Introduction must include:
1) Multicert, Serviços de Certificação Electrónica, S.A.
2) Subject:
O = Multicert, Serviços de Certificação Eletrónica S.A.
CN = Multicert Root Certification Authority 01
C = PT
SHA-1 Fingerprint 46:AF:7A:31:B5:99:46:0D:46:9D:60:41:14:5B:13:65:1D:F9:17:0A
SHA256 Fingerprint 60:4D:32:D0:36:89:5A:ED:3B:FE:FA:EB:72:7C:00:9E:C0:F2:B3:CD:FA:42:A1:C7:17:30:E6:A7:2C:3B:E9:D4
CA hierarchy:
This root has internally-operated subordinate CAs:
- MULTICERT - Entidade de Certificação 001 (only issuing crl's)
- MULTICERT Certification Authority 002;
- Multicert Trust Services Certification Authority 001 (For TimeStamping).

3) BR version 1.5.6
4) List the specific versions of the CA's documents that were evaluated, and provide direct URLs to those documents. All provided CA documents must be public-facing, available on the CA's website, and translated into English.
5) If you intend to submit your self-assessment with statements such as "will add/update in our next version of CP/CPS", indicate when you plan to provide the updated documents.
Note: When you are doing your BR Self Assessment, if you find that the required information is not currently in your CP/CPS documents, then you may indicate what your CA currently does, how it is currently documented, that the next version of your CP/CPS will contain this information, and when the next version of your CP/CPS will be available.

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.		Multicert PKI pratices is aligned with CABForum Baseline Requirements 1.5.6 except for the certificate transparency, which will be implemented on April 30th. Also, a few certificate still have a SubAltName with a RFC822Name extension. We are working on their replacement. We are issuing SSL Certificate without this extension since February 2016. CAA Records validation is beeing performed since 2017 August 31th We are working on a new revision of the CPS in order to include the validity of 2 years for SSL certificate, wich is in place since february. Considering we are reviewing the CP's and CPS's to be compliant to RFC 3647 until May 31th, Multicert is taking this opportunity to restructure the Public Documentation in order to have only a CPS and a CP document, compliant with the RFC 3647 and with all the missing information detected throughout this assessment.

1.2.2. Relevant Dates Note the Compliance date for eachitem in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.		Multicert PKI pratices is aligned with CABForum Baseline Requirements 1.5.6 except for the certificate transparency, which will be implemented on April 30th. Also, a few certificate still have a SubAltName with a RFC822Name extension. We are working on their replacement. We are issuing SSL Certificate without this extension since February 2016. CAA Records validation is beeing performed since 2017 August 31th We are working on a new revision of the CPS in order to include the validity of 2 years for SSL certificate, wich is in place since february.
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	CPS CA002 (cap. 1.3.2)	Multicert has 3 RA`s that **onlyissues qualfied certificates for eletronic signature** for persons (members of associations "Doctor's Order", "Order of Pharmaceuticals" and the Parliament). These RA's are subject to annual audits made by a CAB.
2.1. Repositories Provide the direct URLs to the CA's repositories	CPS CA002 (cap. 1.2, cap. 2.2)	pki.multicert.com URL included in the CPS.
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	CPS CA002 (cap. 2.2)	MULTICERT CA complies with the current version of the baseline requirements for the Issuance and Management of Publicly-Trusted Certificates, published by CA/Browser Forum in the document “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, available at http://www.cabforum.org. In case there is any inconsistency between this document and the described in the Baselines document, the information in the document issued by the CA/Browser Forum overlaps what is described in this document.
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.		Valid: https://demo.mtrust.online Revoked: https://revoked.mtrust.online
2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	CPS CA002 (cap. 2.3)	The CPS is updated annually. The Webserver CP is updated annually.
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	CPS CA002 (Cap. 2)	The information published by MULTICERT S.A. shall be available on the Internet, being subject to access control mechanisms (read-only access). MULTICERT S.A. has implemented physical and logical security measures in order to prevent the addition, deletion, and change of the records in the repository by unauthorized people.

