

### FICHA III

#### REPORTE DE EVALUACION DE DISPOSITIVO CRITOGRAFICO PARA GENERACION DE CERTIFICADOS DIGITALES DE CLASE III PARA ENTIDADES FINALES EMITIDOS POR LA ECEP-RENIEC

REPORTE N°	2017-11	FECHA	17/05/2017	VERSIÓN	1.1
------------	---------	-------	------------	---------	-----

#### 1. DATOS GENERALES DEL DISPOSITIVO

PRESENTACIÓN		DATOS DEL PRODUCTO	
<b>1. Token</b>		Marca	Bit4ID
USB	X	Modelo	tokenME V2 (Vault!C405)
<b>2. Smart Card</b>		Número de serie lógico	244412600009036
Contacto		Número de serie físico	---
Proximidad		¿Cuenta con drivers?	SI
Dual		¿Cuenta con manuales?	NO

MIDDLEWARE DEL PRODUCTO			
Nombre del Manager	Bit4ID PKI Manager	Versión del Manager	1.4.8.359
Librería PKCS#11	C:\Windows\SysWOW64\bit4xpki.dll	Fecha de despliegue	29/08/2016

#### 2. EVALUACIÓN

ETAPA I	INTEROPERABILIDAD NORMATIVA		
FIPS 140-2	Nivel	3	SI
	URL Nivel	<a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2158">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2158</a>	
	URL Certificado	<a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0041.pdf">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0041.pdf</a>	
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 SHA1 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: conforme  
 Prueba de generación de firma digital de documentos PDF con Adobe Acrobat Reader XI: conforme  
 La longitud del PIN permite 4 caracteres como mínimo y 16 como máximo, caracteres 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: 10 segundos  
 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