Document reference:	ROOT PC 0020
Document revision:	1.3
Document date:	21/07/2017
Classification:	Public

Mediacert
Root Certification Authority
Certification Policy

CYRIL LOOTVOET

Signature numérique de CYRIL LOOTVOET
Date : 2018.04.12 15:37:52 +02'00'

Contents

Changelog

Version	Date	Description	Author	Validation
1.0	7/27/2012	Creation	D Cogny	D Bonnin
1.1	11/5/2015	Update before publication	J.J. Milhem	NA
1.2	11/23/2015	Update 2.1 and 2.2	Q Alexandre	NA
1.3	7/21/2017	Update to take into the eIDAS regulation account	A. Borel F. DA SILVA	Security Committee

Introduction

1.1 General presentation

This document describes the certification policy (CP) of Worldline's MediaCert Root Certification Authority. It is the highest-level authority within the MediaCert Private Key Infrastructure (PKI) set up by Worldline. This PKI called MediaCert consists of this Root Certification Authority, to which specialized child Certification Authorities are attached for internal needs or customer project support needs e.g. the provision of extranet access certificates, extranets, signature certificates or other.

NB 1: This Certification Authority marks the early renewal of a MediaCert Root Certification Authority created in 2002.
NB 2: This PKI and its Certification Authorities are not intended for commercial purposes.

1.2 Identification

The name of the Certification Authority concerned by this CP is "MediaCert".

AFNOR has assigned number **1.2.250.1.111** to Worldline as the OID root under which the OIDs of the various Certification Authorities are created. The format of the CAs' OIDs is 1.2.250.1.111.xyz where

- x is the year of creation of the Certification Authority e.g. 2012 => 12
- *y* is the number assigned to the Certification Authority by Worldline; this number is based on the year of creation.
- z is the major version of the CP.

The OID assigned to this CP is **1.2.250.1.111.12.4.1**.

The *Distinguished Name* (DN) of the MediaCert Root Certification Authority is

C = FR
O = Atos Worldline
OU = 0002 378901946
CN = AC Racine - Root CA - 2012

1.3 PKI components

This PKI consists of several functional blocks, in particular Certification Authority and Registration Authority functions.

1.3.1 Certification Authority (CA) function

The CA provides the certificate management services of the associated child CAs:

- processing of certification requests,
- issuance of certificates to requisitioners,
- processing of revocation requests, and
- the publication of its certificate and the CARLs.

The Root CA signs the certificates and the CARLs that it issues with its private key and is responsible for them. This CA is by definition a self-signed CA.

These features are provided by the PKI software used in conjunction with an HSM for the generation and storage of the private key, and the signing of certificates CARLs.

1.3.1.1 Certificate generation function

This function generates the certificates from the information given by the Security Committee as a CSR and a certificate template defined during the configuration of the Root CA.

1.3.1.2 Function for generating the secret elements of a child CA

Not applicable The keys of a child CA are generated at its level.

1.3.1.3 Publication function

The Root CA's certificate is given to persons in charge of the relevant Certification Authorities, or their deputies, who implement certificates of a child CA in the form of a certification chain containing this root certificate and that of the child CA used.

1.3.1.4 Revocation management function

This function processes the revocation requests submitted to the CA. This results in the immediate publication of a new CARL, which is sent to the persons in charge of the Certification Authorities concerned.

1.3.2 Registration Authority (RA) function

There is no administrative entity per se that processes with requests for child CAs because this root only signs CAs that are internal to Worldline. This is dealt with during the preparation of key ceremonies.

The PKI software provides a graphical interface that enables administrators to submit a CSR and to retrieve the corresponding certificate that is then installed in the technical environment of the child CA.

1.4 Use of certificates

1.4.1 Areas of use

The key pair of this Root CA is only used to sign MediaCert Worldline internal child CAs and its CARLs issued at regular intervals.

1.4.2 Prohibited uses

Any other use is prohibited e.g. the signing of external CAs, server certificates or persons.

1.5 CP management

Worldline is responsible for drawing up this CP maintaining it and modifying it as soon as necessary. For this purpose, a Security Committee will make regularly make decisions as to the necessity of making changes to this CP. This committee is made up of

- at least one representative of the CA, and
- the security officer of the CA.

