

FICHA III

REPORTE DE EVALUACION DE DISPOSITIVO CRITOGRAFICO PARA GENERACION DE CERTIFICADOS DIGITALES DE CLASE III PARA ENTIDADES FINALES EMITIDOS POR LA ECEP-RENIEC					
REPORTE N°	2017-03	FECHA	27/01/2017	VERSIÓN	1.1

1. DATOS GENERALES DEL DISPOSITIVO

PRESENTACIÓN		DATOS DEL PRODUCTO			
1. Token		Marca	SafeNet		
USB	X	Modelo	eToken 5100		
2. Smart Card		Número de serie lógico	0230ccf6		
Contacto		Número de serie físico	0230CCF6		
Proximidad		¿Cuenta con drivers?		SI	
Dual		¿Cuenta con manuales?		SI	

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	SafeNet Authentication Client Tools	Versión del Manager	9.0.43.0
Librería PKCS#11	C:\Windows\System32\TPKCS11.dll	Fecha de despliegue	23/01/2015

2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA			
FIPS 140-2	Nivel	3		SI
	URL Nivel	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1883		
	URL Certificado	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0026.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 SHA1 de la ECEP-RENIEC

3. VERIFICACIÓN DE GENERACIÓN DE FIRMA DIGITAL

Prueba satisfactoria de generación de firma digital con el software ReFirma 1.4.7 acreditado por la AAC	SI
---	----

4. CONCLUSIÓN

¿Cumple los requisitos mínimos?	SI
---------------------------------	----

5. OBSERVACIONES Y COMENTARIOS

<p>Prueba de generación de firma digital de correo electrónico con Microsoft Outlook: conforme</p> <p>Prueba de generación de firma digital de documentos PDF con Adobe Acrobat Reader XI: conforme</p> <p>El proceso de generación del certificado digital de usuario final, requiere que el manager del dispositivo esté correctamente instalado en el S.O.</p> <p>La longitud del PIN permite 6 caracteres como mínimo y 20 como máximo, caracteres alfanuméricos y especiales</p> <p>El manager del dispositivo conserva el PIN en cache al realizar la firma digital de documentos en lote</p> <p>Tiempo mínimo de generación de llaves asimétricas detectado: 9 segundos</p> <p>El dispositivo contempla definir un PIN de Usuario</p>
--

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