This summary is to respond to Comment # 52, case 667466, Mozilla - CA Program.

General information about CA's associated organization

CA Email Alias 1 admin-pki@fii.gob.ve

Response to Mozilla's list of Recommended Practices

CA's Response to Recommended Practices

NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices

1) Publicly Available CP and CPS:
CP: https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20natural/080-PCN-F015-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20juridica/080-PCJ-F016-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_email-F017/080-PCS-F017-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_ssl-F073/080-PCS-F073-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_vpn-F072/080-PCS-F072-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_vpn-F072/080-PCS-F072-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20desatendida/080-PCD-F020-INGLES.pdf
https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20empleado%20publico/080-PCF-F021-INGLES.pdf

CPS: https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/DPC/080-DPC-F014-INGLES.pdf

2) CA Hierarchy: in CPS section 8.9 CERTIFICATION AUTHORITY HIERARCHY

3) Audit Criteria: in CPS section 17 COMPLIANCE AUDIT

4) Document Handling of IDNs in CP/CPS: in CPS section 12.2.2. ORGANIZATION IDENTITY AUTHENTICATION

5) Revocation of Compromised Certificates: in CPS section 12.4 KEY REVOCATION REQUESTS IDENTIFICATION

AND AUTHENTICATION

6) Verifying Domain Name Ownership: in CP (https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_ssl-F073/080-PCS-F073-INGLES.pdf) section 13.1. APPLICATION FOR PSC-FII CERTIFICATE

7) Verifying Email Address Control: in CP section 13.1.2. CERTIFICATE REQUEST GENERATION PROCESS AND OBLIGATIONS (-8. RA Operator or VA Operator, -9. RA operator or VA operator, -10. Subscriber, -11. PSC-FII´s RA, -12. RA operator or VA operator, -13. CA-FII, -14. Signatory)

8) Verifying Identity of Code Signing Certificate Subscriber:
Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates.

9) DNS names go in SAN: in CPS section 6.1. CERTIFICATE PROFILE (the CA certificate is in the extension subjectAlternativeName the DNS field has the value of the IP address domain name)

10) Domain owned by a Natural Person: in CPS section 12.2.2.3. AUTHENTICATION OF SIGNATORY´S IDENTITY (Description of regular process (Interview at FII administrative headquarters, Interview at the customer´s headquarters, (Videoconference)

11) OCSP: in CPS section 16.1 CERTIFICATE PROFILE

12) Network Security Controls: in CPS section 15.7. CONTROLS NETWORK SECURITY

Response to Mozilla's list of Potentially Problematic Practices

CA's Response to Problematic Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices

CPS = https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/DPC/080-DPC-F014-INGLES.pdf

CP = https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_ssl-F073/080-PCS-F073-INGLES.pdf

1) Long-lived DV certificates: in CP (https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/PC/pc%20servidor/pc_serv_ssl-F073/080-PCS-F073-INGLES.pdf) 15.3.2. OPERATIONAL PERIODS OF CERTIFICATES AND PERIOD FOR USE OF PAIR OF KEYS.

2) Wildcard DV SSL certificates: Is not defined in the CPS nor the CP.

3) Email Address Prefixes for DV Certs: No restriction in the CPS nor the CP.

4) Delegation of Domain / Email validation to third parties: in CPS 13.1.1. PSC-FII CERTIFICATE REQUEST, 13.1.2. CERTIFICATE REQUEST GENERATION PROCESS AND OBLIGATIONS "- 7. Subscriber: The signatory must provide the identity documents requested by the RA operator (On the CP, for each type of Certificate, Section 13.1 APPLICATION FOR CERTIFICATE OF PSC-FII, published in https://publicador-psc.fii.gob.ve/pc one can get information about the identity documents that are required.
Not delegated, because the CPS indicates that the AR / AV Operator is the one that verifies the collections.

5) Issuing end entity certificates directly from roots: in CPS section 8.9. CERTIFICATION AUTHORITY HIERARCHY, 11.2. PUBLICATION OF CERTIFICATION INFORMATION

6) Allowing external entities to operate subordinate CAs: No, in CPS section 18.6.4. OBLIGATIONS OF THE CA-FII (Infrastructure and Organizational).

7) Distributing generated private keys in PKCS#12 files: in CPS section 15.4.2

8) Certificates referencing hostnames or private IP addresses: Certificates refer to host names and / or private IP addresses, in CPS 16.1

9) Issuing SSL Certificates for Internal Domains: No restriction in the CPS nor the CP.

10) OCSP Responses signed by a certificate under a different root: Yes, in CSP section 9.1. PERMITTED USES (CERTIFICATE TYPE-OCSP SERVER).

1**1) SHA-1 Certificates:** No, in CPS section 16.1.3. OBJECT IDENTIFIER (OID) OF ALGORITHMS

12) Generic names for CAs: in CPS sections 12.1.1 and 12.1.4.

13) Lack of Communication With End Users: ?Yes, in CPS sections 11.2. PUBLICATION OF CERTIFICATION INFORMATION, 11.3.2. (CERTIFICATION PRACTICE STATEMENT) CPS and 13.1.2. CERTIFICATE REQUEST GENERATION PROCESS AND OBLIGATIONS (1. Subscriber).

14) Backdating the notBefore date: Yes, in CPS section 16.1. CERTIFICATE PROFILE (Validity).

Test Results (When Requesting the SSL/TLS Trust Bit)

CA/Browser Forum Lint Test	test website: https://crt.sh/ all errors must be fixed in CA/Browser Forum lint: **The certificate of the CA of the PSC-FII, has as critical the extension keyUsage, see in CPS section 16.1. CERTIFICATE PROFILE.**

CA Hierarchy Information

Cross Signing	No restriction in the CPS nor the CP.

Verification Policies and Practices

Auditor Name	Milthon J. Chavez
Auditor Website	
Standard Audit	https://bug667466.bmoattachments.org/attachment.cgi?id=8670835
BR Audit	As specified in the CPS (https://publicador-psc.fii.gob.ve/docs/DPC_PC2016/DPC/080-DPC-F014-INGLES.pdf) Sections 17.1, 17.2. and 17.4.

BR Audit Type	ETSI TS 102 042: in CPS sectio 4. NORMATIVE REFERENCE.
BR Audit Statement Date	6/12/2015
BR Commitment to Comply	in CPS section 4 and Validated by the External Auditor.

EQUIPO DEL INFORME					
NOMBRE	**CARGO**	**FIRMA**	**NOMBRE**	**CARGO**	**FIRMA**
María Liendo	Especialista de Normalización		**Daniel Sandoval**	Jefe del Centro de Seguridad Informática y seguridad Electrónica	