The authorized contact for any comment, request for additional information, claim or submission of a litigation file concerning this CP is

Comité "MediaCert"
Worldline
1, rue de la Pointe
Zone Industrielle A
59113 Seclin
France
dlfr-mediacert-ac-otu@atos.net

1.6 Acronyms

The following acronyms are used in this document:

- **CA:** Certification Authority
- **CARL:** Certification Authority Revocation List
- **CISO:** Chief Information Security Officer
- **CN:** Common Name
- **CP:** Certification Policy
- **CSR:** Certificate Signing Request
- **DN**: Distinguished Name
- **HSM:** Hardware Security Module
- **KC:** Key Ceremony
- **OID:** Object Identifier
- **PKI:** Public Key Infrastructure
- **RA:** Registration Authority

2 Responsibilities with regard to the information that must be published

2.1 Entities in charge of making the information available

The MediaCert Committee is in charge of publishing this CP.
Technical administrators manage the publication of CARLs.

2.2 Information that must be published

The MediaCert Committee publishes the CP on a shared drive accessible internally by Worldline's staff, as well as on Worldline's website (https://www.mediacert.com) for public consultation purposes.

The CARLs issued by the CA are published by the technical administrators on a shared drive. The address at which CARLs are published can also be found in the certificate of the CA published on the Worldline website for public consultation purposes.

The URLs for accessing this CP and the CARL are available in the extensions of the Certificates issued by the Root CA in accordance with section 7 of this document.

2.3 Publication time and frequency

The CP is published after its internal validation within the Security Committee.
CARLs are published within 24 hours of their generation.

2.4 Access restrictions applicable to the published information

The CP and the CARLs are freely accessible in read-only mode from the web page defined in section 2.2 of this document.

The published elements are signed electronically so they can be duly authenticated.

Write access to the information is strictly limited to the authorized internal administration functions of the PKI, which have write access to the shared environment used to store this information.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The names used comply with the specifications of the X.500 standard.

The *"issuer"* and *"subject"* fields are identified by an X.501-type DN in the form of a "PrintableString".

3.1.2 Pseudonymization

Not applicable

3.1.3 Rules for interpreting the various name forms

Not applicable

3.1.4 Name uniqueness

The "Common Name" (CN) field is unique to each child CA.

Any request (except for renewal) that does not comply with this rule must be refused.
Therefore, throughout the life span of the CA, a CN assigned to a child CA cannot be assigned to another CA.

The uniqueness of the DN is achieved through the presence of the field called "Serial Number in DN".

3.1.5 Identification, authentication and role of registered trademarks

Not applicable

3.2 Initial identity validation

3.2.1 Method for proving the possession of the private key

The signing of a CSR by the associated private key provides this guarantee.

3.2.2 Validation of an organization's identity

The naming data of a child CA to be signed are provided during the key ceremony preparation phase so they can be validated.

3.2.3 Validation of an individual's identity

Not applicable

3.2.4 Unverified information

The certificate information is validated during the key ceremony preparation phase.

3.2.5 Validation of the requisitioner's authority

The requisitioner is an entity internal to Worldline.

3.2.6 Cross-certification of CAs

Not applicable

3.3 Identification and validation of a key renewal request

3.3.1 Identification and validation for common renewal

Identification and validation for the common renewal of a child CA’s certificate are carried out in accordance with section 3.2.

3.3.2 Identification and validation for renewal after revocation

Identification and validation for renewal following the revocation of a child CA’s certificate are carried out in accordance with section 3.2

3.4 Identification and validation of a revocation request

The revocation of a child CA can be decided after a consultation between

- the entity responsible for this CA,
- the director of the MediaCert Committee, and
- the CISO in charge of the security of the Root CA.

4 Operational Requirements with regard to the life cycle of certificates

4.1 Certificate request

4.1.1 Origin of a certificate request

The certificate request comes only from an internal entity.

4.1.2 Process and responsibilities when drawing up a certificate request

Requests are subjected to prior validation of legitimacy by the MediaCert Committee.

4.2 Certificate request processing

4.2.1 Execution of the request identification and validation processes

Requests are identified and validated by the MediaCert Committee during the key ceremony preparation phase.

4.2.2 Acceptance or rejection of the request

If the request is rejected, the MediaCert Committee informs the originator of the request and specifies the reason for the rejection (e.g. the public key is not long enough.).

4.2.3 Certificate duration

This CP formulates no requirements in this regard.

4.3 Certificate issuance

4.3.1 CA's actions regarding the issuance of the certificate

This operation requires that the Root CA be reactivated and that several trusted roles of the PKI be present, which must be summoned.

After the validation, the CSR is submitted to the Root CA through a graphical interface during a key ceremony.

The naming elements are displayed and compared to the values specified in the key ceremony script. If they are consistent, a certificate template is chosen, and the request is submitted to the CA, which provides the certificate in return. Otherwise, the request is rejected.

