1.Name
- •ACCV

2.Website URL http://www.accv.es

3.Organizational type
- •ACCV is a CA operated by a government agency of Spain. Initially had a regional character but now operates nationally.

4.Primary market / customer base
- •The ACCV issues certificates for all citizens for their personal use and for its relations with the public administration and business.
- •The ACCV CA focus its activities mainly in Spain but is collaborating in international recognition of certificates.

5.Impact to Mozilla Users
- •This CA is a CA additional to that included in Mozilla, which improves algorithms and provides certificates issued increased robustness and security. The ACCV continues to issue certificates to citizens and the administration as the primary mechanism to ensure communication between the two.
- •The original CA is included in Mozilla and IE. This additional CA is in the process of inclusion in IE.
- •The set of users who will find our certificates is formed mainly by citizens having to contact or exchange information with the public administration (state and regional). This exchange can be for web, mail or by any other mechanism or service available to citizens. Our certificates are also being used by private companies to secure their business.

6.CA Contact Information
- •CA Email Alias: arangi@accv.es, jamador@accv.es
- •CA Phone Number: 0034961923161, 606943079
- •Title / Department: Systems and development department

Technical information about each root certificate

1.Certificate Name
- •ACCVRAIZ1

2.Certificate Issuer Field
- •C = ES
- O = ACCV
- OU = PKIACCV
- CN = ACCVRAIZ1

3.Certificate Summary
- •The purpose is to sign certificates of subordinate CAs. These in turn signed SSL certificates, user certificates for signature and identification, certificates for code signing, etc. ..

4.Root Certificate URL
- •http://www.accv.es/fileadmin/Archivos/certificados/ACCVRAIZ1.crt

5.SHA1 fingerprint 93 05 7a 88 15 c6 4f ce 88 2f fa 91 16 52 28 78 bc 53 64 17

6.Valid from (2011-05-05)

7.Valid to (2030-12-31)

8.Certificate Version (should be 3)
- •Version3

9.Certificate Signature Algorithm sha1RSA

Signing key parameters

•4096 bits.

1.Test website URL -- if you are requesting to enable the Websites (SSL/TLS) trust bit

•URL to a website whose SSL cert chains up to this root. Note that this can be a test site.

•https://ulik2.accv.es/

2.Example certificates

•If this root does not issue certificates for SSL, then provide example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s).

3.Certificate Revocation Lists (CRLs)

•(ACCVRAIZ1) http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

•(ACCVCA-110) http://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl

•(ACCVCA-120) http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

•The field nextUpdate is marked three days, and CRLs are issued every three hours. This is done to ensure leeway against incidents.

•The sections 4.9.9 of CPS

•4.9.9. Frequency of issue of CRLs

ACCV shall publish a new 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.

•CRLs have been successfully tested in Mozilla Firefox

4.OCSP (OCSP is required for EV enablement)

•http://ocsp.accv.es

•The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation: 1 hour.

•The sections of your CP/CPS specifying availability and update requirements for the OCSP service.

•4.9.11. Availability of online verification of revocation and status

ACCV provides an OCSP server for online verification of certificate status at: ocsp.accv.es:80

4.9.12. Requirements for online verification of revocation

The 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 2560.

•OCSP has been successfully tested in Mozilla Firefox.

5.Requested Trust Bits

•State which of the three trust bits you are requesting to be enabled for this root.

•Websites (SSL/TLS) -> TRUE

•Email (S/MIME) -> TRUE

•Code Signing -> TRUE

6.SSL Validation Type

•Indicate the levels of SSL validation that are used for certificates within this root's hierarchy.

•DV -- The ownership of the domain name is verified, but the identity/organization of the subscriber is not verified.

•OV -- In addition to verifying the domain ownership, you also validate the organization to be listed in the O field - making sure public record and government resources can verify the address, existence, and good legal standing of the organization itself. Verifying that the whois listed address matches the verified address, and any other additional checks that a given CA lists in its CPS.

CA Hierarchy information for each root certificate

1. CA Hierarchy
    - PKI hierarchy rooted at or otherwise associated with this root CA certificate.
        - List and/or describe all of the subordinate CAs that are signed by this root.
            - ACCVCA-110
            - ACCVCA-120
        - All CAs are operated by the ACCV.
2. Sub CAs Operated by 3rd Parties
    - None
3. Cross-Signing
    - None
4. Technical Constraints or Audits of Third-Party Issuers
    - Not applicable. All CAs are operated by the ACCV.

Verification Policies and Practices

We rely on publicly available documentation and audits of those documented processes to ascertain that the CA takes reasonable measures to confirm the identity and authority of the individual and/or organization of the certificate subscriber.

If the CP/CPS documents are not in English, then the portions of those documents pertaining to verification of the certificate subscriber **must be translated into English**. For all of the items listed below, provide both a pointer to the original document (and section or page number of the relevant text) as well as the translated text.

