- In response to doubts of document:

A) What is the relation of this root to the “Root CA Generalitat Valenciana” root that was included via bug #274100? E.g. Will this root eventually replace the other root?

R) Yes, you're right. Between 10 December 2012 and 10 February 2013 will change the emission mechanisms to the new hierarchy. Everything else is equal, procedures and controls are maintained.

A)Code Signing CP: http://www.accv.es/fileadmin/Archivos/Politicas_pdf/PKIGVA-CP-04V2.0-c.pdf (what’s the new version of this?)

R) Yes. Sorry. This policy was drafted after. The link is http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-04V3.0-c.pdf

A)Please update your WebTrust seal at http://www.accv.es/webtrust

R)Ok. The right seal is https://cert.webtrust.org/SealFile?seal=1352&file=pdf

A)What is your status in regards to complying with the CAB Forum Baseline Requirements? (https://www.cabforum.org/Baseline_Requirements_V1.pdf) As per the CAB Forum Baseline Requirement # 8.3, where is the “Commitment to Comply” statement that should be in your CP or CPS?

R) We are working to adopt policies to the requirements of CAB Forum. In the following versions of policies add the text compliance. In the code signing policy (last) appears in 1.1
“*ACCV is set to the current version of the document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published in https://www.cabforum.org/. In the event of any inconsistency between this Certification Policy and those requirements, those requirements prevail over this document.*”

A)Please translate the sections of the SSL CP that describe the steps taken to authenticate the organization, certificate subscriber, and the authority of the subscriber to act on behalf of the organization.

R) 3.2.3
“The authentication of the identity of the requesting a certificate shall be made by the use of recognized certificate of citizen or public employee of the ACCV to sign the application server certificate with SSL support.
The applicant must also submit the necessary documentation to determine the ability of represent the Public or private entity that owns the server that is intended the certificate. This submission will be carried out using telematic means that the ACCV available to users.
The ACCV check both data using for it the information available to personnel records and domain, requiring the applicant or the Administration represented clarifications or additional documents may be required. in case private entities require authorization information from the applicant.”

A) Please translate the sections of the Code Signing CP that describe the steps taken to authenticate the organization, certificate subscriber, and the authority of the subscriber to act on behalf of the organization.

R) 3.2.3
“The authentication of the identity of the applicant for a certificate shall be made by the use of recognized certificate of citizen or public employee of the ACCV to sign the certificate request for

code signing.
The applicant must also submit the necessary documentation to determine the capacity of representing the public administration or private entity on behalf of which, ultimately, is going to issue the certificate. This Presentation is telematically using the means and Technology Agency of Electronic Certification available to users.
Technology Agency of Electronic Certification and verify both data, the ability to re-presentation of the applicant and the veracity of the data of the company or organization, using information available from personnel records, requiring the applicant or the Administration represented the clarifications or additional documents may be required. In case of private entities, will require information on the authorization of the applicant and the information of the company creating searchable in the appropriate register."

A) Please provide the section numbers of the CPS or CP that cover network and system security.

R) In the CPS http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V3.0-EN.pdf (English)

5. Physical security, management and operations controls

A)Document Handling of IDNs in CP/CPS

R)We are not working with IDN certified in SUBJECT or SAN.

A)Revocation of Compromised Certificates

R) In CP 3.4

The ACCV or any of the entities that comprise own motion may request revocation of a certificate if they have knowledge or suspicion of commitment of the private key associated with the certificate issued under this Certificate Policy, or anything which will recommend to take such action.

A) DNS names go in SAN

R) The ACCV issues certificates with the DNS Name inSAN, and, for compatibility, also gets in the CN.

A)Domain owned by a Natural Person

R)The ACCV always issues the certificates to an organization, represented by a person.

A) Long lived DV certificates

R) The ACCV certificates for end entity has a maximum duration of three years (36 months).

A) Wildcard DV SSL certificates

R) Currently, the ACCV not issue wildcard certificates for DV.
For OV only take into account for prestigious organizations (so far there has not been the case).

A) Email Address Prefixes for DV Certs

R) For DV only be taken into account emails that may be related to the domain explicitly proven or emails that appear in the WHOIS record. These are the emails that are used in communications of the request. The ACCV always tries OV checks (as it appears in the policy).

A) Distributing generated private keys in PKCS#12 files

R) No. Not distribute private keys in PKCS12 file for SSL certificates or private keys are distributed through insecure ways.

A) Certificates referencing hostnames or private IP addresses

R) The ACCV not support IP or domain names without resolution in SAN. In SAN only accepted domain names registered in whois and checked the resolution in the verification process.

Formerly it could accept unresolvable domains in CN subject, but is deprecated and never in SAN.

A) Issuing SSL Certificates for Internal Domains

R) The ACCV has revised its bdd of certificates issued and has no certificate for the domain .int. In the application process verifies that the requested name fulfills a basic syntax and also always done a manual verification process conducted by internal ACCV staff. Never SSL certificate is issued without a review by a human operator.