CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)
1) CA's Legal Name: Government of Spain, Autoritat de Certificació de la Comunitat Valenciana (ACCV)
2) Full CA hierarchy ROOT
ACCVRAIZ1
Subject:
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVRAIZ1

Fingerprint:
SHA1: 93:05:7A:88:15:C6:4F:CE:88:2F:FA:91:16:52:28:78:BC:53:64:17
SHA256: 9A:6E:C0:12:E1:A7:DA:9D:BE:34:19:4D:47:8A:D7:C0:DB:18:22:FB:07:1D:F1:29:81:49:6E:D1:04:38:41:13
2) Full CA hierarchy SUBCA
ACCVCA-110 (SHA1)
Subject
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVCA-110

Fingerprint:
SHA1: DB:0E:48:DD:55:97:58:29:61:E9:01:FA:0C:77:FF:21:55:0E:01:10
SHA256: 13:45:C2:D3:9A:E4:B6:5C:CA:71:EB:8E:9A:2B:29:C7:1D:C9:13:F9:52:E9:35:A8:12:B0:04:DB:A7:AE:79:57

2) Full CA hierarchy SUBCA
ACCVCA-110 (SHA2)
Subject
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVCA-110

Fingerprint:
SHA1: 67:7C:DF:63:B9:5E:9E:AE:AE:69:6F:44:50:67:18:FE:0D:2F:6E:41
SHA256: E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:FC:2F:0B:11
2) Full CA hierarchy SUBCA
ACCVCA-120 (SHA1)
Subject
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVCA-120

Fingerprint:
SHA1: 9F:CD:F0:94:36:8D:1B:02:5C:4C:55:74:F8:C5:9D:B8:DF:75:D0:C3
SHA256: 3B:C5:18:56:04:0A:D7:FF:66:83:AA:85:A0:D3:4F:9E:A6:80:CD:23:C3:7C:B8:A0:42:3B:0F:89:A2:44:05:B9
2) Full CA hierarchy SUBCA
ACCVCA-120 (SHA2)
Subject
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVCA-120

Fingerprint:
SHA1: 48:72:A4:C3:DF:17:4C:EF:34:D7:7F:E6:A3:B4:E7:BE:7D:F2:D2:5D
SHA256: 2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2
2) Full CA hierarchy SUBCA
ACCVCA-130 (SHA1)
Subject
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVCA-130

Fingerprint:
SHA1: 28:97:F9:B6:52:9C:6A:AF:B4:3C:32:FF:C6:25:E1:F6:49:40:1C:2C
SHA256: 8F:7C:C4:55:E9:A5:50:78:04:12:06:55:D7:13:91:86:25:3E:43:B0:04:22:E7:34:26:3A:07:69:D2:F8:9F:7D
2) Full CA hierarchy SUBCA
ACCVCA-130 (SHA2)
Subject
C = ES,O = ACCV,OU = PKIACCV,CN = ACCVCA-130

Fingerprint:
SHA1: 00:55:B7:7F:43:2B:54:24:54:06:06:8C:C8:F7:78:05:C3:25:DC:F5
SHA256: 57:2B:F8:99:FD:77:43:62:DC:19:21:96:25:EC:C1:57:BB:55:43:4E:A5:16:6D:57:58:DC:4B:4F:89:0D:66:53
3)
Baseline 1.5.7, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.
4)
CPS: https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V4.0.1-EN-2018.pdf
CP:https://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-3V4.0.1-EN-2018.pdf

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**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.*	*CA is fully compliant with all items in the table*	*CA is fully compliant with all items in the table*
1.2.2. Relevant Dates Note the Compliance date for each item 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.*	*CA is fully compliant with all items in the table*	*CA is fully compliant with all items in the table*
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: 1.3.2	CA does not allow for Delegated Third Parties
2.1. Repositories *Provide the direct URLs to the CA's repositories*	CPS: 2.1	OCSP: http://ocsp.accv.es CRL: ACCVRAIZ1: http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl ACCVCA-110: https://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl ACCVCA-120: https://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCVCA-130: https://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl
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)*	Certificación Electrónica (ACCV) is adjusted to the recent version of the document ". Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ", published at https://www.cabforum.org/ . In case of any incompatibility between this Certification Policy and the CAB Forum requirements, those requirements will prevail over the current 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.*	CPS: 2.2 CP: 2.2	Test sites: https://activo.accv.es/test/hola.html valid https://revocado.accv.es:442/test/hola.html revoked https://caducado.accv.es:444/test/hola.html expired
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: https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V4.0.1-EN-2017.pdf CP: https://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-03V3.0.1-EN-2017.pdf
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: 2.4	*All Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs are publicly available.*
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 3.2.2 3.2.3 CPS 3.2.2 3.2.3	CPS: 3.2.2 If Certification Policy deems it necessary for an organization's identity to be authenticated, this policy shall determine the necessary methods for verifying the aforementioned identity. However, ACCV assumes no commitments in the issuance of certificates about the use of a trademark. Not deliberately allowing the use of a name whose right of use, is not owned by the subscriber. However, ACCV is not obliged to look for evidence of the possession of registered trademarks before the issuance of certificates. In the event of a dispute, ACCV may refuse or suspend any certificate without any responsibility. ACCV uses the mechanisms established by the current technical regulations, specifically from Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market. See corresponding Policy. CPS: 3.2.3 The process of individual identification is defined by the Certification Policy applicable for each type of certificate. As a general rule, remote methods of identification that are different from the digital signature produced with certificates issued by ACCV itself or by any other recognised Certification Services Provider, shall not be used. ACCV uses the mechanisms established by the current technical regulations, specifically from Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market. See corresponding Policy. CP: 3.2.2 The right to apply for certificates that is defined in the current Certification Policy is limited to natural persons. Certificate application carried out in name of legal entities, bodies or organizations will not be accepted. Authentication of the identity of the applicant of a certificate is made through the use of his/her personal certificate qualified for the signing the request for the website qualified certificate. The applicant must submit the necessary documentation which determines The information related to the organization as the inclusion in the corresponding commercial register, address, locality, state or province, country, operating codes, etc.. The necessary representative capabilities of the entity that owns the referred domain. The domain possession (3.2.4). This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this. ACCV will check the supplied data (including the country of the applicant) using for this the available information of Data Protection Agencies Public Administrations register Commercial register Verification services and Consultation of identity data requiring to the applicant the explanations or additional documents that it could consider necessary. All agencies and registers used are official and of high reliability, providing traceable evidence of all searches. ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check. CP: 3.2.3 Certificate's applicant identification will be carried out by the use of his/her qualified personal certificate for the signing the request for the website qualified certificate. The applicant must submit the necessary documentation which determines the representative capabilities of the entity that owns the referred domain and, which also determines that domain possession. This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this task (3.2.4) ACCV will check the supplied data (including the country of the applicant) using for this the available information of Data Protection Agencies Public Administrations register Commercial register Verification services and Consultation of identity data requiring to the applicant the explanations or additional documents that it could consider necessary. All agencies and registers used are official and of high reliability, providing traceable evidence of all searches. ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check.