1. Documentation: CP, CPS, and Relying Party Agreements
    - CPS
      (EN) http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V3.0-EN.pdf
    -
2. Audits
    - WEBTRUST https://cert.webtrust.org/SealFile?seal=1352&file=pdf
    - ISO27001 http://www.accv.es/fileadmin/Archivos/iso27001/Cert-ISO27001-ACCV.pdf
3. SSL Verification Procedures
    - Websites (SSL/TLS) trust bit.

        - http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-03V3.0-c.pdf (Spanish)
        - All other policies are on the website of the ACCV http://www.accv.es. Note that issuing procedures are the same as for the other root, and in no case are issued certificates unattended. All emissions pass through a point (sometimes two) in which a human operator of the ACCV checks and verifies the data in form and substance.
        - Translate
            - 3.2.4 Checking the application domain
              The ACCV verify that domains and addresses associated with the certificate belong to the applicant by consulting the records assigned by ICANN / IANA. This check will be made with using records WHOIS queries enabled by the organization Red.es http://www.nic.es or equivalent in national domains or those provided by Verisign for generic domains (whois.verisign-grs.com) .
              Besides WHOIS query connection will be tested by secure protocol (eg HTTPS) with the domain in question if possible and test DNS response. For any irregularity ACCV contact the applicant for the license and the issuance of the certificate will be suspended until its cure. If this is not remedied within the period of one month the application would be denied.
              In the verification process, the information obtained from the WHOIS or equivalent records was compared with that provided by the applicant, sending personalized emails to technical and administrative contacts obtained from both sources and if necessary to ensure that the data is correct and that domain ownership is confirmed is make phone calls asking for clarification.
    - Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).
        - Specify the procedure for additional verification of a certificate request that is blocked.
    - If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.
        - There should be a description of the types of resources that are used to confirm the authenticity of the information provided by the certificate subscriber, what data is retrieved from public resources, and how that data is used for verification of the entity referenced in the certificate.
4. Email Address Verification Procedures
    - Email/SMIME trust bit.
        - http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-03V3.0-c.pdf (Spanish)
        - All other policies are on the website of the ACCV http://www.accv.es. Note that issuing procedures are the same as for the other root, and

in no case are issued certificates unattended. All emissions pass through a point (sometimes two) in which a human operator of the ACCV checks and verifies the data in form and substance.

- Translate
    - 3.2.4 Checking the application domain
      The ACCV verify that domains and addresses associated with the certificate belong to the applicant by consulting the records assigned by ICANN / IANA. This check will be made with using records WHOIS queries enabled by the organization Red.es http://www.nic.es or equivalent in national domains or those provided by Verisign for generic domains (whois.verisign-grs.com) .
      Besides WHOIS query connection will be tested by secure protocol (eg HTTPS) with the domain in question if possible and test DNS response. For any irregularity ACCV contact the applicant for the license and the issuance of the certificate will be suspended until its cure. If this is not remedied within the period of one month the application would be denied.
      In the verification process, the information obtained from the WHOIS or equivalent records was compared with that provided by the applicant, sending personalized emails to technical and administrative contacts obtained from both sources and if necessary to ensure that the data is correct and that domain ownership is confirmed is make phone calls asking for clarification.

5. Code Signing Subscriber Verification Procedures
    - Code Signing trust bit.
        - http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-03V3.0-c.pdf (Spanish)
        - All other policies are on the website of the ACCV http://www.accv.es. Note that issuing procedures are the same as for the other root, and in no case are issued certificates unattended. All emissions pass through a point (sometimes two) in which a human operator of the ACCV checks and verifies the data in form and substance.
        - Translate
            - 3.2.4 Checking the application domain
              The ACCV verify that domains and addresses associated with the certificate belong to the applicant by consulting the records assigned by ICANN / IANA. This check will be made with using records WHOIS queries enabled by the organization Red.es http://www.nic.es or equivalent in national domains or those provided by Verisign for generic domains (whois.verisign-grs.com) .
              Besides WHOIS query connection will be tested by secure protocol (eg HTTPS) with the domain in question if possible and test DNS response. For any irregularity ACCV contact the applicant for the license and the issuance of the certificate will be suspended until its cure. If this is not remedied within the period of one month the application would be denied.
              In the verification process, the information obtained from the

WHOIS or equivalent records was compared with that provided by the applicant, sending personalized emails to technical and administrative contacts obtained from both sources and if necessary to ensure that the data is correct and that domain ownership is confirmed is make phone calls asking for clarification.

6. Multi-factor Authentication
    - All accounts capable of directly causing certificate issuance require user certificates on smart card. Besides access to the certificate issuance system can only be made from selected systems, with specific IP addresses.
7. Network Security
    - Confirm that you have done the following, and will do the following on a regular basis:
        - Check for mis-issuance of certificates, especially high-profile domains. Yes
        - Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. Yes.
        - Ensure Intrusion Detection System and other monitoring software is up-to-date. Yes.
        - Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion. Yes.