The certificate is copied to removable media so it can be delivered manually after the session.

4.3.2 Notification sent by the CA to inform the subject of the delivery of the certificate

The certificate is issued after the session through the delivery of the certificate, by the MediaCert Committee, to the entity in charge of the child CA. Depending on the case, this delivery can be carried out in person, via a removable medium, or via e-mail.

4.4 Certificate acceptance

4.4.1 Certificate acceptance process

Acceptance is tacit.

4.4.2 Certificate publication

There is no publication in the Root CA’s environment.

4.4.3 Notification sent by the CA to inform other entities of the delivery of the certificate

Not applicable

4.5 Key pair and certificate uses

4.5.1 Use of the private key and the certificate

The use of a child CA’s private key and the associated certificate is strictly limited to the signing of certificates and CRLs within this CA in accordance with the use provided for in its CP. Otherwise, this CA might be held liable.

This use is also indicated in the “Key_Usage” extension of its certificate.

4.5.2 Use of the private key and the certificate by third parties

Third-party certificate users must strictly comply with the authorized uses of certificates. Otherwise, they might be held liable.

4.6 Certificate renewal

Renewal without a change of keys is not allowed.

4.7 Delivery of a new certificate following a change of key pair

This section deals with the issuance of a new certificate to a child CA following the generation of a new key pair.

4.7.1 Possible reasons for a change of key pair

Renewal causes are diverse, expiry being the first one of them. Early renewal is also possible e.g. for technical maintainability reasons or because of the weakness of a key or algorithm used in the current certificate.

4.7.2 Origin of a request for a new certificate

The origin is the same as for an initial request; see subsection 4.1.1.

4.7.3 Processing of a request for a new certificate

The procedure is the same as for an initial request; see section 4.2.

4.7.4 Notification of the creation of the new certificate to the subject

The procedure is the same as for an initial request; see subsection 4.3.2.

4.7.5 Acceptance of the new certificate

The procedure is the same as for an initial request; see subsection 4.4.1.

4.7.6 Publication of the new certificate

The procedure is the same as for an initial request; see subsection **Erreur ! Source du renvoi introuvable.**.

4.7.7 Notification sent by the CA to inform other entities of the delivery of the new certificate

The procedure is the same as for an initial request; see subsection 4.4.3.

4.8 Certificate modification

Certificate modification is prohibited by this CP.

4.9 Revocation and suspension of certificates

4.9.1 Possible causes of revocation

4.9.1.1 Child CA's certificate

There are many possible causes of revocation e.g.

- an error detected in the content of the certificate that appeared after the key ceremony,
- cessation of activity,
- The private key is compromised, suspected of being compromised, is lost or stolen.
- regulatory changes in the algorithms used.

4.9.1.2 Root CA's certificate

Possible causes of revocation are also numerous, including notably

- cessation of activity, or
- The private key is compromised, suspected of being compromised, is lost or stolen.

In this case, all child Certification Authorities must be revoked beforehand, and a final CARL must be published before the final shutdown.

4.9.2 Origin of a revocation request

This type of revocation can only be requested after consultation between:

- the entity responsible for this CA.
- the MediaCert Committee.
- The CISO in charge of the CA.

4.9.3 Revocation request processing

This operation requires that the Root CA be reactivated and that several trusted roles of the PKI be present which must be summoned.

The revocation is performed during a key ceremony on the Root CA, through a graphical interface of the PKI software. This results in the immediate publication of a new CARL that is made available to the entity responsible for this CA. An official report of the session is also produced.

If the revocation concerns the root CA, all child CAs must be revoked beforehand.

4.9.4 Time allotted to request the revocation

As soon as the decision is made, the administrators are contacted so the revocation session is organized.

4.9.5 Time needed by the Root CA to process a revocation request

This operation requires that the Root CA be reactivated and that several roles be present, which must be summoned. It can be performed within 48 working hours of the request.

4.9.6 Requirements with regard to the verification of the revocation by certificate users

There is no systematic requirement for the applications that use MediaCert certificates to check CARLs and CRLs.

The CARL is made available to third-party applications that make this verification using a file.

4.9.7 CARL generation frequency

CARLs are generated on each revocation operation or by default every 12 months. However, a new CARL may be published following the revocation of a child CA.

4.9.8 CARL publication deadline

A CARL is published 24 working hours after its generation at the latest.

4.9.9 Availability of an online system for verifying the revocation and statuses of certificates

Service not provided.

