CA Hierarchy

All SubCAs are internally operated.

The root is always the same and only signed SubCAs and High-level certificates (OCSP certificate and TSA certificate).

CAGVA- Issues end entity certificates, above all personal certificates, code signing certificates and SSL certificates. ACCV check the data from end entities exhaustively (vital statistics and data domain). At present this CA no longer issues certificates (CRL signing only)

ACCV-CA1 Issues end entity certificates. Mainly company certificates

ACCV-CA2 This AC replaces CAGVA. Issues end entity certificates, above all personal certificates, code signing certificates and SSL certificates. ACCV check the data from end entities exhaustively (vital statistics and data domain)

ACCV-CA3 This CA issues logon certificates and DC certificates for internal domains

OCSP Responder URL

The OCSP certificate is signed by Root CA. It´s the same root that signed the subca certificates. That is, OCSP responses are signed by a certificate signed by the root CA, which also signed the subordinate CA

The root is always the same.

Is it a problem? Mozilla does not support this configuration?

Externally Operated sub-CAs

ACCV does not have externally operated CA (and does not plan to have them in the future)

Cross-Signing

ACCV does not have cross-signing certificates with other CA

SSL Validation Type DV, OV, and/or EV

ACCV verify the identity/organization of the subscriber in all certificates issued. The only way to request a SSL certificate or a code signing certificate is to have a personal certificate from the ACCV.

Organization Identity Verification

“SSL CP section 3.1.8, Authentication of the identity of an organization

The right to request certificates defined in this Certification Policy is limited to natural persons. we will not accept applications for certification made on behalf of people legal persons, entities or organizations. Therefore not considered necessary to identify any organization.

For applicants belonging to the scope of the Generalitat Valenciana your order will be validated with information from the official directory.
In case of not belonging to the Generalitat Valenciana, the applicant must attach the publication of the official appointment or document the job occupation or certificate issued by human resources department in his organization, which clearly indicates his position and responsibility."

SSL CP section 3.1.9: Yes. You must have a qualified personal certificate before applying for an SSL certificate or similar.

Domain Name Ownership / Control

4.1. Certification Request
The applicant of a certificate issued under this Certification Policy must fulfill an online certificate request using the non-personal certificate management application (NPSC) available at https://npsc.accv.es:8450/npsc where the PKCS#10 file that was previously generated by the applicant will be embed.
Once the application form is fulfilled, it will be sent by signing the request with one of the qualified certificates admitted by the Autoritat de Certificació de la Comunitat Valenciana.
The Registration Authority has the responsibility to determine the suitability of the certificate type to the applicant characteristics depending on the provisions of the applicable Certification Policy and thus manage or deny the applicant certification request.
Should the Registration Authority Operator refuse the request, an email informing of reasons for rejection will be sent to the address stated in the application.

4.2. Certificate Issuing
The certificate issuing procedure will start once the Registration Authority associated to this Certification Policy has checked all necessary requirements for validating the certification request. This Certification Policy will be the mechanism for determining the nature and how to perform this checking.
Upon issuance of the certificate, the Registration Authority shall notify the subscriber by sending a signed e-mail to the address included in the request. The user must sing in to the non-personal certificate management application (NPSC) available at https://npsc.accv.es:8450/npsc to pick up the certificate by previously signing the Certificate Agreement in this application with a personal qualified certificate.
The Certificate Agreement is a document that must be digitally signed by the applicant in order to bind him/her to the request action, the knowledge of certificate use rules and the accuracy of provided data.

By the time a request arrives, ACCV verifies the identity of the applicant and the information provided (the company in which the user works and the domain requested by the user). All requests are digitally signed with qualified personal certificates. These qualified certificates require that the user is physically present in a registration point and proves his identity.

Email Address Ownership / Control

3.2 Initial Identity Validation

3.2.1. Test methods of the possession of the private key

As specified in the ACCV Certification Practices Statement (CPS).

3.2.2 Identity authentication of an organization

The application for certificates associated to this Certificate Policy is limited to public entities or administrations which have established a certification agreement, contract or some other formula that supports the ACCV service provision.
The public entity or administration identification process will be held in the organization enrollment to be signed by an authorized representative of the entity or administration.

3.2.3. Identity authentication of an individual.

The certificate applicant identity authentication will be made in person while applying or during the certificate delivery. Thus, Registration is delegated to the certificate issuing entity which signed an agreement, contract or some other formula that supports the ACCV service provision.
Presence of the civil servant to whom a certificate is issued will not be required when his/her identity and civil servant status are already recorded in the Personnel Registry of the Public or Corporate Entity or Public Administration which the civil servant belongs to and where his/her application is directed to.