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.*	CP 3.2.2 3.2.3 CPS 3.1.6 3.2.2 3.2.3	Authentication of the identity of the applicant of a certificate is made through the use of his/her personal certificate qualified for the signing the request for Secure Server SSL Certificate. The requester must submit the necessary documentation which determines the information related to the organization as the inclusion in the corresponding commercial register, address, operating codes. The necessary representative capabilities of the entity that owns the referred domain. This submitting will be carried out digitally using the sources and applications that the ACCV provided to the users for this. ACCV will check the data using for this the available information of personal and domain registers, requiring to the applicant the explanations or additional documents that it could consider necessary. ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check. ACCV deliberately prohibits the use of a name whose right of use is not the property of the subscriber. However, the CA is not required to seek evidence of trademark ownership prior to issuing certificates.
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.*	CP 3.2.2 3.2.3 To verify the country, official records are used along with name registration information.	CP: 3.2.2 3.2.3 The right to apply for certificates that is defined in the current Certification Policy is limited to natural persons. Certificate application carried out in name of legal entities, bodies or organizations will not be accepted. Authentication of the identity of the applicant of a certificate is made through the use of his/her personal certificate qualified for the signing the request for the website qualified certificate. The applicant must submit the necessary documentation which determines The information related to the organization as the inclusion in the corresponding commercial register, address, locality, state or province, country, operating codes, etc.. The necessary representative capabilities of the entity that owns the referred domain. The domain possession (3.2.4). **This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this.** **ACCV will check the supplied data (including the country of the applicant) using for this the available information of** **Data Protection Agencies** **Public Administrations register** **Commercial register** **Verification services and Consultation of identity data** requiring to the applicant the explanations or additional documents that it could consider necessary. All agencies and registers used are official and of high reliability, providing traceable evidence of all searches. ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check.
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.***	CP: 3.2.4 We are using: 3.2.2.4.2 3.2.2.4.3 3.2.2.4.4	ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. ACCV will not issue certificates to IP addresses or private domain names. In the case of gTLD, only certificates with approved gTLD names will be issued, and will only be issued to subscribers who have control of the gTLD, as it appears in ICANN. Specifically: By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at http://www.nic.es or equivalent for national domains, or the provided for generic domains by ICANN (whois.icann.org). ACCV will use this information to contact by mail and landline phone with registrant until confirming the data accuracy. Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name. ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es" In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed. If it is a certificate with a wildcard character (*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix). In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.
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.*	N/A	
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.*	CP: 3.2.4	ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. Specifically: By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at http://www.nic.es or equivalent for national domains, or the provided for generic domains by ICANN (whois.icann.org). ACCV will use this information to contact by mail and landline phone with registrant until confirming the data accuracy. Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. **Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number** Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name. ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es" In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed. If it is a certificate with a wildcard character (*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix). In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.
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: 3.2.4	ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. ACCV will not issue certificates to IP addresses or private domain names. In the case of gTLD, only certificates with approved gTLD names will be issued, and will only be issued to subscribers who have control of the gTLD, as it appears in ICANN. Specifically: By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at http://www.nic.es or equivalent for national domains, or the provided for generic domains by ICANN (whois.icann.org). ACCV will use this information to contact by mail and landline phone with registrant until confirming the data accuracy. Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number **Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name.** ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es" In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed. If it is a certificate with a wildcard character (*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix). In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.
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: 3.2.4	ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. Specifically: By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at http://www.nic.es or equivalent for national domains, or the provided for generic domains by ICANN (whois.icann.org). ACCV will use this information to contact by mail and landline phone with registrant until confirming the data accuracy. Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number **Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number** Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name. ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es" In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed. If it is a certificate with a wildcard character (*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix). In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.
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.*	N/A	
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.*	N/A	
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.*	N/A	

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.*	CP: 3.2.4	ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. Specifically: By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at http://www.nic.es or equivalent for national domains, or the provided for generic domains by ICANN (whois.icann.org). ACCV will use this information to contact by mail and landline phone with registrant until confirming the data accuracy. Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name. ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es" In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed. **If it is a certificate with a wildcard character (*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix).** In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	CP: 3.2.2 3.2.3	CP: 3.2.2 3.2.3 The right to apply for certificates that is defined in the current Certification Policy is limited to natural persons. Certificate application carried out in name of legal entities, bodies or organizations will not be accepted. Authentication of the identity of the applicant of a certificate is made through the use of his/her personal certificate qualified for the signing the request for the website qualified certificate. The applicant must submit the necessary documentation which determines The information related to the organization as the inclusion in the corresponding commercial register, address, locality, state or province, country, operating codes, etc.. The necessary representative capabilities of the entity that owns the referred domain. The domain possession (3.2.4). This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this. ACCV will check the supplied data (including the country of the applicant) using for this the available information of Data Protection Agencies Public Administrations register Commercial register Verification services and Consultation of identity data requiring to the applicant the explanations or additional documents that it could consider necessary. **All agencies and registers used are official and of high reliability, providing traceable evidence of all searches.** ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check.
3.2.2.8 CAs MUST check and process CAA records *Indicate your CA's understanding that this section is a requirement as of September 8, 2017, and how your CA meets the requirements in this section of the BRs.*	CP: 3.2.4	ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. Specifically: By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at http://www.nic.es or equivalent for national domains, or the provided for generic domains by ICANN (whois.icann.org). ACCV will use this information to contact by mail and landline phone with registrant until confirming the data accuracy. Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name. **ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es"** In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed. If it is a certificate with a wildcard character (*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix). In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.