4.9.10 Requirements with regard to the online verification of revoked certificates by certificate users

Not applicable

4.9.11 Other ways of obtaining information about revoked certificates

Not applicable

4.9.12 Specific requirements if the private key is compromised

If a child CA’s key is compromised, the entity in charge of it must stop it immediately without waiting for the revocation session.

4.9.13 Possible reasons for certificate suspension

CAs cannot be suspended.

4.9.14 Origin of a suspension request

Not applicable

4.9.15 Suspension request processing

Not applicable

4.9.16 Minimum and maximum CA suspension times

Not applicable

4.10 Certificate status information function

There is no certificate status information function other than the publication of CARLs. The latter are published in CRL v2 format (RFC 5280) on a website accessible via HTTP (s) at

- the address specified in section 2.2 of this CP; and
- the address specified in the Certificate issued by the OTU CA as specified in section 7 of this CP.

4.11 End of the relationship with a child CA

If the relationship ends, for whatever reason, the CA’s certificate must be revoked.

4.12 Key escrow and recovery

There is no escrow of a child CA’s key at Root CA level.

The only form of escrow is the backup of the Root CA’s key itself for recovery purposes should a crash occur. This backup is executed in accordance with the procedures defined by the manufacturer of the HSM used.

5 Non-technical security measures

5.1 Physical security measures

Worldline hosts this Root CA in a data center that provides the necessary guarantees in terms of access control, fire safety, backups, etc.

The CA server and its HSM are installed on premises, the access to which is controlled (logs and videosurveillance) and reserved for authorized personnel.

The initialization and activation of the CA requires the presence of several complementary trusted roles.

5.2 Procedural security measures

5.2.1 Trusted roles

The functions operated in the Root CA are distributed to various types of roles to ensure that knowledge is separated for sensitive tasks.

This separation is deactivated outside of key ceremonies for which different types of stakeholders of the organization may be involved depending on the operations performed:

- system administrators,
- HSM administrators,
- a system auditor,
- the Master of Ceremony,
- secret holders, and
- the center's Manager.

Their respective tasks are specified in the key ceremony scripts.

5.2.2 Number of persons required per task

Depending on the type of operations performed, the number and types of roles and persons that must be present are different. The need is greatest for the creation of the CA with the server, HSM configuration, and PKI software installation phases that also involve system administrators.

5.2.3 Identification and authentication for each role

The verification of stakeholders' identities is generally implicit because the persons working on this PKI are colleagues who know each other. In the opposite case (e.g. a colleague from a Worldline site located outside France), the head of the data center asks for proof of identity.

5.2.4 Roles that require remit separation

Several roles can be assigned to the same person provided such concurrence does not compromise the security of the implemented functions.

5.3 Security measures with regard to the staff

5.3.1 Required qualifications, skills and authorizations

The staff who hold trusted roles within the MediaCert PKI are informed of the associated responsibilities (liability agreement, Certification Practice Statement) and of the procedures pertaining to system security and staff control, which they must comply with.

Management staff are trained and aware of security and risk management to fully fulfill their responsibilities vis-à-vis the MediaCert PKI.

The MediaCert PKI ensures the qualification and competence of the members of its staff who hold trusted roles.

5.3.2 Criminal record verification procedure

In particular, these persons must not have been convicted or find themselves in a situation where a conflict of interest exists and contravenes their remit. They give their employer a copy of bulletin number 3 of their criminal record as part of the hiring procedure and when they hand in their liability agreement.

The candidate's application file is subjected to the validation of the Human Resources department.

Criminal records are verified every three (3) years. With this in mind, a recurring yearly task of checking criminal records is put in place.

The staff in charge of operating the certification services are not responsible for the commercial aspects of these services. Moreover, they are free from any conflict of interest that could influence their way of carrying out the operations they are responsible for, and which might undermine confidence. In this regard, they undertake to confirm in writing, upon their acceptance of the trusted role within the MediaCert PKI, the absence of any conflict of interest related to the exercise of this new activity.

5.3.3 Basic training requirements

The staff are trained in the CA's software, hardware and working procedures.
Through the security awareness campaign, the staff have been made aware of the consequences of the operations that they are in charge of.

5.3.4 Continuous training requirements and frequency

The staff concerned receive the necessary information and training before any change is made to systems, procedures, the organization or others, according to the nature of these changes.

5.3.5 Frequency and sequence of rotation between various assignments

This CP formulates no requirements in this regard.