The applicant public entity or administration has the entire responsibility of determining the civil servant status. The public entity or administration will check the public servant status in its data base if it is updated or by requesting a document where the subscriber's status is stated in case that the applicant public entity or administration has not this record.
These certificates include the subscriber's email address as a necessary element to support digital signature and email encryption operations. However, the Autoritat de Certificació de la Comunitat Valenciana does not guarantee that this electronic address is linked to the certificate subscriber, thus the confidence that this email is linked to the certificate subscriber relates to the relying party only. The Autoritat de Certificació de la Comunitat Valenciana just guarantees that the email stated in the certificate was provided by the Administration or Public Entity which the subscriber belonged to at the time that the application was made and/or that this email is linked to the subscriber in the Valencia Government or other Public Administration personnel data base that the applicant belongs to.

4.1. Certificate Request

This certificate request is responsibility of the Public Entity or Administration which shall verify the certificate owner's civil servant status by checking their organization personnel registry.
The process starts with the Administration, organization or entity enrollment using an entity sign up form as shown in the Annex III of this Certificate Policy.
The persons who will be authorized for the civil servant certificate management of the related entity staff members must be stated in this form.

In order to make a certificates request, the form shown in Annex IV shall be used, signed by one of the certificate management authorized persons and sent to the Autoritat de Certificació de la Comunitat Valenciana.

4.2. Certificate application processing
After receiving the certificates request from the corresponding authorized persons and once, as appropriate, the economic proposal –if any- is accepted, the certificates will be issued and the associated documents prepared. Upon finishing, all will be sent to the applicant Administration or public Entity though the authorized persons.
These certificate management authorized persons will be responsible of the certificate delivery to the subscribers and of sending the certificate agreements back to the Autoritat de Certificació de la Comunitat Valenciana.

4.3. Certificate Issuing
ACCV is not responsible of the monitoring, investigation or confirmation of the certificate information accuracy after issuing. Should any information about the inaccuracy or non applicability of data contained in the certificate be received, the certificate can be revoked.
The certificate issuing procedure will start once the ACCV checks all necessary requirements for validating the certification request. This Certification Policy will be the mechanism for determining the nature and how to perform this checking.
When the ACCV CA issues a certificate associated to a valid certification request, it will send a copy to the Registry Authority that submitted the application and to the ACCV repository.
It is up to the Registry Authority to notify the subscriber of the issuance of the certificate and provide a copy, or failing that, inform them of how to get it.

4.4 Certificate Acceptance
Subscribers accept certificates by signing the certificate agreement associated to each Certificate Policy. The acceptance of agreement implies the Certificate Policy knowledge and acceptance by the subscriber.
The certificate agreement has to be signed by both the subscriber and the person attached to the User Registry Point. Thus, the individual associated to a certificate is linked to the request, the knowledge of use rules and to the accuracy of provided data. The Certificate Agreement form is included in Annex I of this Certificate Policy.

Civil servants certificates are issued from the official lists supplied by the public administration concerned.
These official lists are drawn from selective processes with maximum guarantees (determine who is a civil servant) and involve a process in person at the registration point of administration.

Public administration provides its employees with email accounts for his work as a civil servant. These email accounts are corporate and internally generated.The ACCV accepts these mail accounts because they are imposed by the administration and not by the user.

Identity of Code Signing Subscriber

3.1.8. Identity Authentication of an Organization
The right to apply for certificates defined in this Certificate Policy is limited to individuals. No certificate applications made by legal persons, entities or organizations will be admitted. Thus, no organization identification is required.

When the applicant belongs to the Valencia Government staff, his/her application will be validated with the information contained in the People and Services' Guide.
If they are not Valencia Government staff members, the applicant must submit the appointment publication (Government Gazette) or the civil servants' inauguration certificate or a certificate from his/her organization personnel department specifying occupation and responsibilities.

3.1.9. Identity Authentication of an Individual
The identity authentication of a certificate applicant shall be made by his/her personal digital certificate that is used to sign the certificate application.

As stated in the policy the code-signing certificates can only be ordered with personal qualified certificates. The ACCV requires the applicant to provide documentation or references to ensure their identity in the organization.

Long-lived DV certificates
Are SSL certs DV or OV?
For all requests are verified domain ownership by the organization that owns the applicant (in the company that registers internet domain) and verifies that the applicant belongs to the organization and has the capacity to request the certificate.

OCSP Responses signed by a certificate under a different root
Get Error code: sec_error_ocsp_unauthorized_response when OCSP is enforced.

The answer is the same as in OCSP responder URL :

The OCSP certificate is signed by Root CA. It´s the same root that signed the subca certificates. That is, OCSP responses are signed by a certificate signed by the root CA, which also signed the subordinate CA

The root is always the same.

Is it a problem? Mozilla does not support this configuration?