3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	CP Webserver(cap. 5)	These are the procedures in place in order to issue SSL certificates: • Confirmation that the certificate applicant has the Domain Name registration directly at the domain registrar ; • Direct communication with the responsible for the Domain Name, using the address, email or phone number provided by the domain registrar; • Direct communication with the responsible for the Domain Name using the contact information listed in the file "registrant", "technical" or "administrative" of WHOIS database ; • Communication with the domain administrator using the email address created with the prefix "admin", "administrator", "webmaster", "hostmaster" or "postmaster", followed by the "@" symbol and the Domain Name; • Trust in a Domain Authorization Document; • Statement by the Applicant that he/she has practical control over the Fully Qualified Domain Name, by pre-agreement on an amendment to certain information contained in an online Web page identified by a URI that contains the Fully Qualified Domain Name; or • Using any other method of confirmation (as long as it provides the same level of reliability of the verification methods mentioned above), and the CA will keep the record as evidence to confirm that the Applicant is responsible for the Domain Name or has control over the Fully Qualified Domain Name.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS CA002 (cap 3.1.6 e 3.2.1.3)	The validation of these certificates' applicants is performed through attesting documents issued by credible entities, which allow verifying the data of the organisation which requires the certificate, as well as its legal representatives' data (e.g. Legal document of Entity Constitution or Natural Person).
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS CA002 (cap. 3.2.1.3)	The validation of these certificates' applicants is performed through attesting documents issued by credible entities, which allow verifying the data of the organisation which requires the certificate, as well as its legal representatives' data (e.g. Legal document of Entity Consitution or Natural Person).

3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.	CPS CA002 (cap. 3.2.1.3) CP Web server (cap. 5)	The validation of these certificates' applicants is performed through attesting documents issued by credible entities, which allow verifying the data of the organisation which requires the certificate, as well as its legal representatives' data (e.g. Legal document of Entity Constitution or Natural Person). CP describes the different resources that can be consulted in order to confirm the trustfullness of the information provided in the certificate request form (ex: consulting the WHOIS database, etc). These are the procedures in place in order to issue SSL certificates: • Confirmation that the certificate applicant has the Domain Name registration directly at the domain registrar ; • Direct communication with the responsible for the Domain Name, using the address, email or phone number provided by the domain registrar; • Direct communication with the responsible for the Domain Name using the contact information listed in the file "registrant", "technical" or "administrative" of WHOIS database ; • Communication with the domain administrator using the email address created with the prefix "admin", "administrator", "webmaster", "hostmaster" or "postmaster", followed by the "@" symbol and the Domain Name; • Trust in a Domain Authorization Document; • Statement by the Applicant that he/she has practical control over the Fully Qualified Domain Name, by pre-agreement on an amendment to certain information contained in an online Web page identified by a URI that contains the Fully Qualified Domain Name; or • Using any other method of confirmation (as long as it provides the same level of reliability of the verification methods mentioned above), and the CA will keep the record as evidence to confirm that the Applicant is responsible for the Domain Name or has control over the Fully Qualified Domain Name.
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CP Web server (cap. 5.1 and 5.2) - en version	For each IP address listed in the certificate, the CA confirms that, to date of issuance of the certificate, the Applicant has control over the IP address (ex: obtaining information about the assignment of the IP address from the Internet Assigned Numbers Authority or Regional Internet Registry, etc).
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CP Web server (cap. 5.1 and 5.2) - en version	The CA confirms that, to date of issuance of the certificate, the certificate applicant is the Domain Name responsible or has control over the Full Qualified Domain Name (ex: direct communication with the responsible for the domain name using the contact information listed in the WHOIS database, etc).
