NOTA TÉCNICA Nº 16

Fecha: 14/08/2023

Fecha puesta a disposición para el Ambiente de Test	*25 de Agosto del 2023*
Fecha puesta a disposición para el Ambiente de Producción	*22 de Septiembre del 2023*

Referencia: Correcciones y ajustes sobre el MT versión 150 sobre mejoras y adecuaciones necesarias relacionadas con la nueva Ley de servicios de confianza

1. FORMATO

1.1. Se modifican los siguientes campos y observaciones:

Sección 7.6. Estándar de firma digital

Schema XML 1: xmldsig-core-schema- v150.xsd (Estándar de la Firma Digital)

ID	Campo	Descripción	Nodo Padre	Ocurrencia	Observaciones
XS02	SignedInfo	G	XS01	1-1	Grupo de información de la firma
XS03	CanonicalizationMethod	G	XS02	1-1	Grupo del método de canonicalización
XS04	Algorithm	A	XS03	1-1	Atributo Algorithm de CanonicalizationMethod Atributos válidos: http://www.w3.org/TR/2001/REC-xml-c14n-20010315 (Inclusiva) http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments (Inclusiva con comentarios) http://www.w3.org/2001/10/xml-exc-c14n (Exclusiva) http://www.w3.org/2001/10/xml-exc-c14n#WithComments (Exclusiva con comentarios)
XS05	SignatureMethod	G	XS02	1-1	Tag del método de firma
XS06	Algorithm	A	XS05	1-1	Atributo Algorithm de SignatureMethod Atributos válidos: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (RSA-SHA-256)

					http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 (RSA-SHA-384) http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 (RSA-SHA-512)
XS07	Reference	G	XS02	1-1	Grupo de referencia de la firma
XS08	URI	A	XS07	1-1	Atributo URI del tag Reference que identifica el grupo de campos que están firmados
XS10	Transforms	G	XS07	1-1	Grupo de algoritmos de transformación
XS12	Transform	G	XS10	1-1	Tag del algoritmo de transformación
XS13	Algorithm	A	XS12	1-1	Atributo Algorithm del tag Transform Atributo válido: http://www.w3.org/2000/09/xmldsig#enveloped-signature (Enveloped Signature)
XS15	DigestMethod	G	XS07	1-1	Grupo del DigestMethod
XS16	Algortihm	A	XS15	1-1	Atributo Algorithm del tag DigestMethod Atributos válidos: http://www.w3.org/2001/04/xmlenc#sha256 (SHA-256) http://www.w3.org/2001/04/xmldsig-more#sha384 (SHA-384) http://www.w3.org/2001/04/xmlenc#sha512 (SHA-512)
XS17	DigestValue	E	XS07	1	Digest Value (Valor retornado por el algoritmo definido en XS16)
XS18	SignatureValue	E	XS01	1-1	Signature Value (Valor de la firma retornado por el algoritmo definido en XS06)
XS19	KeyInfo	G	XS01	1-1	Grupo del KeyInfo (Información de la clave)
XS20	X509Data	G	XS19	1-1	Grupo X509Data
XS21	X509Certificate	E	XS20	1-1	Certificado Cualificado de Firma Electrónica X509.v3

Páginas: 38.

1.2. Se eliminan los siguientes campos de la misma tabla

ID	Campo	Descripción	Nodo Padre	Ocurrencia	Observaciones
XS14	XPath	E	XS12	0-n	XPath

1.3 Se modifican las siguientes observaciones

Sección 12.2.4 Validación de certificado de firma

ID	Resultado de validación	C;odigo	Observación	E
AC01	Certificado inválido	0120	No existe el certificado de firma en el mensaje	R
			No se aceptan certificados del PSC	
			KeyUsage no define **firma digita**l y no **Repudio**	
			Cadena de certificación inválida	

Páginas: 152.

Sección 12.2.5 Validación de la firma digital

ID	Resultado de validación	Código	Observación	E
AD01	Firma difiere del estándar [Detalle del error]	0140	No fue firmado el documento completo (falta Reference URI en la firma)	R
			Transform Algorithm previsto en la firma (Enveloped Signature) no informado o no válido	
			Canonicalization Method previsto en la firma no informádo o no válido	
			Signature Method previsto en la firma no informádo o no válido	
			Digest Method previsto en la firma no informádo o no válido	
			Reference URI no coincide con el atributo Id del documento	
AD02	Valor de la firma (SignatureValue) diferente del calculado por el PKI [Detalle del error]	0141	XML modificado luego de la firma o mal firmado	R
			Certificado del PCSC no habilitado por el MIC	
			Certificado del PCSC revocado	
			Certificado no está firmado por el PCSC	
			Dirección de la LCR no informada (CRLDistributionPoint)	
			Error en el acceso a la LCR	
			LCR inexistente	
			Certificado de firma revocado	
			Certificado raíz no corresponde al MIC	

Páginas: 153.

Sección 12.4. Validaciones del formato

Subsección I. Información de la Firma Digital del DTE (I001-I049)

Nro. Val	ID	Mensaje de validación	Código	Observación	E
278	I002	Certificado digital no vigente al momento de firma del DE [Detalle del error]	2450	El certificado digital (I002) debe estar vigente(no revocado) al momento de la firma digital (A004)	R
				Certificado del PCSC no habilitado por el MIC	
				Certificado del PCSC revocado	
				Certificado no está firmado por el PCSC	
				Dirección de la LCR no informada (CRLDistributionPoint)	
				Error en el acceso a la LCR	
				LCR inexistente	
				Certificado de firma revocado	
				Certificado raíz no corresponde al MIC	
				Certificado expirado	

Páginas: 152.

PCSC : Prestadores Cualificados de Servicios de Confianza. Según Art 4. Definiciones #38 de la Ley 6822

1.4 Se modifica la siguiente

Sección 12.2.1 Validaciones del certificado de transmisión. Protocolo TLS

Retorna un html con el mensaje de error de Acceso Denegado por las políticas de acceso. Estas validaciones se realizan durante la conexion con el servicio y son propias del protocolo TLS.

La siguiente tabla muestra las posibles causas

Inconveniente	Observación
Certificado de Transmisor Inválido	Certificado de Transmisor inexistente en el mensaje
	Versión incorrecta
	No se aceptan certificados de la AC
	ExtendKeyUsage no define “ClientAuth“
Plazo de validez del Certificado cualificado de firma electrónica	
Cadena de Certificación	Certificado del emisor no corresponde a un PCSC habilitado en el país

	Certificado del PCSC revocado
	Certificado no firmado por el PCSC emisor del Certificado
LCR del Certificado Transmisor	No existe la dirección de la LCR (CRL DistributionPoint)
	LCR indisponible
	LCR invalida
Certificado del transmisor revocado	
Certificado Raíz no pertenece al MIC	
No existe la extensión del RUC del emisor en el certificado	Si el Certificado es de persona jurídica, el RUC debe estar informado en el campo SerialNumber en caso de ser del tipo de Persona Física el RUC, estará informado en el campo: SubjectAlternativeName
Inconveniente temporal del SIFEN	

Páginas: 150.

Histórico del Documento

AUTOR	FECHA DE ELABORACIÓN	REVISOR	FECHA DE REVISIÓN	PRINCIPALES ALTERACIONES
Norma Rojas	05/06/2023	DTICs	08/08/2023	Elaboración del documento