significant system evolution of a PKI component is tested and validated before deployment. These operations are carried out by trusted personnel.

6.7 Network security measures

CAs within the scope of this CP-CPS are offline CAs. They do not have entry or exit access to the public network. However, the requirements of the [GP] remain applicable to publication functions.

6.8 Time-stamping / Dating system

CAs within the scope of this CP-CPS are offline CAs. Their clock is manually synchronized before any use. However, the requirements of the [GP] remain applicable to publication functions.

7 Certificate and CRL Profile

7.1 Certificate Profiles

7.1.1 Root CA Certificates "MediaCert Root CA 2018"

7.1.1.1 Certificate base fields

The following table shows the basic fields:

Field	Value
Version	2 (for version 3)
SerialNumber	Automatically generated during the Key Ceremony
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	Same as issuer (Self-signed certificate)
Validity	• notBefore: date of creation • notAfter: notBefore + 20 years
Subject Public Key Info	RSA 4096 bits

7.1.1.2 Certificate extensions

The following table shows the extensions:

Field	OID	Criticality	Value
Subject Key Identifier	2.5.29.14	No	[RFC 5280] method [0]: public key identifier contained in the Certificate
Key Usage	2.5.29.15	Yes, it is.	keyCertSign, CRLSign
Basic Constraint	2.5.29.19	No	CA: true Maximum Path Length: absent

7.1.2 Root CA « Root CA 2012 »

7.1.2.1 Certificate base fields

The following table shows the basic fields:

Field	Value
Version	2 (for version 3)
SerialNumber	Automatically generated during the Key Ceremony
Signature	Sha256WithRSAEncryption
Issuer	• CN = AC Racine – Root CA - 2012 • O = Atos Worldline • OU = 0002 378901946 • C = FR
Subject	Same as issuer (Self-signed certificate)

Validity	• 21 years
Subject Public Key Info	RSA 4096 bits

7.1.2.2 Certificate extensions

The following table shows the extensions:

Field	OID	Criticality	Value
Subject Key Identifier	2.5.29.14	Non	[RFC 5280] method [0]: public key identifier contained in the Certificate
Key Usage	2.5.29.15	Oui	keyCertSign, CRLSign
Basic Constraint	2.5.29.19	Non	CA: true Maximum Path Length : 4
Certificate Policies	2.5.29.3	Non	policyIdentifier: 1.2.250.1.111.12.4.1 policyQualifierId : 1.3.6.1.5.5.7.2.1 qualifier : https://www.mediacert.com
CRL Distribution Points	2.5.29.25	Non	http://root.mediacert.com/LatestCRL[1]

7.1.3 Intermediate CA Trust Certificate

7.1.3.1 Certificate base fields

The following table shows the basic fields:

Field	Value
Version	2 (for version 3)
SerialNumber	Automatically generated during the Key Ceremony
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	• CN =Mediacert Trust CA 2019. • O = Worldline • OR = 0002 378901946 • C = FR • *(optional)* SNU = Unique DN serial number [1]
Validity	• notBefore: creation date • notAfter: notBefore + 10 years

[1] This SERIALNUMBER is used to differentiate between the different Technical CAs. This is an incremented counter each time a new Technical CA is issued. It is constructed as follows:

SERIALNUMBER =

- *1:* represents the Technical Certification Authority 1;
- *2:* represents the Technical Certification Authority 2;
- …

It is not mandatory. The choice of its insertion is free to the decision-maker.

Field	Value
Subject Public Key Info	RSA 4096 bits

The CA ensures that the Intermediate Trust CA's CN is unique.

7.1.3.2 Certificate extensions

The following table shows the extensions:

Field	OID	Criticality	Value
Authority Key Identifier	2.5.29.35	No	[RFC 5280] method [0]: public key identifier of the issuing CA
Subject Key Identifier	2.5.29.14	No	[RFC 5280] method [1]: public key identifier contained in the Certificate
Key Usage	2.5.29.15	Yes, it is.	keyCertSign, CRLSign
Certificate Policies	2.5.29.32	No	• Policy Identifier : anyPolicy (2.5.29.32.0) • Policy Qualifier Id: 1.3.6.1.5.5.7.2.1 • Qualifier: https://www.mediacert.com
Basic Constraint	2.5.29.19	No	• CA: true • Maximum Path Length : 0
CRL Distribution Points	2.5.29.31	No	• fullName: http://www.mediacert.com/rootCA2018/rootCA2018.crl • reason : Absent • cRLIssuer : Absent
Authority Information Access	1.3.6.1.5.5.7.1.1	No	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt