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CP Web server (cap. 5.1) - en version	The CA confirms that, to date of issuance of the certificate, the certificate applicant is the Domain Name responsible or has control over the Full Qualified Domain Name (ex: through communication with the domain administrator using the email address created with the prefix "admin", "administrator", "webmaster", "hostmaster" or "postmaster", followed by the "@" symbol and the Domain Name)

3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CP Web server (cap. 5.1 and 5.2) - en version	The CA confirms that, to date of issuance of the certificate, the certificate applicant is the Domain Name responsible or has control over the Full Qualified Domain Name (ex: consulting the WHOIS database, etc).
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N.A.	
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N.A.	
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CP Web server (cap. 5.2) - en version	For each IP address listed in the certificate, the CA confirms that, to date of issuance of the certificate, the Applicant has control over the IP address (ex: Obtaining information about the assignment of the IP address from the Internet Assigned Numbers Authority (IANA), etc).
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N.A.	
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N.A.	
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	CP Web server (cap. 5.2) - en version	For each IP address listed in the certificate, the CA confirms that, to date of issuance of the certificate, the Applicant has control over the IP address (consulting IANA, statement of the applicant, research the IP, etc).
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.	N.A.	
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	CPS CA002 (CAP - 3.2.1.3)	The validation of these certificates' applicants is performed through attesting documents issued by credible entities, which allow verifying the data of the organisation which requires the certificate, as well as its legal representatives' data (e.g. Legal document of Entity Constitution or Natural Person).
3.2.2.8 CAA Records		CAA Records is executed manually, however the solution was automated and will be in production until April 30th.

3.2.3. Authentication of Individual Identity	CPS CA002 (CAP - 3.2.1.3)	The validation of these certificates' applicants is performed through attesting documents issued by credible entities, which allow verifying the data of the organisation which requires the certificate, as well as its legal representatives' data (e.g. Legal document of Entity Constitution or Natural Person).
3.2.5. Validation of Authority	CPS CA002 (CAP - 3.2.1.3)	The validation of these certificates' applicants is performed through attesting documents issued by credible entities, which allow verifying the data of the organisation which requires the certificate, as well as its legal representatives' data (e.g. Legal document of Entity Constitution or Natural Person).
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	N.A.	
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CPS CA 002 (cap. 4.3.1)	The Registry Administrators team validates all incoming applicants and their authencity.
4.1.2. Enrollment Process and Responsibilities	CPS CA002 (cap. 4.1) CPS CA002 (cap. 4.5)	The request of issuance of any certificate to MULTICERT CA begins with the filling of a form, which is appropriate to the desired certificate, and the application is only accepted if the terms and conditions, and the subscriber agreement is accepted as well.
4.2. Certificate application processing		
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	CPS CA002 (cap. 4.1) CP Web server (cap. 5.1, 5.2) - en version	The request of issuance of any certificate to MULTICERT CA begins with the filling of a form which is appropriate to the desired certificate. This form has to be sent on paper to MULTICERT, All documentation, which confirms the administrators identity and powers, is verified using Legal Documents, and a call is made to the public telephone number in order to identifiy if a certificate resquest was made to Multicert. This call is recorded. The CA confirms that, to date of issuance of the certificate, the certificate applicant is the Domain Name responsible or has control over the Full Qualified Domain Name.
4.2.2. Approval or Rejection of Certificate Applications	CPS CA002 (cap. 4.2.2)	Multicert only aprooves applications if the domain is already registed in a third party database (f.g www.whois.net)
4.3.1. CA Actions during Certificate Issuance	CPS CA002 (cap 4.3.1, cap. 4.3.2) CPS Root (cap 5.2.1)	Any certificate issued in the Multicert PKI has to be approved. This approval depends on the type of certificate and the Certification Authority envolved. For end-user certificates approval, the Registry Administration Working Group is responsible for managing and processing certificate requests. Multicert Root Certification Authority only issues certificates (for Subordinate CA's or OCSP) with the intervention of 1 System Auditor, 1 System Administrator and 1 Securty Officer.
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	4.9.1 CPS CA002	All possibles situations that can induce in a revocation are listed in the Certification Pratice Statment.