5.3.6 Penalties for unauthorized actions

Worldline's by-laws indicate that appropriate administrative disciplinary sanctions are applicable in the event of a fault (failure to comply with this CPS, etc.). This is particularly recalled in the liability agreement signed by any person holding a trusted role within the MediaCert PKI.

5.3.7 Requirements with regard to external providers' staff

Not applicable. Only Worldline's staff are involved in trusted roles for these applications.

5.3.8 Documents given to the staff

Each person has at least the documents pertaining to the operational procedures and the specific tools that they implement, as well as the general policies and practices of the component which they work in.

5.4 Procedures for constituting audit data

All the operations related to the CA are traced using computer or handwritten traces. They help ensure the audibility, traceability and accountability of operations.

5.4.1 Types of events to log

Event logs explicitly include

- the identifier of the software or operator that executes the operation,
- the date and type of the operation, and
- a description.

5.4.1.1 CA's computer traces

Each component logs the events and incidents that concern it. Here is a non-exhaustive list thereof:

- startups and shutdowns of computer systems and applications;
- user account management;
- user login;
- certificate creation;
- certificate revocation;
- CARL publication.

5.4.1.2 Access control

The access control system of the premises also logs its own events on its own system.

5.4.1.3 Handwritten traces

Manual logs concern

- key ceremonies and their official reports;
- CARL creation;
- the revocation or renewal of a CA;
- interventions that require access to sensitive premises and vaults, such as the reactivation of the HSM or the restoration from backups following a failure;
- disposal.

5.4.2 Event log processing frequency

The Root CA's logs are not checked regularly. They are only used for internal investigation and auditing purposes.

5.4.3 Event log retention period

The logs are kept throughout the life of the CA.

5.4.4 Event log protection

Both computer and handwritten logs are protected by strict access control and can only be viewed by authorized persons.

5.4.5 Event log backup procedure

Event logs are saved at the end of each key ceremony, just before the CA is deactivated.

5.4.6 Event log collection system

This CP formulates no specific requirements in this regard.

5.4.7 Transmission of an event logging notification to the person responsible for this event

This CP formulates no specific requirements in this regard.

5.4.8 Evaluation of vulnerabilities

Because the CA is disabled outside of key sessions, there is no systematic, regular log analysis. It is carried out only if there if an internal investigation is needed.

5.5 Data archiving

5.5.1 Type of data to archive

The archiving is carried out to ensure the traceability of operations. Notably, the data that must be archived are

- For the CA:

- child CA certificate requests,
- revocation or renewal requests, and
- certificates and CARLs.

- For the technical platform (server and HSM):

- the technical documents that describe IT configurations and equipment;
- software operation settings;
- operation procedure documents;
- event logs.

- For documents:

- day book of access to sensitive premises;
- key ceremony manuals;
- versions and revisions of the CP; and
- liability agreements/terminations of trusted roles.

5.5.2 Archive retention period

Archives are kept throughout the CA's life and 3 years beyond.

5.5.3 Archive protection

Depending on their form (paper-based or electronic) and their means of preservation, protection is provided by the access rights and possibly integrity check tools (e.g. for magnetic cartridges).

5.5.4 Archive backup procedure

Paper-based archives are most often digitized and deposited in document databases.

The technical operation documents are also deposited in document databases.

Computer archives are of two types:

- Information Service Management Portal (ISMP) “tickets”; and
- event logs.

5.5.5 Data timestamping requirements

The Root CA’s server clock is synchronized to a reliable external source.

5.5.6 Archive collection system

The collection is organized after each key session except for ISMP “tickets” which are automatically processed.

5.5.7 Recovery and verification of archives

Electronic versions are recoverable almost immediately. Paper-based versions (e.g. daily log of access to sensitive premises) are available within two working days.

5.6 Change of the CA’s key

The CA cannot generate a child CA certificate whose end date is later than the expiry date of its own certificate.

It must be renewed no later than its expiry or before the expiry if necessary e.g. to switch to stronger algorithms, higher key lengths, or if need be, to sign a child CA whose desired expiry is later than that of the Root CA. In this case, the old Root CA is maintained so it can revoke the CAs that it has signed and can continue publishing its CARLs. The new one is used to sign and revoke new CAs and publish its CARLs.

5.7 Recovery following compromise and disaster

5.7.1 Procedures for reporting and handling incidents and compromises

Worldline’s staff are aware of how to handle incidents, including security incidents. In the latter case, and in accordance with our specific procedures, they open an ISMP incident with a specific object code that generates a “workflow” for the security team. This team will coordinate the analysis and the resulting actions including communication towards the entities in charge of the child CAs.

