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°	2016-02	**FECHA**	24/05/2016	**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

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

DATOS DEL PRODUCTO		
Marca	Athena Smartcard	
Modelo	MS-IDProtect Key with Laser PKI	
Número de serie lógico	0A53001133134606	
Número de serie físico	J001995	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		SI

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	IDProtect Manager	Versión del Manager	6.28.04
Librería PKCS#11	C:\Windows\System32>asepkcs.dll	Fecha de despliegue	15/12/2013

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#1750	
	URL Certificado	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0019.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 1.2.1 acreditado por la AAC	SI

4. CONCLUSIÓN

¿Cumple los requisitos mínimos?	SI

5. OBSERVACIONES Y COMENTARIOS

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 máxima del alias del certificado digital generado en el dispositivo es de 38 caractéres
El proveedor del usuario entregó un brochure del dispositivo criptográfico que no ha sido emitido por el fabricante
El dispositivo solo permite importar certificados digitales cuyos datos contengan los caracteres imprimibles ASCII (Alfabeto Ingles), no soporta el conjunto ASCII extendido, que contempla el uso de caracteres especiales como la ñ, Ñ, ü, Ü, ´, entre otros del conjunto

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