7.1.4 Time-stamping CA Certificates

7.1.4.1 Certificate base fields

The following table shows the basic fields:

Field	Value
Version	2 (for version 3)
SerialNumber	Automatically generated during the Key Ceremony
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	• CN = MediaCert Timestamp CA 2018 • O = Worldline • OR = 0002 378901946 • C = FR
Validity	• notBefore: creation date • notAfter: notBefore + 10 years
Subject Public Key Info	RSA 4096 bits

7.1.4.2 Certificate extensions

The following table shows the extensions:

Field	OID	Criticality	Value
Authority Key Identifier	2.5.29.35	No	[RFC 5280] method [0]: public key identifier of the issuing CA
Subject Key Identifier	2.5.29.14	No	[RFC 5280] method [1]: public key identifier contained in the Certificate
Key Usage	2.5.29.15	Yes, it is.	keyCertSign, CRLSign
Certificate Policies	2.5.29.32	No	• Policy Identifier : anyPolicy (2.5.29.32.0) • Policy Qualifier Id: 1.3.6.1.5.5.7.2.1 • Qualifier: https://www.mediacert.com
Basic Constraint	2.5.29.19	No	• CA: true • Maximum Path Length : 0
CRL Distribution Points	2.5.29.31	No	• fullName: http://www.mediacert.com/rootCA2018/rootCA2018.crl • reason : Absent • cRLIssuer : Absent
Authority Information Access	1.3.6.1.5.5.7.1.1	No	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt

7.1.5 TSU certificate

7.1.5.1 Certificate base fields

The following table shows the basic fields:

Field	Value
Version	2 (for version 3)
SerialNumber	Automatically generated by the issuing CA
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Timestamp CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	• CN = MediaCert Timestamp Unit xxx • O = Worldline • OI = SI:FR-378901946 • C = FR
Validity	• notBefore: creation date • notAfter : notBefore + 3 years
Subject Public Key Info	RSA 2048 bits

The CA ensures that the TSU CN is unique by incrementing the xxx counter with each request. The first Certificate will therefore have index 001, the second 002 etc.

7.1.5.2 Certificate extensions

The following table shows the extensions:

Field	OID	Criticality	Value
Authority Key Identifier	2.5.29.35	No	[RFC 5280] method [0]: public key identifier of the issuing CA
Subject Key Identifier	2.5.29.14	No	[RFC 5280] method [1]: public key identifier contained in the Certificate
Key Usage	2.5.29.15	Yes, it is.	digitalSignature (0)
Certificate Policies	2.5.29.32	No	• Policy Identifier: 1.2.250.1.111.20.3.1.2 • Policy Qualifier Id: reference to CP-CPS (id-qt-cps: 1.3.6.1.5.5.7.2.1) • Qualifier: https://www.mediacert.com
Basic Constraint	2.5.29.19	No	• CA: false • Maximum Path Length: absent
Extended Key Usage	2.5.29.37	Yes, it is.	KeyPurposeId: id-kp-timeStamping (1.3.6.1.5.5.7.3.8)
CRL Distribution Points	2.5.29.31	No	• fullName: http://www.mediacert.com/timestampCA2018/timestampCA2018.crl • reason : Absent • cRLIssuer : Absent
Authority Information Access	1.3.6.1.5.5.7.1.1	No	• accessMethod: id-ad-caIssuers (1.3.6.6.1.5.5.5.7.48.2) • accessLocation: http://www.mediacert.com/timestampCA2018/timestampCA2018.crt

7.2 List of Revoked Certificates

7.2.1 Root CA LAR "Mediacert Root CA 2018"

7.2.1.1 Base field

Field	Value
Version	1 (for version 2)
Signature	SHA256WithRSA
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OR = 0002 378901946 • C = FR
Validity	1 year
Revoked Certificates	• Serial Number • Revocation Date

7.2.1.2 Extensions

Field	Criticality	Value
Authority Key Identifier	no	[RFC 5280] method [0]: public key identifier of the issuing CA

