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°	2016-03	**FECHA**	29/11/2016	**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

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

DATOS DEL PRODUCTO		
Marca	Sagem Orga	
Modelo	ypsID S2 v2 Iden	
Número de serie lógico	0001509614141410	
Número de serie físico	---	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		SI

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	Morpho Middleware ypsID	Versión del Manager	6.3.2
Librería PKCS#11	C:\Windows\System32\CnfPkcs11v220.dll	Fecha de despliegue	10/12/2013

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-historical.htm#1459	
	URL Certificado	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1459.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 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

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 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 generación del par de llaves y del certificado digital de usuario final se autorizó utilizando el PIN de la tarjeta
La longitud del PIN permite 8 caractéres como mínimo y 256 como máximo, caractéres alfanuméricos y especiales
El manager del dispositivo conserva el PIN en cache al realizar la firma digital de documentos en lote
Tiempo mínimo de generación de llaves asimétricas detectado: 15 segundos
La longitud máxima del alias del certificado digital generado en el dispositivo es de 31 caractéres
La entidad será responsable del despliegue de los certificados de autoridades del RENIEC, en sus sistemas de información
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