3.2.3. Authentication of Individual Identity	CP: 3.2.3	
3.2.5. Validation of Authority	N/A	
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.	CP: 4.1	This type of certificates request is the responsibility of private or public entities. The process starts by accessing to the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc. If the websites authentication certificate that is linked to an entity is requested for the first time, the applicant must attach the document that accredits him/her as a qualified person for carrying out this application (document certifying the employment relationship or an official journal where the associated information is collected, notarial powers and registration in the corresponding registries), in PDF format digitally signed. If the access has been carried out with a certificate that accredits the necessary capability for managing the websites authentication certificates, the Organization, Organizational Unit and the Occupation data of certificate will be used. **ACCV keeps the information associated with the requests indefinitely (with a limit of at least 15 years), including its approval or rejection, and the reasons thereof.**
4.1.2. Enrollment Process and Responsibilities	CP: 4.2 4.4	**After receiving the certificate request in electronic format** through the application by the authorized persons and once the economic proposition is accepted, it will proceed to the application approval. After the acceptance, the Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email that is listed in the request. The user must go into the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc identifying himself/herself with a personal qualified certificate for generating and downloading the certificate. ACCV will check the application data and accredit the applicant for the websites authentication certificate application, during 13 months since the approval with no need of submitting any additional documentation. In case of identifying with public employee certificate there is no temporal limit existent while the certificate is still in force. In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2, 3.2.3 and 3.2.4 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application. This acceptance will be carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is carried out using the established capabilities in the management application. In this process, ACCV will check that certificate requests do not include domains that can be used for phishing or other fraudulent uses, using available mechanisms and lists. ACCV will use this information to decide on new applications. The certificates acceptance by the subscribers part is carried out in the moment of the certification contract acceptance associated to each Certification Policy. The contract acceptance involves the knowledge and acceptance of the associated Certification Policy by the subscriber part. The Certification Contract is a document that must be accepted by the applicant, and which purpose is to link the person who applies for the website authentication certificate, and the knowledge of usage rules and the submitted data veracity. The Certification Contract form is collected in the Annex I of this Certification Policy. **The user must accept the contract prior to the issuance of a Certificate.**
4.2. Certificate application processing	CP: 4.2	After receiving the certificate request in electronic format through the application by the authorized persons and once the economic proposition is accepted, it will proceed to the application approval. After the acceptance, the Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email that is listed in the request. The user must go into the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc identifying himself/herself with a personal qualified certificate for generating and downloading the certificate. ACCV will check the application data and accredit the applicant for the websites authentication certificate application, during 13 months since the approval with no need of submitting any additional documentation. In case of identifying with public employee certificate there is no temporal limit existent while the certificate is still in force. In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2, 3.2.3 and 3.2.4 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application. This acceptance will be carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is carried out using the established capabilities in the management application. In this process, ACCV will check that certificate requests do not include domains that can be used for phishing or other fraudulent uses, using available mechanisms and lists. ACCV will use this information to decide on new applications.
4.2.1 Re-use of validation information is limited to 825 days *Indicate your CA's understanding that this is a requirement as of March 1, 2018, and indicate how your CA meets the requirements of this section.*	CP: 4.2	After receiving the certificate request in electronic format through the application by the authorized persons and once the economic proposition is accepted, it will proceed to the application approval. After the acceptance, the Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email that is listed in the request. The user must go into the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc identifying himself/herself with a personal qualified certificate for generating and downloading the certificate. **ACCV will check the application data and accredit the applicant for the websites authentication certificate application, during 13 months since the approval with no need of submitting any additional documentation. In case of identifying with public employee certificate there is no temporal limit existent while the certificate is still in force.** In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2, 3.2.3 and 3.2.4 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application. This acceptance will be carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is carried out using the established capabilities in the management application. In this process, ACCV will check that certificate requests do not include domains that can be used for phishing or other fraudulent uses, using available mechanisms and lists. ACCV will use this information to decide on new applications.
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.*	CP: 4.2	After receiving the certificate request in electronic format through the application by the authorized persons and once the economic proposition is accepted, it will proceed to the application approval. After the acceptance, the Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email that is listed in the request. The user must go into the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc identifying himself/herself with a personal qualified certificate for generating and downloading the certificate. ACCV will check the application data and accredit the applicant for the websites authentication certificate application, during 13 months since the approval with no need of submitting any additional documentation. In case of identifying with public employee certificate there is no temporal limit existent while the certificate is still in force. In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2, 3.2.3 and 3.2.4 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application. This acceptance will be carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is carried out using the established capabilities in the management application. **In this process, ACCV will check that certificate requests do not include domains that can be used for phishing or other fraudulent uses, using available mechanisms and lists.** **ACCV will use this information to decide on new applications.**
4.2.2. Approval or Rejection of Certificate Applications	CP: 4.2	After receiving the certificate request in electronic format through the application by the authorized persons and once the economic proposition is accepted, it will proceed to the application approval. After the acceptance, the Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email that is listed in the request. The user must go into the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc identifying himself/herself with a personal qualified certificate for generating and downloading the certificate. ACCV will check the application data and accredit the applicant for the websites authentication certificate application, during 13 months since the approval with no need of submitting any additional documentation. In case of identifying with public employee certificate there is no temporal limit existent while the certificate is still in force. In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2, 3.2.3 and 3.2.4 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application. This acceptance will be carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is carried out using the established capabilities in the management application. In this process, ACCV will check that certificate requests do not include domains that can be used for phishing or other fraudulent uses, using available mechanisms and lists. ACCV will use this information to decide on new applications.
4.3.1. CA Actions during Certificate Issuance	CPS: 4.3	ACCV is not responsible for monitoring, investigating or confirming the accuracy of the information contained in the certificate subsequent to its issue. In the event of receiving information on inaccurate or currently non-applicable information contained on the certificate, the certificate may be revoked. The certificate shall be issued once ACCV has carried out the necessary verification to validate the request for certification. This Certification Policy is the system via which it determines the nature and the method of carrying out these types of verification. When ACCV's CA issues a certificate in accordance with a valid request for certification, it shall send a copy of the certificate to the Registration Authority that issued the request and another to ACCV's repository. It is the Registration Authority's responsibility to notify the certificate's subscriber of the certificate issue and to provide him/her with a copy, or failing that, to inform the subscriber of how a copy can be obtained. Everything specified in this section is subordinate to the stipulations of the different Certification Policies for the issue of each type of certificate. **Certificate issuance directly by the Root CA require at least two individual authorized by the CA (manager, system administrator or security manager) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.**
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	CPS: 4.9.1.1	A certificate is revoked when: • The certificate subscriber or the subscriber's keys or the keys of the subscriber's certificates have been compromised by: ◦ The theft, loss, disclosure, modification or other compromise or suspected compromise of the user's private key. ◦ Deliberate improper use of keys and certificates, or failure to observe the operational requirements of the subscription agreement, the associated CP or this CPS. • An actual prerequisite for issue of the certificate has not been fulfilled. • A fundamental factor in the certificate is known to be or is reasonably believed to possibly be false. • A data entry error or other processing error. • The key pair generated by a final user proves to be "weak". • The information contained in a certificate or used to make a request for a certificate becomes inaccurate, for example when the owner of a certificate changes his/her name. • ACCV is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name). • ACCV is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name. • A valid revocation request is received from an end-user. • A valid revocation request is received from an authorized third party, for example a court order. • The certificate of a higher RA or CA in the certificate's hierarchy of trust is revoked The revocation must be made within a period not exceeding 24 hours from the request.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	CPS: 4.9.1.2	A Subordinate CA certificate is revoked when:: • ACCV obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise. • ACCV obtains evidence that the Certificate was misused. • ACCV is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement. • ACCV determines that any of the information appearing in the Certificate is inaccurate or misleading. • ACCV ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate. • ACCV's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository. • Revocation is required by ACCV's Certificate Policy and/or Certification Practice Statement. • The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties. The revocation must be made within a period not exceeding 7 days from the request.