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	5.2 CP SUBEC	http://pkiroot.multicert.com/politicas/MULTICERT_PJ.ECRAIZ_405_pt.pdf
4.9.2. Who Can Request Revocation	5.2 CP SUBEC	
4.9.3. Procedure for Revocation Request	5.2 CP SUBEC	

4.9.5. Time within which CA Must Process the Revocation Request	4.9.5 CPS CA002 5.2 CP SUBEC	CPS CA002: Multicert guarantees the publication of the new status of the certificate 24 hours after the request for revocation whenever it proves to be reliable. CP SUBEC: Multicert will immediately assess the request and, within 5 working days, it will issue a verdict to the requesting entity, as well as the entity holding the certificate to be revoked.
4.9.7. CRL Issuance Frequency	CPS CA002 (cap 2.3, cap 4.9.6)	CRL is published at least once a week. Delta CRL is published in a daily basis
4.9.9. On-line Revocation/Status Checking Availability	CPS (cap 4.9.7)	. The OCSP respondes are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. This information is will be updated to the CPS until May 30th.
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.		Multicert OCSP GET support is implemented in a manner equivalent to the commonly used POST. In this way, we don't have pre-generated responses , and although each response has a designated ttl, if the client issues another query then we will present a freshly produced response. Since each status update is immediately propagated from the CA to the OCSP, every response issued is coherent with the certificate status known by the CA.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	N.A.	
4.10.1. Operational Characteristics	4.10.1 CPS	The status of the issued certificates is openly available through CRLs, Delta-CRLs and OCSP service.
4.10.2. Service Availability	4.10.2 CPS	The service on the status of the certificate is available 24 hours a day, 7 days a week.
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS		
5.2.2. Number of Individuals Required per Task	5.2.2 CPS	There are rigorous control procedures that require the division of responsibilities based on the specificities of each Working Group, and in order to ensure that sensitive tasks can only be performed by a multiple group of authenticated people. The internal control procedures were elaborated in order to ensure a minimum of 2 authenticated individuals to be able to have physical and logical access to the security equipment. The access to the CE's cryptographic hardware follows strict procedures involving multiple individuals authorized to access to it during its life cycle, from reception and inspection to physical and/or logical destruction of the hardware. After the activation of a module with operational keys, additional access controls are used in order to ensure that the physical and logical accesses to the hardware are only possible with 2 or more authenticated individuals. Individuals with physical access to the modules do not hold the activation keys and vice-versa.
5.3.1. Qualifications, Experience, and Clearance Requirements	5.3.1. CPS	The admission of new members in the Working Groups is only possible if they present proof of the required knowledge, qualifications and experience to perform the tasks of the Working Groups.

5.3.3. Training Requirements and Procedures	5.3.3 CPS	Adequate training and experience is given to the members of the Working Groups in order to perform their tasks in a satisfactory and competent manner. The Working Group elements are additionally subject to a training and experience plan, including the following topics: a) Digital certification and Public Key Infrastructures; b) General concepts on information security; c) Specific training for their role inside the Working Group; d) Operation of software and/or hardware used in the CE; e) Certificate Policy and Certification Practices Statement; f) Recovery from disasters; g) Procedures for the continuation of the activity, and h) Basic legal aspects regarding the certification services.
5.3.4. Retraining Frequency and Requirements	5.3.4.CPS	Whenever necessary, complementary training and experience shall be provided to the Working Group members, in order to ensure the required professional level for the competent and satisfactory performance of their responsibilities. In particular, – Whenever there are any technological change, introduction of new tools or changes in the procedures, an adequate training is given to all personnel allocated to the CE; – Whenever there are changes introduced to the Certificate Policies or Certification Practices Statement, recycling sessions are held for all the elements of the CE
5.3.7. Independent Contractor Controls	5.3.7 CPS	Independent consultants or service providers have permission to access the high security zone as long as they are escorted and directly supervised by Working Group members, and after taking notice and accepting the Confidentiality Privacy Statement for External Contributor or Guest 13, existing for this purpose.
