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°	2017-14	**FECHA**	21/12/2017	**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

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

DATOS DEL PRODUCTO		
Marca	Advanced Card Systems Ltd.	
Modelo	CryptoMate Nano ACOS5T2-B (CTMT2-B)	
Número de serie lógico	9013005BA10A6500	
Número de serie físico	RC013-00678	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		SI

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	ACS Certificate Management Essentials	Versión del Manager	4.6.0.0
Librería PKCS#11	C:\WINDOWS\System32\acospkcs11.dll	Fecha de despliegue	08/03/2017

2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA		
FIPS 140-2	Nivel	3	SI
	URL Nivel	https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2664	
	URL Certificado	https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/FIPS140ConsolidatedCertJune2016.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)	NO
¿La librería PKCS#11 funciona en modo standalone?	NO

Nota: El certificado generado pertenece a la jerarquía de certificación SHA-256 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

Prueba de generación de firma digital de correo electrónico con Microsoft Outlook 2010: conforme
Prueba de generación de firma digital de documentos PDF con Adobe Acrobat Reader XI: conforme
El proceso de generación del certificado digital de usuario final, requiere que el manager del dispositivo esté correctamente instalado en el S.O.
El dispositivo criptográfico solo permite la importación del certificado digital del usuario final
La longitud del PIN permite 4 caractéres como mínimo y 8 como máximo, caractéres alfanuméricos y especiales
El manager del dispositivo conserva el PIN en cache al realizar la firma digital de documentos en lote, por defecto
Tiempo mínimo de generación de llaves asimétricas detectado: 18 segundos
La entidad será responsable del despliegue de los certificados digitales de autoridades del RENIEC, en sus sistemas de información
El dispositivo contempla definir un PIN de Usuario (ACS Certificate Management Essentials), y un PIN de Administrador

Es responsabilidad exclusiva del proveedor y fabricante del producto brindar el soporte técnico necesario en cuanto a la configuración y el uso

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