4.9.2. Who Can Request Revocation	CPS: 4.9.2	The revocation of a certificate may be requested by the certificate's subscriber or by ACCV, as well as by anyone who knows conclusively that the data associated with the certificate become inaccurate or incorrect. Certificate subscribers can request certificate revocation for any reason and must request revocation in accordance with the conditions specified in the following section.
4.9.3. Procedure for Revocation Request	CPS: 4.9.3 CP: 4.9.3	The request procedure for revocation of each type of certificate is defined in the corresponding Certification Policy. In general, and without prejudice to the stipulations of the Certification Policies: •Remote revocation requests shall be accepted after a strong identification process based on a ACCV certificate or a certificate of any other recognized Certification Services Provider, and revocation requests submitted via attendance in person shall be accepted if the user identification requirements established for initial registration are fulfilled. •After certificate revocation, the certificate subscriber must destroy the private key that corresponds to the certificate and not use the revoked certificate. There is a request form for certificate revocation on ACCV website at: http://www.accv.es, in the Personal Certification Services Area. A revocation request, whether it is made on paper or electronically (e.g. e-mail o by phone), must contain the information that is described on the revocation request form, referred to in each of the Certification Policies. Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates in the URL https://www.accv.es/contacto/. In that URL are the support email and contact telephones. ACCV accepts revocation applications by the following procedures 4.9.3.1. Telematic By accessing to the Non-Personal Certificates Management Area located at https://npsc.accv.es:8450/npsc the user can revoke the certificates that were requested or the ones he/she has a permit for it.
4.9.5. Time within which CA Must Process the Revocation Request	CPS: 4.9.5	Revocation shall occur immediately when each request verified as valid is processed. There is therefore no period of grace associated with this process.
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	CPS: 4.9.7	ACCV shall publish a new subCA CRL in its repository at maximum intervals of 3 hours, even if there have been no modifications to the CRL (changes to the status of certificates) during the aforementioned period. ACCV shall publish a new RootCA CRL in its repository at maximum intervals of 6 months, even if there have been no modifications to the CRL (changes to the status of certificates) during the aforementioned period. If a sub is revoked, the CRL will be published in a period not exceeding three hours.
4.9.9. On-line Revocation/Status Checking Availability	CPS: 4.9.9	ACCV provides an OCSP server for online certificate status verification at: ocsp.accv.es:80 conform to RFC 6960 and RFC 5019. OCSP responses is signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. ACCV provides a service to obtain the status of a certificate beyond its validity period, using its serial number. The access URL to this service is: https://endor.accv.es/lando/
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.*	CPS: 4.9.10	OCSP server is free to access and there is no requisite for its use except those derived from use of the OCSP protocol according to the provisions of RFC 6960. OCSP supports calls to the service using GET method (in addition to POST method). For the status of Subscriber Certificates: • ACCV update information provided via OCSP at least 3 hours. • OCSP responses from this service have a maximum expiration time of 3 days. For the status of Subordinate CA Certificates: • ACCV update information provided via OCSP at least 6 months and within 12 hours after revoking a Subordinate CA Certificate. If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder respond with a "revoked" status, with reason certificateHold(6) and revocationTime January 1, 1970. ACCV monitor the responder for such requests as part of its security response procedures. ACCV also provides web services for consultation of the validity status of issued certificates.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CPS: 4.9.11	ACCV provides an OCSP server for online certificate status verification at: ocsp.accv.es:80 conform to RFC 6960 and RFC 5019. OCSP responses is signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. **ACCV provides a service to obtain the status of a certificate beyond its validity period, using its serial number. The access URL to this service is:** **https://endor.accv.es/lando/**
4.10.1. Operational Characteristics	CPS: 4.10	Revoked certificates remain in the CRL or OCSP until they reach their expiration date. Once this is reached, they are removed from the List of Revoked Certificates, due to their inability to be used because they are expired CRL systems and online certificate status consultation systems shall be available 24 hours a day and 7 days a week. The response time of the OCSP is not higher than 2s and the download time of CRL is ni higher than 5s.
4.10.2. Service Availability	CPS: 4.10	Revoked certificates remain in the CRL or OCSP until they reach their expiration date. Once this is reached, they are removed from the List of Revoked Certificates, due to their inability to be used because they are expired CRL systems and online certificate status consultation systems shall be available 24 hours a day and 7 days a week. The response time of the OCSP is not higher than 2s and the download time of CRL is ni higher than 5s.
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS		
5.2.2. Number of Individuals Required per Task	CPS: 5.2.2	Two persons are required for activation of the keys of cryptography hardware devices for key generation and storage. Modification of the configuration parameters of cryptography hardware requires authentication by two authorized persons with sufficient privileges.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS: 5.3.1	ACCV requires all personnel who carry out duties in its installations to have sufficient qualifications and experience in environments relating to the provision of certification services. All personnel must comply with the organization's security requirements and must possess: • Knowledge and training in digital certification environments. • Basic training in information systems security. • Specific training for their post. • Academic qualification or experience in the equivalent industry
5.3.3. Training Requirements and Procedures	CPS: 5.3.3	The personnel of ACCV are subject to a specific training plan for carrying out their role within the organization: This training plan includes the following aspects: 1. Training in the basic legal aspects relating to the provision of certification services. 2. Training in information systems security. 3. Services provided by ACCV. 4. Basic concepts of PKI. 5. Certification Practice Statement and the relevant Certification Policies. 6. Incident management
5.3.4. Retraining Frequency and Requirements	CPS: 5.3.4	Prior to technological changes in the environment, the introduction of new tools or the modification of operating procedures, the appropriate training will be carried out for the personnel affected. Training sessions will be carried out prior to changes in the Certification Practice Statement, Certification Policies or other relevant documents.
5.3.7. Independent Contractor Controls	CPS: 5.3.7	The external personnel that is involved in the issuance of certificates receives the necessary technical and legal training to carry out their tasks with due diligence (at least the detailed training on section 5.3.3). All personnel are subject to a secrecy obligation by virtue of signing the confidentiality agreement begin working for ACCV. In this agreement, they also undertake to carry out their duties in accordance with this Certification Practice Statement, ACCV Information Security Policy and the approved procedures of ACCV.