5.4.1. Types of Events Recorded	5.4.1 CPS	Significant events generate auditable records. These include at least the following: – Request, issuance, renewal, reissuance and revocation of certificates; – CRL publication; – Events related with safety issues, including: o Access attempts (successful or not) to sensitive CE's resources; o Operations performed by members of the Working Groups, o Physical safety devices of entry/exit of several levels of security. The entries in the records include the following information: – Serial number of the event; – Date and time of the event; – Identity of the individual who caused the event; – Category of the event; – Description of the event
5.4.3. Retention Period for Audit Logs	5.4.3 e 5.5 do CPS	he records are maintained for at least 2 (two) months after processing, and then stored at least for 7 years
5.4.8. Vulnerability Assessments	5.4.8 do CPS	The auditable records are regularly assessed in order to minimize and eliminate potential attempts to break the system security.
5.5.2. Retention Period for Archive	5.4.3 e 5.5 do CPS	The auditable records are regularly assessed in order to minimize and eliminate potential attempts to break the system security.
5.7.1. Incident and Compromise Handling Procedures	5.7.1 CPS	Auditable events are registered in the audit system and stored in a safe way, without notification to the event causing subject.

6.1.1. Key Pair Generation	6.1.1 CPS	The generation of cryptographic keys from self-signed MULTICERT CA is done by a Working Group, composed by authorized elements for that purpose, in a ceremony planned and audited according to the written procedures for the operations to perform. All key creation ceremonies are registered, dated and signed by the elements involved in the Working Group. The cryptographic hardware used for the generation of keys from MULTICERT CA is compliant with the FIPS 140-2 level 3 and/or Common Criteria EAL 4+ requirements, and performs the key maintenance, storage, and all the operations involving cryptographic keys using the hardware exclusively. The access to critical keys is protected by security policies, role division between the Working Groups, as well as through limited user access rules. The backup copies from cryptographic keys are done using only the hardware, thus allowing the proper audit of these copies, and a full and safe recovery of the keys in the event of a data loss. The private key for the certificates issued to a natural or collective person are generated by MULTICERT CA using cryptographic hardware compliant with FIPS 140-2 level 3 and/or Common CriteriaEAL 4+ requirements.
6.1.2. Private Key Delivery to Subscriber	6.1.2 CPS	The delivery of the private key associated to the certificates of a natural or collective person is performed in SSCD cryptographic device (Secure Signature-Creation Device). For SSL certificates the private key is generated and stored by the holder
6.1.5. Key Sizes	6.1.5	The keys sizes are at least 2048 bit
6.1.6. Public Key Parameters Generation and Quality Checking	6.1.6	The generation of the public key parameters and quality check shall always be based on the standard that defines the algorithm. The CA's keys are generated based on the use of random/pseudo random processes described on ANSI X9.17 (Annex C), according to the stipulated in PKCS#11
6.1.7. Key Usage Purposes	6.1.7 and 7.1. CPS and CP (ver cap)	The keys usage is defined according to the purpose of the certificate profile. SSL certicates: KU --> Digital Signature Root Certificate: KU--> Certificate Signing and CRL signing
6.2. Private Key Protection and Cryptographic Module Engineering Controls	6.2.CPS	**Safety standards and measures of the cryptographic module** --> For the generation of the key pairs from MULTICERT CA, as well as for the storage of the private keys,MULTICERT uses a cryptographic module in hardware thaht complies with Common Criteria EAL 4+ and/or FIPS 140-2, level 3 . **Multi-personnel control (n of m) for the private key**--> The activation data necessary for using the private key from MULTICERT CA are divided in several parts (stored in the PED keys – small digital identification tokens, with physical USB pen format, identifying different access roles to HSM), being accessible, and at the responsibility of different members of the Working Group. A defined number of these parts (n) from the total number of parts (m) is necessary to activate the private key from MULTICERT CA stored in the hardware cryptographic module. Two parts (n) are necessary for the activation of the private key form MULTICERT CA
6.2.5. Private Key Archival	6.2.5 and 4.12 CPS	The private key from MULTICERT CA is stored in a security hardware token and a backup copy is made using a direct connection hardware to hardware between two security tokens. The backup copy creation is the last step for issuing a new key pair from MULTICERT CA. This backups are only available to Security officers.