CRL Number	no	Defined by the tool

7.2.2 ROOT CA LAR « Root CA 2012 »

7.2.2.1 Base Field

Field	Value
Version	1 (for version 2)
Signature	SHA256WithRSA
Issuer	• CN = AC Racine – Root CA - 2012 • O = Atos Worldline • OU = 0002 378901946 • C = FR
Validity	1 year
Revoked Certificates	• Revoked CA certificate List

7.2.2.2 Extensions

Field	Criticality	Value
Authority Key Identifier	no	[RFC 5280] method [0]: public key identifier of the issuing CA
CRL Number	no	LAR Number

7.2.3 Intermediate CA LAR « Mediacert Trust CA 2019 »

7.2.3.1 Base Field

Field	Value
Version	1 (for version 2)
Signature	SHA256WithRSA
Issuer	CN = MediaCert Trust CA 2019 O = Worldline OU = 0002 378901946 C = FR
Validity	1 an
Revoked Certificates	• Serial Number • Revocation Date

7.2.3.2 Extensions

Champ	Criticité	Valeur
Authority Key Identifier	no	[RFC 5280] method [0]: public key identifier of the issuing CA
CRL Number	no	Define by tool

7.2.4 Time-stamping CA CRL

7.2.4.1 Base field

Field	Value
Version	1 (for version 2)
Signature	SHA256WithRSA
Issuer	• CN = MediaCert Timestamp CA 2018 • O = Worldline • OR = 0002 378901946 • C = FR
Validity	7 days
Revoked Certificates	• Serial Number • Revocation Date

7.2.4.2 Extensions

Field	Criticality	Value
Authority Key Identifier	no	[RFC 5280] method [0]: public key identifier of the issuing CA
CRL Number	no	Defined by the tool

8 Compliance audit and other evaluations

8.1 Frequency and/or circumstances of evaluations

All requirements and practices described in the [GP] apply.

CAs within the scope of this CP-CPS are not subject to external compliance audit or qualification within the meaning of the [eIDAS] Regulation.

8.2 Identities / qualifications of assessors

All requirements and practices described in the [GP] apply.

8.3 Relations between evaluators and evaluated entities

All requirements and practices described in the [GP] apply.

8.4 Topics covered by the evaluations

All requirements and practices described in the [GP] apply.

8.5 Actions taken in response to evaluation findings

All requirements and practices described in the [GP] apply.

9 Other business and legal issues

9.1 Price

CAs within the scope of this CP-CPS may charge for their service with the exception of the certificate status provision service, which is provided free of charge.

9.2 Financial responsibility

9.2.1 Insurance coverage

All requirements and practices described in the [GP] apply.

9.2.2 Other resources

All requirements and practices described in the [GP] apply.

9.2.3 Coverage and guarantee for user entities

All requirements and practices described in the [GP] apply.

9.3 Confidentiality of professional data

9.3.1 Scope of confidential information

All requirements and practices described in the [GP] apply.

In particular, within the scope of this CP-CPS, the following information is considered confidential:

- TDCP;
- CA private keys;
- activation data associated with CA private keys;
- all the secrets of the PKI;
- event logs of the PKI components;
- registration files of the holders;
- causes of revocations.

9.3.2 Information outside the scope of confidential information

All requirements and practices described in the [GP] apply.

9.3.3 Responsibilities in terms of protecting confidential information

All requirements and practices described in the [GP] apply.

9.4 Protection of personal data

9.4.1 Personal data protection policy

All requirements and practices described in the [GP] apply.

9.4.2 Personal information

Within the scope of this CP-CPS, the holder's registration file is considered as personal information. Access to personal data shall be provided in accordance with the [GP].

9.4.3 Responsibility for the protection of personal data

All requirements and practices described in the [GP] apply.

9.4.4 Notification and consent to the use of personal data

In accordance with the laws and regulations in force in France, personal information provided by holders to the CA is not disclosed or transferred to a third party except in the following cases: prior consent of the holder, judicial decision or other legal authorization.

9.4.5 Conditions for disclosing personal information to judicial or administrative authorities

All requirements and practices described in the [GP] apply.

9.4.6 Other circumstances for disclosing personal information

Not applicable.

