TECHNICAL INFORMATION ABOUT EACH ROOT CERTIFICATE (PSC PUBLICO DEL MPPCTII PARA EL ESTADO VENEZOLANO)

CA INFORMATION	DESCRIPTION
1. Certificate Name	PSC Publico del MppCTII para el Estado Venezolano
2. Certificate Issuer Field	Autoridad de Certificacion Raiz del Estado Venezolano (PSC is signaed by The SUSCERT root.)
3. Certificate Summary	The **PSC Publico del MppCTII para el Estado Venezolano** (PSC-FII) is the first public provider credited by the Venezuelan state to offer electronic signature certificates. Is a subCA under the venezuelan root of certification ("Sistema Nacional de Certificacion Electronica"). Types of certificates: Persona Natural: (Digital Signature), Content Commitmen (Non Repudiation). This type of certificate authorizes the signing of e-mail and documents with CE in the name of the natural person appearing as a signatory. Perdona Jurídica:Digital Signature), Content Commitmen (Non Repudiation). This type of certificate authorizes the email signature and documents with the CE on behalf of the legal person that figure as a signatory. Empleado Público: Digital Signature and/or encryption of messages, email and documents to manage inside the public institution on behalf of the public employee as a signatory. Firma Desatendida: Digital Signature), Key Encipherment, Content Commitmen (Non Repudiation). Used to identify a legal person, company or society when making arrangements making use of unattended electronic signature.In this case, the entity is represented by a legal representative, acting on behalf of the company that represents. Operador AR/AC: Digital Signature), Key Encipherment, Content Commitmen (Non Repudiation).Used by ICP staff, for the operations of RA and the PSCFII AC. This PC is for internal use. Servidor Web (SSL): Digital Signature, Content Commitmen (Non Repudiation), Key Encipherment, Data Encipherment, TLS Web Client AuthenticationUsed to prove the identity of the server on the network, ensuring the transmission of encrypted data. Servidor E-Mail: Digital Signature), Content Commitmen (Non Repudiation), Key Encipherment y E-mail Portecton. Used to ensure and guarantee the integrity of the e-mails, users, passwords on the mail server. Servidor VPN: Digital Signature, Content Commitmen (Non Repudiation), Key Encipherment, Data Encipherment, VPN, TLS Web Client Authenticatio). Used to verify both the identity of the issuer and protection in a secure channel transactions/communications. Servidor OCSP:Digital Signature, Content Commitmen (Non Repudiation), Key Encipherment, OCSP Signing. Used to obtain information about the status of the certificates issued by your AC, indicating if the certificate is active, suspended or revoked, returning their signed response. This PC is for internal use. Firma de Código: Digital Signature, Content Commitmen (Non Repudiation), Key Encipherment, Data Encipherment, Code Signing, E-mail Protection. Used to ensure the authenticity and integrity of a software code.
4. Root Certificate URL	Root Certificate (Autoridad de Certificacion Raiz del Estado Venezolano): https://ar.fii.gob.ve/pub/caraiz/cariz.crt Root Certificate (PSC Publico del MppCTII para el Estado Venezolano): https://ar.fii.gob.ve/pub/cacert/cacert.crt
5. SHA1 fingerprint	3E:B1:8B:67:37:B3:30:2F:03:55:16:34:58:1C:FB:BF:38:EA:92:96 (PSC Publico del MppCTII para el Estado Venezolano)
6. Valid from (YYYY-MM-DD)	2011.01.25
7. Valid to (YYYY-MM-DD)	2021.01.22
8. Certificate Version (should be 3)	X.509 v3

9. Certificate Signature Algorithm	PKCS #1 SHA-256 con cifrado RSA
10. Signing key parameters	4096
11. Test website URL -- if you are requesting to enable the Websites (SSL/TLS) trust bit	https://publicador-psc.fii.gob.ve
12. Example certificates	https:/publicador-psc.fii.gob.ve
13. Certificate Revocation Lists (CRLs)	https://publicador-psc.fii.gob.ve/crlsha256/cacrl.crl
14. OCSP (OCSP is required for the SSL trust bit to be enabled)	http://publicador-psc.fii.gob.ve:2560/ocsp
15. Test Revocation	https://certificate.revocationcheck.com/publicador-psc.fii.gob.ve
16. Requested Trust Bits	**1.** Websites (SSL/TLS) **2.** Email (S/MIME) **3.** Code Signing
17. SSL Validation Type	DV
18. The EV certificates are issued within the hierarchy rooted at this root	None

EQUIPO DEL INFORME					
NOMBRE	**CARGO**	**FIRMA**	**NOMBRE**	**CARGO**	**FIRMA**
Maria Liendo	PIDTI-Especialista de Normalización				