6.2.6. Private Key Transfer into or from a Cryptographic Module	6.2.6 CPS	The private keys from Multicert CA are not extractable from the cryptographic token FIPS 140-2 level 3. Even if a backup copy of the private keys from Multicert CA is made to another cryptographic token, that copy is done directly, hardware to hardware, thus ensuring the transport of the keys between modules in an enciphered transmission.
6.2.7. Private Key Storage on Cryptographic Module	6.2.1 and 6.2.7 CPS	For the generation of the key pairs from MULTICERT CA, as well as for the storage of the private keys,MULTICERT uses a cryptographic module in hardware that complies with Common Criteria EAL 4+ and/or FIPS 140-2, level 3.
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	6.3.2 CPS	The period to use the keys is determined by the certificate's validity period, so that after the certificate expires, its keys can no longer be used, originating the permanent termination of the operability and use for which they were meant. In this sense, the validity of the various types of certificates and the period in which these should be renewed is the following: SSL certificates has a maximum validity of 24 months.

6.5.1. Specific Computer Security Technical Requirements	6.5.1 CPS	The access to the servers from MULTICERT CA is restrict to the members of the Working Groups with a valid reason for that access. MULTICERT CA works online, and the certificate issuance request is done from the System for Managing the Certificate Life-cycle (SGCVC) and/or the operation console. MULTICERT CA and SGCVC have border protection devices, namely a firewall system, and comply with the necessary requirements for identification, authentication, access control, administration, audit, reuse, service responsibility and recovery, and information exchange.
7.1. Certificate profile	7.1 CPS	The profile of the certificates issued by MULTICERT CA is compliant with: • ITU.T recommendation X. 509; •RFC 5280; •Applicable legislation, national and European • Baseline Requirements from CABForum.
7.1.1. Version Number(s)		Version Number is 3.
7.1.2. Certificate Content and Extensions; Application of RFC 5280		
7.1.2.1 Root CA Certificate	MULTICERT Root CA Certificate Policy	a. basicConstraints This extension appears as a critical extension. The CA field is set TRUE. The pathLenConstraint field is not present. b. keyUsage This extension is present and is marked critical. Bit positions for keyCertSign and cRLSign are set. The Root CA Private Key is used for signing OCSP responses, so the digitalSignature bit is set. c. certificatePolicies This extension is not present. d. extendedKeyUsage This extension is not present.
7.1.2.2 Subordinate CA Certificate	Multicert SubCA Certificate Policy	a. certificatePolicies: This extension is present and is not marked critical. certificatePolicies:1.3.6.1.4.1.25070.1.1.1.0.7 b. cRLDistributionPoints This extension is present and is not marked critical. It contains the HTTP URL of the CA's CRL service: URL=http://pkiroot.multicert.com/crl/root_mc_crl.crl c. authorityInformationAccess : this extension is present. It is not marked critical, and it contains the HTTP URL of the Issuing CA's OCSP responder (http://ocsp.multicert.com/ocsp). d. basicConstraints: This extension is present and is marked critical. The cA field is set true. The pathLenConstraint field is present. e. keyUsage This extension is present and is marked critical. Bit positions for keyCertSign and cRLSign are set.