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	CPS: 5.4.1	ACCV records all events relating to: • Successful or failed attempts to change the security parameters of the operating system. • Start-up and stoppage of applications. • Successful or failed attempts to start or end a session. • Successful or failed attempts to create, modify or delete system accounts. • Successful or failed attempts to create, modify or delete authorized system users. • Successful or failed attempts to request, generate, sign, issue or revoke keys and certificates. • Successful or failed attempts to generate, sign or issue a CRL. • Successful or failed attempts to create, modify or delete certificate holder information. • Successful or failed attempts to access installations by authorized or unauthorized personnel. • Backup, file and restoration. • Changes to system configuration. • Software and hardware updates. • System maintenance. • Changes of personnel
5.4.3. Retention Period for Audit Logs	CPS: 5.4.3	ACCV shall retain all the audit records generated by the system for a minimum period from the date of their creation of two (2) years for those relating to daily audits, five (5) years for those relating to monthly audits and fifteen (15) years for those relating to annual audits.
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	CPS: 5.4.8	At least one yearly analysis is carried out of vulnerabilities and perimeter security. It is the responsibility of the analysis team coordinators to inform ACCV, via the Security Manager, of any problem preventing the performance of the audits, or the delivery of the resulting documentation. It is ACCV's responsibility to inform the audit teams of the suspension of analyses. The security analyses involve the initiation of the specific tasks to correct the vulnerabilities detected and the issue of a counter-report by ACCV.
5.5.2. Retention Period for Archive	CPS: 5.5.2	All the information and documentation relating to the life cycle of certificates issued by ACCV is retained for a period of 15 years.
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	CPS: 5.7.1	The Incident Response Plan and the Disaster Recovery Plan describe all the actions carried out and the material and human resources to solve a specific incident. These documents detail the actions to: Notify users, evaluate the incident, activate safeguards Recover affected services to provide adequate levels Restore regular operations and processes to normal levels In the event of unavailability of the installations of the Certification Authority for a period greater than six hours, ACCV's Incident Response Plan and a Disaster Recovery Plan shall be activated. The Disaster Recovery Plan guarantees that services identified as critical due to their availability requirement will be available in the Continuity DPC in less than 12 hours following activation of the Plan. ACCV annually test, review, and update these procedures.
6.1.1. Key Pair Generation	CPS: 6.1.1 CP: 6.1.1	CPS: Key pairs for all ACCV's internal components are generated on cryptography hardware modules with FIPS 140-1 Level 4 certification. In the case of components of CA type, there is audited documentation of the creation ceremony, which includes the steps followed, the personnel involved and the distribution of the activation mechanisms. All these steps are carried out and recorded in the presence of a qualified auditor and in a secured environment. Key pairs for end entities are generated in accordance with the stipulations in the applicable Certification Policy. CP: The key pair for the certificate that is issued under this Certification Policy is generated in software support by the certificate subscriber.
6.1.2. Private Key Delivery to Subscriber	CPS: 6.1.2 CP: 61.2	CPS: In cases when keys generation is not carried out via methods under the control of the actual end-entity, it shall be the corresponding Certification Policy that specifies the procedure to be used in order to deliver the private key to the end entities. CP: The private key is generated by the subscriber, therefore, it is not delivered to him.
6.1.5. Key Sizes	CPS: 6.1.5 CP: 6.1.5	CPS: The keys for ACCVRAIZ1 and the CAs in the same hierarchy are RSA keys with a length of 4096 bits The key sizes for each certificate type issued by ACCV are defined in the related Certification Policy. In every case, key sizes will never be less than 2048 bits. CP: The keys of ACCVRAIZ1 and ACCVCA-120 root are RSA keys of 4096 bits length. The key size for the certificates issued under this Certification Policy is at least 2048 bits of length.
6.1.6. Public Key Parameters Generation and Quality Checking	CPS: 6.1.6 CP: 6.1.6	CPS: The keys for ACCVRAIZ1 and the CAs in the same hierarchy are created with RSA algorithm. The key generation parameters for each type of certificate issued by ACCV are defined by the Certification Policy applicable to the relevant certificate Parameters defined at ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" document, are used (6 - Signature schemes). The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2). The procedures and methods of verification of the quality of the key generation parameters for each type of certificate issued by ACCV are defined by the Certification Policy applicable to the relevant certificate. CP: The keys of ACCVRAIZ1 and ACCVCA-120 root are created with the RSA algorithm. Parameters defined at ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" document, are used (6 - Signature schemes). The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2).
6.1.7. Key Usage Purposes	CPS: 6.1.7 CP: 6.1.7	CPS: The purposes of key use for each type of certificate issued by ACCV are defined by the Certification Policy applicable to the relevant certificate. All subscribers certificates issued by ACCV contain the extensions KEY USAGE and EXTENDED KEY USAGE defined by the standard X.509 v3 for the definition and limitation of such purposes. Private Keys corresponding to Root Certificates is not used to sign Certificates except in the following cases: Self-signed Certificates to represent the Root CA itself Certificates for SubCAs, and, if the case arises, Cross Certificates. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates) Certificates for OCSP Response verification and Time Stamping service. CP: The keys that are defined in the current policy will be used for the uses described at the section 1.3 User community and scope of application of this document. The detailed definition of the certificate profile and the usage of keys is located in the section 7 of this document "Certificate profiles and certificate revocation list".
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS: 6.2.1	It is compulsory for modules used for the creation of keys used by every CAs integrated in the trust hierarchies comply with an appropriated security certification for its functionality and the security that it requires. A hardware security module (HSM) is a security device that generates and protects cryptographic keys. Such products must therefore meet at least with FIPS 140-2 Level 3 criteria, or Common Criteria EAL 4+ for the corresponding protection profile. ACCV holds procedures and policies to check that an HSM has not been manipulated during transport and storage Cryptographic devices with qualified electronic signature certificates, suitable as qualified signature creation devices (DSCF), meet the requirements of security level CC EAL4+, although certifications complying with a minimum of ITSEC E3 or FIPS 140-2 Level 2 security criteria or equivalent are also acceptable. The European reference standard for subscriber devices used is Commission Implementing Decision (EU) 2016/650 dated 25 April, 2016.
6.2.5. Private Key Archival	CPS: 6.2.5	Backup copies of the expired private keys of ACCV entities are held in safekeeping in encrypted form in secure fireproof lockbox, accessible only by authorized personnel with at least dual access. All private keys are under the exclusive control of the ACCV.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS: 6.2.6	Private keys are created on the cryptography module at the time of the creation of each ACCV entity that use these modules, fulfilling the requirements defined in section 6.2.1.
6.2.7. Private Key Storage on Cryptographic Module	CPS: 6.2.7	Private keys are created on the cryptography module at the time of the creation of each ACCV entity that use these modules, fulfilling the requirements defined in section 6.2.1.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	CP: 6.3.2	The certificates issued over the scope of the current policy have as maximum 27 months of validity. The key that is used for the certificates issuance is created for each issuance, and therefore is valid for 27 months as maximum. That is the maximum validity date that is allowed in the application for the certificates issued under this policy. ACCVCA-120 certificate is valid since 13th October 2011 until 1st January 2027.

