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°	2018-06	**FECHA**	21/09/2018	**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

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

DATOS DEL PRODUCTO		
Marca	Feitian EnterSafe	
Modelo	BePass2003	
Número de serie lógico	24FA34B8001E0016	
Número de serie físico	---	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		SI

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	Administrador EnterSafe PKI – ePass2003	Versión del Manager	1.1.18.321
Librería PKCS#11	C:\Windows\SysWOW64\eps2003csp11.dll	Fecha de despliegue	20/03/2018

2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA		
FIPS 140-2	Nivel	3	SI
	URL Nivel	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2204	
	URL Certificado	https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/certificates/FIPS140ConsolidatedCertList0043.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?	SI

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 PDF 1.5.2 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
La longitud del PIN permite 8 caractéres como mínimo y 255 como máximo, caractéres alfanuméricos y especiales, por defecto
El manager guarda en la memoria cache de la estación el PIN del dispositivo, al realizar la firma digital de un lote de documentos
Tiempo mínimo de generación de llaves asimétricas detectado: 4 segundos
La generación de certificados digitales y la generación de firmas digitales, se realizó utilizando la interface USB proveida por el dispositivo
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