7.1.2.3 Subscriber Certificate		a. certificatePolicies This extension is present and is marked critical. certificatePolicies: contains the policyIdentifier: 1.3.6.1.4.1.25070.1.1.1.1.0.7 (CPS) and 1.3.6.1.4.1.25070.1.1.1.1.0.1.5 (CP) b. cRLDistributionPoints This extension is present , it is not marked critical, and it contains the HTTP URL of the CA's CRL service: URL=http://ec2pki.multicert.com/crl/crl_mca002.crl c. authorityInformationAccess This extension is present. It is not marked critical, and it contains the HTTP URL of the Issuing CA's OCSP responder (http://ocsp.multicert.com/ocsp). It also contains the HTTP URL of the Issuing CA's certificate (http://ec2pki.multicert.com/cert/mca_002.cer). d. basicConstraints The cA field is not true. e. keyUsage (optional) This extension contains DigitalSiganture, dataEnciphrment, keyEnciphrment. Th bits for keyCertSign and cRLSignare are not set. f. extKeyUsage This extension contains the value id-kp-serverAuth [RFC5280] and/or id-kp-clientAuth [RFC5280] .
7.1.2.4 All Certificates		All other fields and extensions are set in accordance with RFC 5280. The CA does not issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in the CP/CPS.
7.1.2.5 Application of RFC 5280		
7.1.3. Algorithm Object Identifiers		The CAs issue only new Subscriber certificates or Subordinate CA certificates using the SHA-256 hash algorithm (see section 6,1,5 of the CP/CPS
7.1.4. Name Forms		
7.1.4.1 Issuer Information		The content of the Certificate Issuer Distinguished Name field matchs the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280: DN: CN = MULTICERT Root Certification Authority 01 O = MULTICERT - Serviços de Certificação Electrónica S.A. C = PT
7.1.4.2 Subject Information	CP Webserver	
7.1.4.3 Subject Information - Subordinate CA Certificates	CP SubCAS	By issuing a Subordinate CA Certificate, Multicert SubCA's represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.
7.1.5. Name Constraints		The subordinate CA does not contain any Extended Key Usage. The Subscriber Certificates contain Server Authentication as extended Key Usage.
7.1.6. Certificate Policy Object Identifier		
7.1.6.1 Reserved Certificate Policy Identifiers		All issued certificates are under the 1.3.6.1.4.1.25070
7.1.6.2 Root CA Certificates		Multicert Root Certificate does not contain the certificatePolicies extension.
7.1.6.3 Subordinate CA Certificates		All certificates containing a policy identifier (1.3.6.1.4.1.25070.1.1.1.1.7) indicating compliance with these Requirements are issued and managed in accordance with these Requirements. Subscriber certificates do not contain the "anyPolicy" identifier (2.5.29.32.0).

7.1.6.4 Subscriber Certificates		Certificate Policy and/or Certification Practice Statement, all certificates containing a policy identifier (1.3.6.1.4.1.25070.1.1.1.1.7) indicating compliance with these Requirements are issued and managed in accordance with these Requirements. Subscriber certificates do not contain the "anyPolicy" identifier (2.5.29.32.0).
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS		
8.1. Frequency or circumstances of assessment		The compliance audits are performed periodically as foreseen by the regulation. The CA must prove, through audit and anual safety reports (produced by the accredited security auditor), that the risk assessment was assured, having identified and implemented all necessary measures for the information security.
8.2. Identity/qualifications of assessor		The National Accreditation Body (IPAC) is responsible for accrediting the Conformity Assessment Bodies, which are qualified to carry out the conformity assessments resulting from these evaluations, a Conformity Report (CAR) to be made available to the Supervisory Entity, to assess the continuity of availability Of reliable services.
8.4. Topics covered by assessment		The scope of audits and other assessments include the accordance with the national legislation and this CPS and other rules, procedures and processes (especially the ones related with key management operations, resources, management and operation controls and management of the certificates life-cycle)