6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. *Indicate how your CA meets the requirements of this section.*	CPS: 6.5	The data relating to this section is considered to be confidential information and is only provided to persons who can provide evidence of their requirement to know it. In any case, the Security Policy (accessible to the auditors) guarantees the use of at least two-factor authentication in the applications that manage the life cycle of the certificates (smartcard + PIN).
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. *Indicate how your CA meets the requirements of this section.*	CPS: 7.1	ACCV generates serial numbers with 64 bits of entropy. The core application forces this behavior. Implements a singleton serial number generator using SecureRandom. This generator generates random 8 octet (64 bits) serial numbers.
7.1.1. Version Number(s)	CPS: 7.1.1 CP: 7.1.1	CPS: ACCV supports and uses X.509 version 3 (X.509 v3) certificates. X.509 is a standard developed by the International Telecommunication Union (international United Nations organization that coordinates telecommunications networks services between Governments and companies) for Public Key Infrastructures and digital certificates CP: ACCV supports and uses X.509 version 3 (X.509 v3) certificates. This certification policy specifies the usage of a certificate with three different uses; digital signature, subscriber authentication and data encryption.
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CPS: 7.1.2	The extensions used in a generic form on the certificates are as follows: Key Usage. Marked as critical in all cases. Root CA and SubCA: KeyCertSign CRLSign Subscriber: Established in the associated certification policy Basic Constraint. RootCA and SubCA Present and marked as critical. CA field TRUE Subscriber: Not present Certificate Policies. Present in all cases and marked as not critical. Subject Alternative Name. Present in all cases and marked as not critical. CRL Distribution Point. Present in all cases and marked as not critical. extkeyUsage RootCA and SubCA: Not present Subscriber: Established in the associated certification policy. authorityInformatioAccess: Present in all cases and marked as not critical. nameConstraints: Not present. ACCV Certification Policies can establish overall variations of the extensions used for each type of certificate. In all cases the specifications and limits established in RFC-5280 will be met.
7.1.2.1 Root CA Certificate	CPS: 7.1.2	The extensions used in a generic form on the certificates are as follows: Key Usage. Marked as critical in all cases. Root CA and SubCA: KeyCertSign CRLSign Subscriber: Established in the associated certification policy Basic Constraint. RootCA and SubCA Present and marked as critical. CA field TRUE Subscriber: Not present Certificate Policies. Present in all cases and marked as not critical. Subject Alternative Name. Present in all cases and marked as not critical. CRL Distribution Point. Present in all cases and marked as not critical. extkeyUsage RootCA and SubCA: Not present Subscriber: Established in the associated certification policy. authorityInformatioAccess: Present in all cases and marked as not critical. nameConstraints: Not present. ACCV Certification Policies can establish overall variations of the extensions used for each type of certificate. In all cases the specifications and limits established in RFC-5280 will be met.
7.1.2.2 Subordinate CA Certificate	CPS: 7.1.2	The extensions used in a generic form on the certificates are as follows: Key Usage. Marked as critical in all cases. Root CA and SubCA: KeyCertSign CRLSign Subscriber: Established in the associated certification policy Basic Constraint. RootCA and SubCA Present and marked as critical. CA field TRUE Subscriber: Not present Certificate Policies. Present in all cases and marked as not critical. Subject Alternative Name. Present in all cases and marked as not critical. CRL Distribution Point. Present in all cases and marked as not critical. extkeyUsage RootCA and SubCA: Not present Subscriber: Established in the associated certification policy. authorityInformatioAccess: Present in all cases and marked as not critical. nameConstraints: Not present. ACCV Certification Policies can establish overall variations of the extensions used for each type of certificate. In all cases the specifications and limits established in RFC-5280 will be met.
7.1.2.3 Subscriber Certificate	CPS: 7.1.2 CP: 7.1.2	Text Retention period of material information QcPDS https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf PKI Disclosure Statement location In all cases the specifications and limits established in RFC-5280 will be met.
7.1.2.4 All Certificates	CPS: 7.1.2	The extensions used in a generic form on the certificates are as follows: Key Usage. Marked as critical in all cases. Root CA and SubCA: KeyCertSign CRLSign Subscriber: Established in the associated certification policy Basic Constraint. RootCA and SubCA Present and marked as critical. CA field TRUE Subscriber: Not present Certificate Policies. Present in all cases and marked as not critical. Subject Alternative Name. Present in all cases and marked as not critical. CRL Distribution Point. Present in all cases and marked as not critical. extkeyUsage RootCA and SubCA: Not present Subscriber: Established in the associated certification policy. authorityInformatioAccess: Present in all cases and marked as not critical. nameConstraints: Not present. ACCV Certification Policies can establish overall variations of the extensions used for each type of certificate. **In all cases the specifications and limits established in RFC-5280 will be met.**
7.1.2.5 Application of RFC 5280	CPS: 7.1.2	The extensions used in a generic form on the certificates are as follows: Key Usage. Marked as critical in all cases. Root CA and SubCA: KeyCertSign CRLSign Subscriber: Established in the associated certification policy Basic Constraint. RootCA and SubCA Present and marked as critical. CA field TRUE Subscriber: Not present Certificate Policies. Present in all cases and marked as not critical. Subject Alternative Name. Present in all cases and marked as not critical. CRL Distribution Point. Present in all cases and marked as not critical. extkeyUsage RootCA and SubCA: Not present Subscriber: Established in the associated certification policy. authorityInformatioAccess: Present in all cases and marked as not critical. nameConstraints: Not present. ACCV Certification Policies can establish overall variations of the extensions used for each type of certificate. **In all cases the specifications and limits established in RFC-5280 will be met.**
7.1.3. Algorithm Object Identifiers	CPS: 7.1.3 CP: 7.1.3	Object Identifiers (OID) of the Cryptography algorithms: • SHA1withRSAEncryption (1.2.840.113549.1.1.5) • SHA256withRSAEncryption (1.2.840.113549.1.1.11)
7.1.4. Name Forms	CPS: 7.1.4 CP: 7.1.4	
7.1.4.1 Issuer Information	CPS: 7.1.4 CP: 7.1.4	CPS: Certificates issued by ACCV contain the X.500 distinguished name of the issuer and the certificate subscriber in the issuer name and subject name fields respectively. CP: The certificates that are issued by ACCV contain the distinguished name X.500 of the certificate issuer and the certificate subscriber in the issuer name and subject name fields, respectively. For certificates issued under this policy: Issuer name: cn=ACCVCA-120, ou=PKIACCV o=ACCV, c=ES