5.7.2 Recovery procedures should IT resources get corrupted

Worldline has procedures, backups, maintenance contracts, and replacement hardware to restore the CA’s service if a technical problem occurs.

The private key, which is the most sensitive element, is stored as a precaution in two copies on two different sites.

5.7.3 Recovery procedures should the private key be compromised

If the MediaCert CA’s private key is compromised or suspected of being compromised, if it is destroyed, or if the algorithm used is compromised:

- After investigating the event, Worldline decides to revoke or not the Root CA’s certificate.

- If it decides to revoke the relevant Root CA certificate:
    - All the certificates delivered by the child CAs and signed with their private key concerned are revoked.
    - All the certificates delivered by the Root CA and signed with the private key concerned are revoked.
- If an algorithm is compromised, it is replaced.
- A new key pair is generated and a new corresponding Root CA certificate is issued.
- Worldline decides on the communication plan intended for
    - the Authorities that accredit the certificate in question [Adobe, ANSSI (*French National Cybersecurity Agency*...)]; and
    - Subscribers and users of the child CA's certificates.

5.7.4 Disaster recovery

The Root CA does not need to operate continuously; indeed, it is disabled most of the time. The backups in place make it possible to rebuild the service within a reasonable time i.e. a few days.

5.8 End of the PKI's life

5.8.1 Activity transfer

Not applicable

5.8.2 Cessation of activity

If Worldline decided to discontinue this MediaCert activity, it would inform its partners with prior notice.

On the appointed date, a key session is organized to revoke the child CAs' keys (execution of the activity cessation plan of the child CAs), and the MediaCert Root CA's certificate. Its private key and the associated secrets are then destroyed.

6 Technical security measures

6.1 Key pair generation and installation

6.1.1 Generation of the Root CA's key pairs

The generation of the CA's key pairs is performed in an HSM whose qualification level is described in subsection 6.2.11 of this document.

This generation takes place during a key ceremony on Worldline's secure premises. Various trusted roles are involved to enable the HSM and the PKI software used.

6.1.2 Transmission of a child CA's private key

Not applicable

6.1.3 Transmission of a child CA's public key

It is transmitted in the form of a CSR in PKCS # 10 format, which makes it possible to check its integrity.

6.1.4 Transmission of the CA's public key to users

It is transmitted via its root certificate during the signing ceremonies of the child CAs at the same time as the child certificate.

6.1.5 Key size

According to the child CA's expiry and the importance of what the issued certificates will be used for, the size of its keys can be 2,048 or 4,096 bits.

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

The quality of the generation is verified upon the receipt of the CSR by the CA. The key sizes must match the template of the relevant child CA.

6.1.7 Target uses of the key

The Root CA's and child CAs' private keys are limited to signing certificates and CRLs. This is determined by the *KeyUsage* extension with the *keyCertSign* and *cRLSign* values. This extension is critical.

6.2 Security measures for the protection of private keys and for cryptographic modules

6.2.1 Security standards and measures for cryptographic modules

The CA's key pairs are generated in an HSM whose qualification level is described in subsection 6.2.11 of this document.

It is located in particular in Worldline's secure data centers in Vendôme and Brussels.

6.2.2 Control of the private key by several persons

The generation and activation of the CA's private key implements a shared secrets system between several trusted roles. These procedures are described in detail in the key ceremony document.

6.2.3 Private key escrow

The Root CA's or child CAs' private keys are not held in escrow.

6.2.4 Private key emergency backup

The Root CA’s private key is saved using the HSM manufacturer’s procedures.
The backup consists of a file containing a cryptogram of the private key encrypted by the HSM’s master key.

6.2.5 Archiving of the private key

The Root CA’s or its child CAs’ private keys are not archived.

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

This transfer is only possible through the manufacturer’s backup / restoration procedures; see subsection 6.2.4

6.2.7 Storage of a private key into a cryptographic module

The private key is stored in an HSM evaluated as defined in subsection 6.2.11 or encrypted with the HSM’s master key of in the case of external backups, in accordance with the manufacturer’s backup procedures.

6.2.8 Private key activation method

The CA’s private key can be activated only during a key ceremony, with multiple trusted roles being present and holding the HSM’s activation data and parts of its master key.

6.2.9 Private key deactivation method

The private key is disabled by removing the HSM after the backup and uninstalling the HSM’s software.

6.2.10 Private key destruction method

The private key can be destroyed by an HSM administrator after its activation. In addition, all backups must be destroyed either through secure deletion software or by physically destroying the removable backup media.