9.5 Intellectual and industrial property rights

All requirements and practices described in the [GP] apply.

9.6 Contractual interpretations and guarantees

The obligations common to the components of the PKI are as follows:

- protect and guarantee the integrity and confidentiality of their secret and/or private keys;
- use their cryptographic keys (public, private and/or secret) only for the purposes intended when they are issued and with the tools specified under the conditions set out in the CA CP-CPS and related documents;
- respect and apply the part of the TDCP for which they are responsible (this part must be communicated to the corresponding component);
- submit to compliance checks carried out by the audit team mandated by the CA (see chapter 8);

- respect the agreements or contracts that bind them between themselves or to the holders;
- document their internal operating procedures, implement the resources (technical and human) necessary to carry out the services to which they commit themselves under conditions guaranteeing quality and safety.

9.6.1 Certification Authorities

The MediaCert TSP, as a Certification Authority, is responsible for:

- the validation and publication of the CP-CPS;
- validation of the TDCP and its compliance with the CP-CPS;
- the conformity of the Certificates issued with respect to this CP-CPS;
- the compliance of all security principles by the various components of the PKI and the related controls.

The MediaCert TSP, as a Certification Authority, is liable, unless it can be shown that it has not committed any intentional fault or negligence, for damages caused to users, if:

- the information contained in the Certificate does not correspond to the registration information;
- the latter did not register the revocation of a certificate and did not publish this information in accordance with its commitments.

9.6.2 Registration Authorities

As the MediaCert TSP operates its own Registration Authority within this scope, please refer to chapter 9.6.1.

9.6.3 Certificate Holders

The Holder has the duty to:

- provide accurate and up-to-date information when applying for or renewing the Certificate;
- protect your private key activation data;
- respect the conditions of use of the service;
- inform the CA of any changes to the information contained in its Certificate;
- request the renewal of its Certificate with a reasonable time before its expiry;
- make, without delay, a request to revoke its Certificate in the event of compromise or suspected compromise of its activation data or private key.

9.6.4 Certificate users

Users of Certificates must:

- verify and respect the use for which a Certificate has been issued;
- for each Certificate in the certification chain, from the Subscriber's Certificate to the Root CA, verify the digital signature of the CA issuing the relevant Certificate and check the validity of this Certificate (validity dates, revocation status).

9.6.5 Other participants

Not applicable.

9.7 Limit of guarantee

Not applicable.

9.8 Limitation of liability

MediaCert TSP shall not be liable for any unauthorized or non-compliant use of authentication data, Certificates, LAR/LCRs, and any other equipment or software made available.
MediaCert TSP shall not be liable for any damage resulting from errors or inaccuracies in the information contained in the Certificates, when such errors or inaccuracies result directly from the incorrect nature of the information provided by the Subscriber. In addition, to the extent of the limitations of French law, MediaCert TSP cannot be held liable:

- no financial loss;
- no data loss;
- any indirect damage related to the use of a Certificate;
- of any other damage.

In any event, MediaCert TSP's liability shall be limited, for all events and for all damages combined, to the amount paid to MediaCert TSP for access to the service, in compliance with and within the limits of applicable law.

9.9 Indemnities

Not applicable.

9.10 Duration and early termination of the validity of the CP

9.10.1 Period of validity

The CP-CPS must remain in force at least until the end of the life of the last Certificate issued under this CP-CPS.

9.10.2 Early end of validity

This CP-CPS remains in use until a new version is released.

9.10.3 Effects of the end of validity and remaining clauses applicable

Not applicable.

9.11 Amendments to the CP

All requirements and practices described in the [GP] apply.

9.12 Provisions concerning conflict resolution

All requirements and practices described in the [GP] apply.

9.13 Competent Jurisdictions

All requirements and practices described in the [GP] apply.

9.14 Compliance with laws and regulations

All requirements and practices described in the [GP] apply.

9.15 Miscellaneous provisions

9.15.1 Global agreement

Not applicable.

9.15.2 Transfer of activities

Not applicable.

9.15.3 Consequences of an invalid clause

Not applicable.

9.15.4 Application and waiver

Not applicable.

9.15.5 Force majeure

All requirements and practices described in the [GP] apply.

9.15.6 Other provisions

Not applicable.