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°	2018-04	**FECHA**	18/05/2018	**VERSIÓN**	1.1

1. DATOS GENERALES DEL DISPOSITIVO

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

DATOS DEL PRODUCTO		
Marca	Bit4ID	
Modelo	JS2048 (L)	
Número de serie lógico	2444009000000013	
Número de serie físico	---	
¿Cuenta con drivers?		SI
¿Cuenta con manuales?		NO

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	Bit4ID Universal MW	Versión del Manager	1.4.2.273
Librería PKCS#11	C:\Windows\SysWOW64\bit4xpki.dll	Fecha de despliegue	29/08/2016

2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA		
FIPS 140-2	Nivel	---	NO
	URL Nivel	---	
	URL Certificado	---	
Common Criteria	Nivel	EAL5+	SI
	URL HW	https://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC_2012-68fr.pdf	
	URL FW	https://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC-2015_16.pdf	
	URL APP	https://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC-2015_17.pdf	

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 1.4.8 acreditado por la AAC	SI

4. CONCLUSIÓN

¿Cumple los requisitos mínimos?	SI

5. OBSERVACIONES Y COMENTARIOS

La generación de certificados digitales y la generación de firmas digitales, se realizó utilizando la interface USB proveída por el dispositivo
Tiempo mínimo de generación de llaves asimétricas detectado: 13 segundos
La longitud del PIN permite 4 caractéres como mínimo y 8 como máximo, caractéres alfanuméricos y especiales
El dispositivo contempla definir un PIN de Usuario, y un PIN de Administrador
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 manager del dispositivo conserva el PIN en cache al realizar la firma digital de documentos en lote
Prueba de generación de firma digital utilizando un smartphone con Android 7.0, el app DDNA y la interfaz bluethoot del dispositivo: conforme
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