7.1.4.2 Subject Information - Subscriber Certificates	CP: 7.1.4	The certificates that are issued by ACCV contain the distinguished name X.500 of the certificate issuer and the certificate subscriber in the issuer name and subject name fields, respectively. For certificates issued under this policy: Issuer name: cn=ACCVCA-120, ou=PKIACCV o=ACCV, c=ES All the fields of the certificate of the Subject, excepting the ones that are referred to the DNS name or email address, are filled necessarily in capital letters, without accents. SubjectAlternativeName contain at least one entry. Each entry in the SubjectAlternativeName is a dNSName containing the Fully-Qualified Domain Name of a server. Subject: commonName (required). It must match one of the DNSName fields of the subjectAlternativeName serialNumber (required). Administration NIF, as defined in Royal Decree 1065/2007, of July 27. OrganizationIdentifier (required) Entity NIF, as defined in the European standard ETSI EN 319 412-1 OrganizationalUnit (required) fixed string "SERVIDORES" jurisdictionCountry (required) Country code ISO 3166-1 BusinessCategory (required) One of the following fixed chains "PRIVATE ORGANIZATION" "GOVERNMENT ENTITY" "BUSINESS ENTITY" "NON-COMMERCIAL ENTITY" , depending on the organization type Organization (required) Designation ("official" name) of the Administration, organism or entity that is the certificate subscriber and the domain owner. locality (required) Locality, City or Town state (required) State o province country (required) Country code ISO 3166-1
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CPS: 7.1.4	Certificates issued by ACCV contain the X.500 distinguished name of the issuer and the certificate subscriber in the issuer name and subject name fields respectively. In the case of RootCA or SubCAs Issuer name: cn=ACCVRAIZ1, ou=PKIACCV o=ACCV, c=ES Subject: commonName (required). It must match the name of ACCV entity, such that the certificate's Name is unique across all certificates issued by the issuing certificate. OrganizationalUnit (required) fixed string "PKIACCV" Organization (required) fixed string "ACCV" country (required) Country code ISO 3166-1 ACCV Certification Policies establish the overall variations of the name forms used for each type of certificate.
7.1.5. Name Constraints *Indicate your CA's understanding of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section.*	CPS: 7.1.5 Our CA understands Mozilla's requirements to disclose SubCAs that are not technically constrained.	The names contained on the certificates are restricted to X.500 distinguished names, which are unique and allow for no ambiguity. There are not name constraints defined in SubCA certificates.
7.1.6. Certificate Policy Object Identifier	CPS: 7.1.6 CP: 7.1.6	CPS: To be defined by each Certification Policy. ACCV has established a policy for assignment of OIDs within its private numbering range. The OIDs of all ACCV's Certification Policies begin with the prefix 1.3.6.1.4.1.8149.3 In the case of RootCA and SubCA have as policy any policy. CP: The object identifier defined by ACCV for identifying the current policy is the following: 1.3.6.1.4.1.8149.3.3.4.0 In this case an OID is added for identifying the type of entity that is representing with the regulation ETSI TS 119 411-2 0.4.0.194112.1.4Certification Policy for EU qualified certificates issued to websites
7.1.6.1 Reserved Certificate Policy Identifiers	N/A	
7.1.6.2 Root CA Certificates	CPS: 7.1.6	To be defined by each Certification Policy. ACCV has established a policy for assignment of OIDs within its private numbering range. The OIDs of all ACCV's Certification Policies begin with the prefix 1.3.6.1.4.1.8149.3 In the case of RootCA and SubCA have as policy any policy.
7.1.6.3 Subordinate CA Certificates	CPS: 7.1.6	To be defined by each Certification Policy. ACCV has established a policy for assignment of OIDs within its private numbering range. The OIDs of all ACCV's Certification Policies begin with the prefix 1.3.6.1.4.1.8149.3 In the case of RootCA and SubCA have as policy any policy.
7.1.6.4 Subscriber Certificates	CP: 7.1.6	The object identifier defined by ACCV for identifying the current policy is the following: 1.3.6.1.4.1.8149.3.3.4.0 In this case an OID is added for identifying the type of entity that is representing with the regulation ETSI TS 119 411-2 0.4.0.194112.1.4Certification Policy for EU qualified certificates issued to websites
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CPS: 8	ACCV carries out the necessary controls to ensure that: issue Certificates and operate the services in accordance with all law applicable to its business meets the technical requirements set complies with the audit requirements set forth in this section

8.1. Frequency or circumstances of assessment The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	CPS: 8.1 We understand the requirements established in this section.	A fully audit shall be carried out on ACCV at least once a year to guarantee the compliance of its running and operating procedures with the provisions included in this CPS. Certificates capable of issuing new certificates and all their operations fall within the scope of the audit, these operations are divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration. Other technical and security audits shall be carried out in accordance with the stipulations of ACCV's Audit Policy, which include an audit on compliance with personal data protection legislation
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	CPS: 8.2	The auditor shall be selected at the time that each audit is performed. Any company or person contracted to perform a security audit on ACCV must fulfill the following requirements: - Adequate and proven training and experience in PKI, security and audit processes for information systems. - Independence at an organizational level from ACCV authority, in case of external audits. - Meet all the requirements and have all the necessary accreditations that have been established at the legal and technical level for carrying out the audit.
8.4. Topics covered by assessment	CPS: 8.4	The audit shall determine the compliance of ACCV services with this CPS and the applicable CPs. It shall also determine the risks of non-fulfillment of compliance with the operating procedures defined by these documents. The aspects covered by an audit shall include, but shall not be limited to: - Security policy - Physical security - Technological evaluation - Administration of the CA's services - Selection of personnel - CPS and CPs in force - Contracts - Privacy policy ACCV carries out at least one annual audit under the scheme WebTrust for Certification Authorities v2.0, in addition to the necessary audits established by the legislation in force and by the technical norms of application for the fulfillment of its functions.
8.6. Communication of results	CPS: 8.6	The auditor shall notify the results of the audit to ACCV Security Manager, and the managers of the various areas in which non-conformance is detected. ACCV, where possible, will keep public and accessible audit reports, ensuring that no more than three months will pass from the end of the previous audit period.
Also indicate your understanding and compliance with Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). ... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). "	ACCV understands and complies with Mozilla's Root Store Policy	
8.7. Self-Audits	CPS: 8.7	ACCV constantly monitors compliance with procedures and policies, establishing periodic controls of relevant indicators and conducting self-audits on at least a quarterly basis against a randomly selected sample of three percent of the Certificates issued during the period commencing immediately after the previous self-audit sample was taken.