6.2.11 Level of qualification of the cryptographic module and authentication devices

The HSM used is FIPS 140-2 L3 certified.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

The public keys of the root CA and each child CA are archived as part of the MediaCert PKI’s data.

6.3.2 Key pair and certificate life spans

The Root CA cannot issue a child CA certificate that has a life span longer than its own. The life span of key pairs and certificates are defined in particular within certificates.

6.4 Activation data

6.4.1 Generation and installation of activation data

The HSM’s activation data are generated during the key ceremony of initialization of the Root CA.

6.4.2 Protection of activation data

These data are under the responsibility of the secret holders who have safes to keep them in a secure environment.

6.4.3 Other aspects pertaining to activation data

This CP formulates no specific requirements in this regard.

6.5 IT systems security measures

6.5.1 Technical security requirements specific to IT systems

The server hosting the Root CA meets the following security objectives:

- user identification and authentication for accessing the system;
- use session management (disconnection after idle time, file access restrictions according to roles...);
- management of users' accounts and rights;
- access protection through an internal firewall; and
- traceability of operations.

6.5.2 Evaluation of IT systems

This CP formulates no specific requirements in this regard.

6.6 Security measures for systems throughout their life cycles

6.6.1 Security measures with regard to system development

Not applicable since the CA relies solely on external software packages without any extra development.

6.6.2 Security management measures

If certain software packages have to be upgraded, they are tested beforehand in an acceptance tests environment. The resulting changes are reflected in the operating manuals and are logged.

6.6.3 Evaluation of the security of systems' life cycles

This CP formulates no specific requirements in this regard.

6.7 Network security measures

The CA's server is not connected to any network outside of key ceremony operations during which a private, closed network is specifically set up.

6.8 Timestamping system

The server's clock is synchronized to a reliable external source.

7 Certificate, OCSP and CRL profiles

7.1 Certificate profiles

The certificates issued by the OTU CA contain the following basic fields:

- **Version**: version of the X.509 certificate (v3);
- **Serial number**: serial number of the certificate (value unique to each issued certificate);
- **Signature**: OID of the algorithm used by the CA to sign the certificate;
- **Issuer**: value of the DN (X.500) of the CA that issues the certificate;
- **Validity**: activation and expiry dates of the certificate;
- **Subject:** value of the DN (X.500) of the equipment;
- **Subject Public Key Info** OID of the algorithm and value of the public key of the equipment
- **Extensions**: extension list.

These fields are supplemented by extensions that can be critical or non-critical. They are a combination of extensions from the child CAs' CSRs, and extensions imposed by the certificate template at Root CA level.

7.1.1 Certificate of the MediaCert PKI's Root CA

All these fields are signed with the Root CA's private key. Two fields are used for this signature:

- **Signature**: OID of the algorithm used, and
- **Signature Value**: result of the signature.

The root certificate is defined below. It is presented in two parts: basic fields and extensions. The information described below is indicative, since the data of the root certificate have evidentiary value.

Basic fields

Fields		Value
Version		V3 (Value: 2)
Serial number		66:a7:15:98:de:e3:46:da
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C	FR
	O	Atos Worldline
	OI	0002 378901946
	CN	AC Racine – Root CA – 2012
Validity		21 years
Subject	C	FR
	O	Atos Worldline
	OU	0002 378901946
	CN	AC Racine – Root CA – 2012
Subject Public Key Info		RSA 4096 bits

Extensions

Fields	Critical	Value
Authority Key Identifier	No	11 28 8e f4 56 7b cf bd 80 cb 31 9d 42 82 ed 4a 5c ef

			25 a7
Subject Key Identifier		No	11 28 8e f4 56 7b cf bd 80 cb 31 9d 42 82 ed 4a 5c ef 25 a7
Key Usage		Yes	keyCertSign, CRLSign
Basic Constraint	Certificate Authority	No	true
	Maximum Path Length		4
Certificate Policies	policyIdentifier	No	1.2.250.1.111.12.4.1
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		http://www.mediacert.com
CRL Distribution Points		No	http://root.mediacert.com/LatestCRL[1]

7.1.2 Child CAs' certificates

The template of a child CA must be described in its own CP. It must comply with all the technical constraints defined in this CP.

7.2 CARL profile

The CARLs issued contain the following fields:

- **Version** : version of the CRL standard (v2 - RFC 5280);
- **Signature**: OID of the algorithm used by the CA to sign the CARL;
- **Issuer**: value of the DN (X.500) of the CA that issues the CARL;
- **This Update**: date on which this CARL update was generated;
- **Next Update**: date on which the next CARL update will be generated;
- **Revoked Certificates**: list of the revoked certificates with their serial numbers, revocation dates, and reasons
- **CRL Extensions** : extension list

All these fields are signed with the Root CA's private key. Two fields are used for this signature:

- **Signature**: OID of the algorithm used, and
- **Signature Value**: result of the signature.