8.6. Communication of results		The results shall always be communicated to the Supervisory Body
8.7. Self-Audits		A Self Assessment isto performed annualy by internal auditors.
9.6.1. CA Representations and Warranties		MULTICERT CA is obliged to: a) Carry out its operations in accordance with this Policy; b) Clearly state all its Certification Practices in the appropriate document; c) Protect its private keys; d) Issue certificates in accordance with the X.509 standard; e) Issue certificates that are compliant with the information known at the time it is issued and free from data input errors; f) Ensure confidentiality in the data generating process for creating the signature and forwarding it through a safe procedure to the titleholder; g) Use reliable systems and products that are protected against all changes and which ensure the technical and cryptographic safety of the certification processes; h) Use reliable systems to store recognized certificates, that enable proving their authenticity and prevent unauthorised people from changing data; i) Store the certificates issued without any changes; j) Ensure that they can determine the precise date and hour in which it issued, extinguished or suspended a certificate; k) Employ personnel with the necessary qualifications, knowledge, and experience to provide certification services; l) Revoke the certificates under the terms of section "Certificate Suspension and Revocation" of this document and publish the revoked certificates on the CRL in the repository from MULTICERT CA, with the frequency stipulated in section 2.3; m) Publish their CPS and applicable Certificate Policies in its repository guaranteeing the access to current versions; n) Make available, since dully justified the access request, to the previous versions of its CPS as well as the Certificate Policies; o) Notify with the necessary speed, by e-mail the certificate titleholders in case the CE revokes or suspends the certificates, indicating the corresponding motive for such action;

9.6.1. CA Representations and Warranties		p) Collaborate with the audits performed by the Accreditation Authority to validate the renewal of its own keys; q) Operate in accordance with the applicable legislation; r) Protect eventual existing keys that are under its custody; s) Guarantee the availability of the CRL in accordance with the dispositions, t) In case its activity ceases this shall be communicated with a minimum prior notice of two months to all titleholders of the certificates issued, as well as to the Accreditation Authority; u) Comply with the specifications contained in the standard on Protection of Personal Data; v) Maintain all information and documentation relative to a recognised certificate and the Certification Practices Statements in force at each moment and for fifteen years from issuance; and w) Make the certificates from MULTICERT CA available.
9.6.3. Subscriber Representations and Warranties		It is the obligation of the titleholders of the issued certificates to: a) Limit and adjust the use of the certificates in accordance with the uses foreseen in the Certificate policies; b) Take all care and measures necessary to guarantee possession of its private key; c) Immediately request that a certificate be revoked in the case of having knowledge or suspicion that the private key corresponding to the public key contained in the certificate has been compromised, according to section 0; d) Not use a digital certificate that has lost its effectiveness, both due to revocation, suspension or expiration of its validity period; e) Submit to the Certifying Entity (or Registration Entity) the information that they consider accurate and complete with relation to the data that these require to carry out the registration process. The CE should be informed on any changes in this information; and f) Not monitor, manipulate or carry out reversed engineering on the technique implemented (hardware and software) for certification services, without the previous duly authorization, in writing, from MULTICERT CA
9.8. Limitations of liability		MULTICERT CA: a) shall answer for the damages caused to any person exercising its activity in accordance with Article 26, of the Decree-Law 62/2003; b) shall answer for the damages caused to titleholders or third parties due to lack or delay of including in the consultation service the validity of the certificates, and revocation or suspension of a certificate, once it has knowledge of it; c)shall assume all liability before third parties for the actions of the titleholder for functions necessary to provide certification services; d) The responsibility for the administration / management rests on an objective base and covers all the risks that a private individual may undergo whenever this is a consequence of the normal or abnormal operation of its services; e) shall only answer for damages caused by misuse of the recognised certificate, when the limits of its possible use have not been clearly consigned on the certificate, in a clear recognized way by third parties; f) shall not answer if the electronically signed documents' addressee doesn't comprove them and takes into account the restrictions that are stated in the certificate concerning its possible usage, and g) shall not assume any responsibility in case of loss or damage: ii) Of the services it provides, in the case of war, natural disasters or any other case of force majeure; iii) Resulting from the use of certificates when these exceed the limits set forth in the Certificates Policy and corresponding CPS; iv) Resulting from the undue or fraudulent use of the certificates or CRLs issued by MULTICERT CA.
9.9.1. Indemnification by CAs		In accordance with the legislation in force
9.16.3. Severability		The Regulation 910/2014 requirements shall take precedence over CabForum Baseline Requirements. Untill today no modification was needed to notify. This information will be updated on the next CPS version.