NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI-Paraguay

LIZ ROSANNA CRAMER CAMPOS

Firmado digitalmente por LIZ ROSANNA CRAMER CAMPOS
Fecha: 2020.09.30 16:52:53 -04'00'

DOC-PKI-06

Versión 2.0

CONTROL DOCUMENTAL

Documento	
Título: Normas de algoritmos Criptográficos PKI-Paraguay	**Nombre Archivo:** DOC-PKI-06 V2.0
Código: DOC-PKI-06	**Soporte Lógico:** https://www.acraiz.gov.py/
Fecha: 30/09/2020	**Ubicación Física:** DGFDyCE
Versión: 2.0	

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	28/10/2016	Versión inicial
2.0	30/09/2020	Generación de las Claves Asimétricas de Usuarios finales
		Firma de Listas de Certificados Revocados CRL y Respuestas OCSP
		Firma Digital de la PKI-Paraguay CAdES, XAdES y PAdES
		Estándares de Hardware

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)

Autoridad Certificadora (CA)	Prestadores de Servicios de Certificación (PSC)
Documento Público	https://www.acraiz.gov.py/

Control del Documento		
Elaborado por:	**Verificado por:**	**Aceptado por:**
JENNY ELIZABETH RUIZ DIAZ LEZCANO Digitally signed by JENNY ELIZABETH RUIZ DIAZ LEZCANO Date: 2020.09.30 14:17:47 -04'00'	MARIA LUJAN OJEDA CHAMORRO Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO Fecha: 2020.09.30 15:18:19 -04'00'	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2020.09.30 15:35:56 -04'00'
JENNY RUÍZ DÍAZ	**LUJAN OJEDA**	**LUCAS SOTOMAYOR**

Contenido

1. INTRODUCCIÓN

Este documento regula el estándar de hardware, algoritmos y parámetros criptográficos que serán utilizados en todos los procesos realizados en el ámbito de la Infraestructura de Claves Públicas del Paraguay (PKI-Paraguay), que incluyen, entre otros:

a) generación de claves criptográficas;
b) solicitud, emisión y revocación de certificados digitales;
c) generación y verificación de firmas digitales;
d) cifrado de mensajes; y
e) autenticación con certificados digitales.

Las directrices contenidas en este documento deben ser cumplidas obligatoriamente por las autoridades de certificación(CA Raíz-Py y PSC), autoridades de registro (RA), prestadores de servicios de soporte (PSS), Prestadores de Servicio de Almacenamiento (PSA), las empresas de Auditoría Independiente y otros organismos acreditados o registrados ante la PKI-Paraguay a través del Ministerio de Industria y Comercio, así como también por los titulares finales y los desarrolladores de aplicaciones que utilizan certificados digitales de PKI-Paraguay.

2. SIGLAS Y ACRÓNIMOS

Sigla/Acrónimo	Descripción
CA	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
CA Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CAdES	CMS Advanced Electronic Signature
CBC	Cipher Block Chaining
CP	Política de Certificación (CP por sus siglas en inglés, Certificate Policy)
DOC-PKI	Documentos principales de la Infraestructura de Claves Públicas del Paraguay
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
GCM	Galois/Conter Mode
MIC	Ministerio de Industria y Comercio
PAdES	PDF Advanced Electronic Signature
PKI	Infraestructura de Claves Públicas PKI por sus siglas en inglés, Public Key Infrastructure).

PKI-Paraguay	Infraestructura de Claves Públicas del Paraguay.
PSC	Prestador de Servicios de Certificación.
RSA	Rivest, Shamir and Adleman Algorithm
SHA	Secure Hash Algorithm
XAdES	XML Advanced Electronic Signature

3. APLICABILIDAD DE LOS ALGORITMOS Y PARÁMETROS CRIPTOGRÁFICOS

Esta sección relaciona los principales procedimientos que involucra a la criptografía en el ámbito de la PKI-Paraguay, con los algoritmos y parámetros que deben ser utilizados obligatoriamente, para su ejecución, y los documentos normativos que tratan dichos procedimientos.

Solicitud de certificados a la CA	
Normativa PKI-Paraguay	DOC-PKI-02 [1] - ítem 4.1.1 CP CA Raíz
	DOC-PKI-02 [1] - ítem 6.1.3 CP CA Raíz
	DOC-PKI-03 [2] - ítem 6.1.3
	DOC-PKI-04 [3] - ítem 6.1.3

Formato	Estándar PKCS#10

Entrega de certificados emitidos por la CA	
Normativa PKI-Paraguay	DOC-PKI-02 [1] - ítem 4.3.1
	DOC-PKI-02 [1] - ítem 6.1.4
	DOC-PKI-03 [2] - ítem 6.1.4
	DOC-PKI-04 [3] - ítem 6.1.4
Formato	Estándar PKCS#7

Generación de las Claves Asimétricas de la CA	
Normativa PKI-Paraguay	DOC-PKI-02 [1] - ítem 6.1.1
	DOC-PKI-02 [1] - ítem 6.1.5
	DOC-PKI-03 [2] - ítem 6.1.5
	DOC-PKI-04 [3] - ítem 6.1.5
Algoritmo	RSA

Tamaño de clave	RSA 4096

Generación de las Claves Asimétricas de Usuarios finales	
Normativa PKI-Paraguay	DOC-PKI-04 [3] - ítem 6.1.5
	DOC-PKI-04 [3] - ítem 6.1.1
	DOC-PKI-08 [5] - ítem 7.5.1
Algoritmo	RSA
Tamaño de clave F1 y C1	RSA 2048
Tamaño de clave F2, F3, C2 y C3	RSA 2048 o RSA 4096