The template used is defined below. It is presented in two parts: basic fields and extensions.

Basic fields

Fields		Value
Version		V2 (Value: 1)
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C	FR
	O	Atos Worldline
	OU	0002 378901946
	CN	AC Racine – Root CA – 2012
This Update		CRL issuance date
Next Update		CRL issuance date + 12 months

[1] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

Revoked Certificates	List of the revoked CA certificates:

Extensions

Fields	Critical	Value
Authority Key Identifier	No	11 28 8e f4 56 7b cf bd 80 cb 31 9d 42 82 ed 4a 5c ef 25 a7
CRL Number	No	LAR number

7.3 OCSP profile

The Root CA does not implement any OSCP-type services.

8 Compliance audit and other evaluations

8.1 Frequency and circumstances of evaluations

Every other year, Worldline performs a default compliance audit involving a key ceremony.

8.2 Auditors' identities and qualifications

The audit is performed by an entity in charge of compliance audits and which is independent of the MediaCert Root CA.

8.3 Relationships between auditors and audited entities

This entity is different from the one that administers the MediaCert Root CA.

8.4 Subjects covered by audits

These audits are carried out through sampling and mainly aim to verify compliance with this CP.

8.5 Actions carried out following audit conclusions

The remarks are taken into account within a reasonable time and at the latest for the next key session (signing or revocation of a CA, publication of a CARL).

8.6 Publication of results

The audit is the subject of an internal report.

9 Other business and legal issues

9.1 Prices

Not applicable since this is an internal PKI.

9.2 Financial liability

Not applicable. If applicable, the child CA would be held liable.

9.3 Confidentiality of professional data

Worldline, as Head of the MediaCert PKI, implements the necessary means to ensure the protection of confidential data including:

- the Root CA's private key;
- the activation data of this key and of the HSM used; and
- the CA's information and technical documents.

9.4 Protection of personal data

Not applicable since the data processed by the MediaCert PKI does not contain any personal data.

9.5 Intellectual and industrial property rights

This CP formulates no specific requirements in this regard.

9.6 Contractual interpretations and guarantees

The MediaCert Root CA ensures that

- The private key is protected (integrity and confidentiality) during its generation and throughout the validity periods of the key and activation data.
- Key pairs and certificates are used in the context for which they were issued, in accordance with the applications defined in section 1.4 of this CP.
- The public information specified in section 2.2 of this document is published in a durable, secure manner.
- It will subject itself to the compliance verifications carried out by internal external auditors, and will implement their recommendations.
- Internal operation and use procedures will be properly documented.
- Consistency is maintained between this CP and its associated CPS.
- The trusted staff will be made aware of their obligations.

Worldline ensures that certificate management complies with the requirements specified in the CP and this CPS of the MediaCert PKI.

9.7 Limited guarantee

Not applicable

9.8 Limited liability

Not applicable

9.9 Indemnification

Not applicable

9.10 Validity period and early expiry of the CP

9.10.1 Validity period

The CA's CP remains in force until the last certificate issued in accordance with it expires.

9.10.2 Early end of validity

Compliance work due to a change in the CP does not affect the certificates that have already been issued.

9.10.3 Effects of expiry - Clauses that remain applicable

This CP formulates no specific requirements in this regard.

9.11 Individual notifications and communications between participants

In the event of a significant change in the Root CA, the entities responsible for the child CAs are informed in advance, within a reasonable time.

9.12 Amendments to the CP

The MediaCert Committee is in charge of any amendment made to this CP. The CP may evolve to be consistent with the CA. In the event of a major change, the OID must be modified, which leads to an early renewal of the CA.

9.13 Dispute resolution clause

Potential conflicts are settled internally between:

- the entity responsible for this CA; and
- the MediaCert Committee.

9.14 Jurisdiction

Not applicable

9.15 Compliance with laws and regulations

Not applicable

9.16 Miscellaneous clauses

Not applicable

9.17 Other clauses

Not applicable

10 Annexes

TECHNICAL DOCUMENTATION OF THE MEDIACERT PKI	
Reference	**Description**
[CPS]	Certification Practice Statement of the MediaCert Root PKI MediaCert Certification Authority Reference: ROOT DPC 0021