ANEXO Nº 03
REPORTE DE EVALUACION DEL MÓDULO CRITOGRÁFICO

GENERACIÓN DE CERTIFICADOS DIGITALES DE CLASE III PARA ENTIDADES FINALES EMITIDOS POR LA ECEP-RENIEC

REPORTE N°	2020-01	FECHA	16/11/2020	VERSIÓN	1.0

1. DATOS GENERALES DEL MÓDULO

PRESENTACIÓN	
1. Token	
USB	X
2. Smart Card	
Contacto	
Proximidad	
Dual	
3. Software	

DATOS DEL PRODUCTO		
Nombre del módulo	mToken CryptoID	
Marca del producto	Longmai	
Modelo del producto	E	
Número de serie lógico	4CA1195946E0481D	
Número de serie físico	PE200702743	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		NO

MIDDLEWARE DEL PRODUCTO			
Nombre del Middleware	Utilidad de Certificados mToken CryptoID	Versión del Middleware	2.2.18.928
Librería PKCS#11	cryptoide_pkcs11.dll	Fecha de despliegue	05/11/2020

2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA		
FIPS 140-2	Nivel	3	SI
	URL Nivel	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2626	
	URL Certificado	https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/FIPS140ConsolidatedCertApril2016.pdf	
Common Criteria	Nivel	---	NO
	URL HW	---	
	URL FW	---	
	URL APP	---	

ETAPA II	INTEROPERABILIDAD TÉCNICA
Generación de par de llaves RSA de 2048 bits	SI
Generación de CSR	SI
Importación de certificado de entidad final (usuario)	SI
Importación de certificados digitales de autoridades (intermedia y raíz)	SI
¿La librería PKCS#11 funciona en modo standalone?	SI

Nota: El certificado generado pertenece a la jerarquía de certificación ECERNEP PERU CA ROOT 3

3. VERIFICACIÓN DE GENERACIÓN DE FIRMA DIGITAL

Prueba satisfactoria de generación de firma digital con el software ReFirma 1.5.4 acreditado por la AAC	SI

4. CONCLUSIÓN

¿Cumple los requisitos mínimos?	SI

5. OBSERVACIONES Y COMENTARIOS

Prueba de generación de firma digital de documentos PDF con Adobe Acrobat Reader DC 2020.013.20064: conforme
La longitud del PIN permite 6 caractéres como mínimo y 32 como máximo, caractéres alfanuméricos y especiales
El middleware del dispositivo conserva el PIN en cache al realizar la firma digital de documentos en lote
Tiempo mínimo de generación de llaves asimétricas detectado: 2 segundos
El dispositivo contempla definir un PIN de Usuario, y un PIN de Administrador

Nota: En el contexto de este documento, el acrónimo PIN (Personal Identification Number) se utiliza para referirse a una secuencia de caracteres alfanuméricos