Firma de Certificados de la CA	
Normativa PKI-Paraguay	DOC-PKI-02 [1] - ítem 7.1.3
	DOC-PKI-03 [2] - ítem 7.1.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Firma de certificados de Usuarios Finales	
Normativa PKI-Paraguay	DOC-PKI-04[3] - ítem 7.1.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Firma de Listas de Certificados Revocados CRL y Respuestas OCSP	
Normativa PKI-Paraguay	DOC-PKI-02 [1] - ítem 7.2 y 7.3
	DOC-PKI-03 [2] - ítem 7.2 y 7.3
	DOC-PKI-04 [3] - ítem 7.2 y 7.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Guarda de la Clave Privada de la entidad titular y de su Backup	
Normativa PKI-Paraguay	DOC-PKI-04 [3] - ítem 6.1.1
	DOC-PKI-04 [3] - ítem 6.2.4
	DOC-PKI-03 [2] - ítem 6.2.4

Algoritmo y tamaño de clave	3DES – 112 bits AES – 128 o 256 bits
Modo de operación	CBC o GCM

Firma Digital de la PKI-Paraguay CAdES, XAdES y PAdES	
Normativa PKI-Paraguay	DOC-PKI-08 [5] - ítem 7.6.2
Tipo de certificado	F1, F2 y F3
Función de Resumen (Función HASH)	SHA - 1 SHA - 256 SHA - 512
Suite de Firmas	sha1WithRSAEncryption sha256WithRSAEncryption sha512WithRSAEncryption

Esquema de acuerdo de claves
RSA 2048
RSA 4096

Esquema de Envelopes Criptográficos
3desWithRSA1024Encryption
3desWithRSA2048Encryption
aes128WithRSA2048Encryption
aes256WithRSA4096Encryption

4. ESTÁNDARES DE HARDWARE

En la siguiente tabla se relaciona los estándares mínimos a ser empleados en los hardware criptográficos utilizados en la PKI-Paraguay con los documentos normativos que tratan su uso.

Utilización	Requisito obligatorio	Estándares	Norma
Módulo criptográfico de generación de claves asimétricas de usuario final.	Homologado por el MIC	• FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). • FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2). • FIPS 140-2 nivel 3 (para certificados tipo F3 o C3).	DOC-PKI-03 [2] - ítem 6.2.1 DOC-PKI-04 [3] - Ítem 6.2.1 DOC-PKI-07 [4] - Ítem 6.4 DOC-PKI-08 [5] - Ítem 7.3.3

Módulo criptográfico para almacenamiento de la clave privada del usuario final titular del certificado.	Homologado por el MIC	• FIPS 140-2 nivel 2 o nivel 1 (para certificados tipo F1o C1). • FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2). • FIPS 140-2 nivel 3 (para certificados tipo F3 o C3).	DOC-PKI-04 [3] - ítem 6.2.1 y 6.2.7 DOC-PKI-07 [4] - Ítem 6.4 DOC-PKI-08 [5] - Ítem 7.3.3
Parámetro de generación de claves asimétricas de usuario final.	Homologado por el MIC	• FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). • FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2). • FIPS 140-2 nivel 3 (para certificados tipo F3 o C3).	DOC- PKI-04 [3] - ítem 6.1.6 DOC-PKI-07 [4] - Ítem 6.4 DOC-PKI-08 [5] - Ítem 7.3.3
Módulo criptográfico de generación de claves asimétricas para el PSC.	Homologado por el MIC	• FIPS 140-2 nivel 3	DOC-PKI-03 [2] - ítem 6.2.1
Módulo criptográfico para almacenamiento de la clave privada del PSC.	Homologado por el MIC	• FIPS 140-2 nivel 3	DOC-PKI-03 [2] - ítem 6.2.7

Parámetro de generación de claves asimétricas del PSC	Homologado por el MIC	• FIPS 140-2 nivel 3	DOC- PKI-03 [2] - ítem 6.1.6
Módulo criptográfico de generación de claves asimétricas para CA Raíz-Py.		• FIPS 140-2 nivel 3	DOC- PKI-02 [1] - ítem 6.2.1
Módulo criptográfico para almacenamiento de la clave privada de la CA Raíz-Py.		• FIPS 140-2 nivel 3	DOC- PKI-02 [1] - ítem 6.8
Parámetro de generación de claves asimétricas de la CA Raíz-Py.		• FIPS 140-2 nivel 3	DOC- PKI-02 [1] - ítem 6.1.6
Proceso para Verificación de parámetros de generación de claves asimétricas de la CA Raíz-Py.		• FIPS 140-2 nivel 3	DOC- PKI-02 [1] - ítem 6.1.6 DOC- PKI-03 [2] - ítem 6.1.6 DOC- PKI-04 [3] - ítem 6.1.6

5. DOCUMENTOS DE REFERENCIA

5.1 REFERENCIAS

- Ley N° 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Ley N° 4610/2012 " que modifica y amplia la ley nº 4017/10 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Decreto N° 7369/2011 "Por el cual se aprueba el reglamento general de la ley nº 4017 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
-

5.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Política de certificación de la autoridad certificadora raíz del Paraguay.	DOC-PKI-02
[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores de servicios de certificación de la PKI-Paraguay.	DOC-PKI-03
[3]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los prestadores de servicios de certificación de la PKI-Paraguay.	DOC-PKI-04
[4]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores de servicio de almacenamiento de la PKI-Paraguay.	DOC-PKI-07

[5]	Procedimientos operacionales mínimos para los prestadores de servicios de almacenamiento de la PKI-Paraguay.	DOC-PKI-08