9.6.1. CA Representations and Warranties	CPS: 9.6.1	ACCV is obliged to: - Carry out its operations in accordance with this CPS. - Protect its private keys. - Issue certificates in accordance with the Certification Policies that are applicable to them. - After receiving a valid certificate request, to issue a certificate compliant with the X.509 standard and with the request requirements. - Issue certificates that conform to the information known at the time of their issue, and that are free of data entry errors. - Guarantee confidentiality in the generation process of signature creation data and its delivery via a secure procedure to the signatory. - Use reliable systems and products that are protected against any alteration and which guarantee the technical and cryptography security of the certification processes which they support. - Use reliable systems to store recognized certificates which permit verification of a certificate's authenticity and prevent unauthorized persons from altering data, restrict its accessibility in cases or to persons indicated by the signatory and permit the detection of any change that affects these security conditions. - Publish issued certificates in ACCV's LDAP directory (ldap.accv.es) without alteration. - Guarantee that the date and the time at which a certificate was issued or its validity was terminated or suspended can be accurately determined. - Employ personnel with the qualifications, knowledge and experience required for the provision of the certification services offered and the appropriate security and management procedures in the field of electronic signatures. - Revoke certificates according to the terms of the Revocation and Suspension of Certificates section of this document and publish the revoked certificates in the CRL of ACCV's LDAP directory (ldap.accv.es) with the frequency stipulated in the point Frequency of issue of CRLs of this document. - Publish this CPS and the applicable CP on the website www.accv.es/cps, guaranteeing access to the current versions as well as to previous versions. - Promptly notify certificate subscribers by e-mail in the event that the CA proceeds with the revocation or suspension of the certificate, and also inform them of the reason that led to this action. - Collaborate with the audits led by ACCV to validate the renewal of its own keys. - Operate in accordance with the applicable legislation, specifically with: 1. Decree 220/2014 of 12 December of the Valencian Government, which governs the use of the advanced electronic signature in the Autonomous Government of Valencia. 2. Law 59/2003 of 19 December on Electronic Signatures. 3. European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market. 4. Law 39/2015, October 1st, about the Common Administrative Procedure of Public Administrations 5. Decree 15/2014 of 24 January of the Consell, which approves the Regulation of the Organization and Functioning of Institut Valencià de Finances (IVF). - Where keys exist, protect them by holding them in safekeeping. - Guarantee the availability of the CRLs in accordance with the provisions of section 4.9.9 Frequency of issue of CRLs, of this CPS. - In the event of ceasing its activity, it must communicate this with a minimum notice of two months from effective cessation, to the holders of the certificates issued by ACCV, and to the Ministry of Industry, Tourism and Trade, specifying what will happen to the certificates. - Comply with the specifications contained in the regulations on Personal Data Protection. - Keep records of all the information and documentation relating to a recognized certificate and the certification practice statements in force at any time for fifteen years from the time of their issue, so that the signatures carried out with the certificates can be verified.
9.6.3. Subscriber Representations and Warranties	CPS: 9.6.3	The subscribers of the certificates issued under this policy are bound by the following obligations: - To limit and tailor the use of the certificate to legal purposes in accordance with the uses permitted by the relevant Certification Policy and this CPS. - To apply the necessary care and methods to guarantee the safekeeping of their private key. - Immediately to request the revocation of a certificate in the event of becoming aware of or suspecting the compromise of the private key corresponding to the public key contained in the certificate. The ways in which this request can be carried out are specified in this document in the section 4.9.3 Revocation request procedure. - Not to use a digital certificate that is no longer effective, due to having been suspended, revoked or due to the certificate's period of validity having expired. - To provide the Registration Authorities with information that they consider accurate and complete in relation to the data that these Authorities request from them to carry out the Registration process, as well as inform ACCV managers of any modification of this information. - To pay the fees resulting from the certification services that they request from the corresponding Registration Authority in relation to the services that are requested.
9.8. Limitations of liability	CPS: 9.8	9.8.1. Guarantees and limitations of guarantees ACCV shall be responsible for damages that it causes to any person in carrying out its activity, when it fails to fulfill the obligations imposed by Law 59/2003 of 19 December on Electronic Signatures, Decree 220/2014 of 12 December of the Valencian Government, and European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market, or it acts negligently. ACCV shall be responsible for damages that are caused to the signatory or to third parties in good faith due to the failure of or delay in the inclusion in the certificate validation service of the expiry or suspension of validity of the certificate issued by ACCV, once it becomes aware of this. ACCV shall accept all liability vis-à-vis third parties for the actions of persons who carry out the necessary functions for provision of the certification service. ACCV is the Certification Authority of the Autonomous Government of Valencia. The responsibility of the Administration is founded on objective bases and covers any injury that individuals might suffer, provided that it is the consequence of normal or abnormal operations of the public services. ACCV only shall be responsible for damage caused by improper use of the recognized certificate, when it has not recorded on it, in a form clearly recognizable by third parties, the limit with regard to its possible use or the amount of the value of the valid transactions that can be carried out using it. It shall not be responsible if the signatory exceeds the limits recorded on the certificate in relation to its possible uses and the individualized amount of the transactions that can be carried out with it or does not use it in accordance with the stipulated conditions communicated to the signatory by ACCV. ACCV shall also not be responsible if the addressee of the electronically signed documents does not check and take into account the restrictions recorded on the certificate in relation to its possible uses and the individualized amount of the transactions that can be carried out with it. 9.8.2. Limitations of liability ACCV Registration Entities shall not accept any liability in the event of loss or damage: - To the services that they provide, in the event of war, natural disasters or any other case of force majeure. - Caused by the use of certificates which exceeds the limits stipulated by the certificates, the relevant Certification Policy and this CPS. - Caused by the improper or fraudulent use of the certificates or CRLs issued by ACCV. - Caused to the signatory or third parties in good faith if the addressee of the electronically signed documents does not check or take into account the restrictions recorded on the certificate in relation to its possible uses, or if the addressee does not take into account the revocation or loss of validity of the certificate published on the CRL, or if the addressee does not verify the electronic signature. 9.8.3. Loss limitations With the exception of the stipulations set out in this CPS, ACCV shall accept no other obligation nor offer any other guarantee, and in addition shall accept no other liability vis-à-vis subscribers or relying parties.
9.9.1. Indemnification by CAs	CPS: 9.9.1	ACCV is a government entity, so it is not applicable.
9.16.3. Severability	CPS: 9.16.3	In case of conflict of any part of this document with current legislation of any jurisdiction in which a CA operates or issues certificates, after the corresponding legal review, ACCV can modify the conflicting points the minimum extent necessary to fulfill the aforementioned legislation. In such event, (prior to issuing a certificate under the modified requirements) ACCV will include in subsections of this Section information about the Law requiring modification and the specific change implemented by ACCV. ACCV will also (prior to issuing a certificate under the modified requirement) inform interested parties such as the CAB Forum of the relevant information newly added.