FICHA III

REPORTE DE EVALUACION DE DISPOSITIVO CRITOGRÁFICO PARA GENERACIÓN DE CERTIFICADOS DIGITALES DE CLASE III PARA ENTIDADES FINALES EMITIDOS POR LA ECEP-RENIEC					
REPORTE N°	2018-02	**FECHA**	01/03/2018	**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

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

DATOS DEL PRODUCTO		
Marca	Gemalto	
Modelo	SafeNet eToken 5110	
Número de serie lógico	0x025ceb01	
Número de serie físico	025CEB01	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		SI

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	SafeNet Authentication Client Tools	Versión del Manager	10.3.25.0
Librería PKCS#11	C:\Windows\System32\eTPKCS11.dll	Fecha de despliegue	29/03/2017

2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA		
FIPS 140-2	Nivel	3	SI
	URL Nivel	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2825	
	URL Certificado	https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/FIPS140ConsolidatedCertJan2017.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?	NO

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 1.4.8 acreditado por la AAC	SI

4. CONCLUSIÓN

¿Cumple los requisitos mínimos?	SI

5. OBSERVACIONES Y COMENTARIOS

Prueba de generación de firma digital de correo electrónico con Microsoft Outlook: conforme
Prueba de generación de firma digital de documentos PDF con Adobe Acrobat Reader DC: conforme
El proceso de generación del certificado digital de usuario final, requiere que el manager del dispositivo esté correctamente instalado en el S.O.
La longitud del PIN permite 8 caractéres como mínimo y 24 como máximo, caractéres alfanuméricos y especiales, por defecto
El manager del dispositivo requiere ingresar el PIN cada vez al realizar la firma digital de un lote de documentos
Tiempo mínimo de generación de llaves asimétricas detectado: 7 segundos
El dispositivo contempla definir un PIN de Usuario, y un PIN de Administrador
La entidad debe coordinar con el proveedor del dispositivo criptográfico, la integración funcional del dispositivo en sus sistemas de información

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