

Recomendaciones Facturae

Formato factura

Estándares de referencia:

- W3C-- Extensible Markup Language (XML) 1.0 (Second Edition)

Recomendaciones:

- Esquema Facturae versión 3.2 (<http://www.facturae.es/>)

Firma electrónica

Estándares de referencia:

- W3C-- XMLDSig RFC 3275. <http://www.w3.org/TTR/xmlldsig-core/>.
- ETSI – XADES V.1.2.2 y V.1.3.2. ETSI TS 101 903.
- RFC2459: Internet X.509 Public Infrastructure Certificate and CRL Profile.

Recomendaciones:

- Formato de firma:
 - XMLDSig ENVELOPED.con extensiones XADES-EPES
- Algoritmo de canonicalización:
 - C14N (<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>)
- Algoritmo de firma:
 - RSA sobre SHA1 (<http://www.w3.org/2000/09/xmlldsig#rsa-sha1>)
- Transformaciones:
 - ENVELOPED-SIGNATURE (<http://www.w3.org/2000/09/xmlldsig#enveloped-signature>)
 - C14N con comentarios (<http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>)
- Algoritmo de digest SHA1:
 - (<http://www.w3.org/2000/09/xmlldsig#sha1>)



- Identificación del firmante:
 - Certificado del firmante incluido en la etiqueta
//KeyInfo/X509Data/X509Certificate
 - Formato certificado: X.509

- Extensiones XADES:
 - Versiones XADES 1.3.2 (recomendado) y 1.2.2
 - Fecha y hora de la firma en la etiqueta
//SignedProperties/SignedSignatureProperties/SigningTime
 - Digest del certificado firmante en la etiqueta
//SignedSignatureProperties/SigningCertificate/Cert/CertDigest
 - Campo *emisor* del certificado firmante en la etiqueta
//SigningCertificate/Cert/IssuerSerial/X509IssuerName
 - Número de serie del certificado firmante en la etiqueta
//SigningCertificate/Cert/IssuerSerial/X509SerialNumber
 - Referencia a la URI del documento de política de seguridad en la etiqueta
//SignaturePolicyIdentifier/SignaturePolicyId/SigPolicyId/Identifier
 - Digest del documento de política de seguridad en la etiqueta
//SignaturePolicyIdentifier/SignaturePolicyId/SigPolicyHash/DigestValue
 - Oid de la política de seguridad en la etiqueta
//SignaturePolicyId/SigPolicyQualifiers/SigPolicyQualifier/SPURI
 - Rol del firmante de la factura (emisor / receptor / tercero) en la etiqueta
//SignerRole/ClaimedRoles/ClaimedRole

Envío a través de Web Services

Estándares de referencia:

- W3C-- Simple Object Access Protocol (SOAP) 1.1.
- W3C--Web Service Description Language (WSDL) 1.1.
- RFC2616: Hypertext Transfer Protocol – HTTP/1.1.
- The SSL Protocol Version 3.0.
- RFC2246: The TLS Protocol Version 1.0.