Spécifications techniques de la signature électronique pour la plateforme el fatoora

Table des matières

Table des figures

1-Version et mise à jour

Version	Date	Remarque
1.0	21/06/2018	Version initiale

2- Avant-propos

Le lecteur de ce document doit impérativement lire la politique de signature avant de se focaliser sur l'aspect technique : Politique de signature

Le format de la facture électronique doit appliquer la norme TEIF (Voir spécification).

Une seule signature électronique d'un fournisseur est autorisée par la plateforme el fatoora.

L'implémentation de la signature est basée sur la librairie DSS (Digital Signature Services) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS+v5.2 .

3-Introduction

La solution de signature doit répondre aux besoins d'assurer

- L'authentification,
- L'intégrité
- La non-répudiation,
- La simplification des procédures de signature,
- Ajout de la confiance dans les transactions.

Ce document présente les spécifications fonctionnelles et techniques exigées pour le service facture électronique en tant que fournisseur.

4-Specifications

4.1-Specifications fonctionnelles

La signature devra être à l'épreuve des attaques, c'est-à-dire qu'un message signé, ne peut pas être modifié ou altéré sans être détecté.

Toute personne possédant un certificat délivré par l'Agence Nationale de Certification Electronique peut utiliser la solution dans son environnement d'intégration.

4.2-Specifications techniques

La signature électronique d'une facture par un fournisseur est enveloppée (signature est insérée dans le document) en appliquant la norme XADES -B (Basic).

L'algorithme de cryptage utilisé dans la signature est l'algorithme RSA-SHA256.

Avant de signer un message ou de vérifier une signature, le certificat du signataire doit être vérifié pour s'assurer de sa validité. La vérification de la révocation se fait en mode d'accès OCSP ou CRL.

4.3-Description d'un scénario d'échange

Pour signer une facture électronique, l'émetteur doit disposer une paire de clés (publique et privé) qui se trouve dans le certificat fourni par l'ANCE (Agence Nationale de Certification Electronique).

Pour la lecture du certificat électronique, l'émetteur peut utiliser le magasin du certificat de Windows ou bien utiliser le module PKCS délivré avec le Token ou bien un serveur HSM.

La signature sera intégrée dans la facture à signer contenant les empreintes du message, le certificat du signataire et des informations supplémentaires.

A la réception d'un message signé dans la plateforme el fatoora, toutes les empreintes reçues seront vérifiées. Les certificats de la chaine de confiance et le certificat fournisseur doivent être valide et non révoqué.

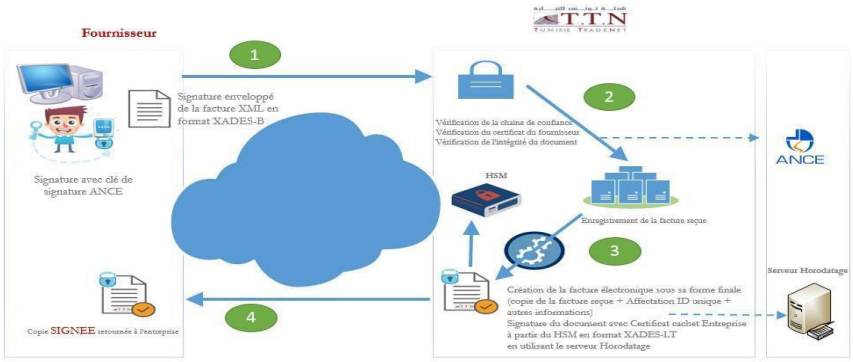

Figure 1. Schématisation de la solution

5-Description du format de fichier de la signature

La signature électronique doit respecter la norme XAdES-B (ETSI EN 319 132-1) maintenu et mises à jour par le World Wide Web Consortium **(W3C)** et Européen Télécommunications Standards Institute **(ETSI)** (http://uri.etsi.org/01903/v1.3.2#).

Ci-dessous la figure de la structure XML de la signature

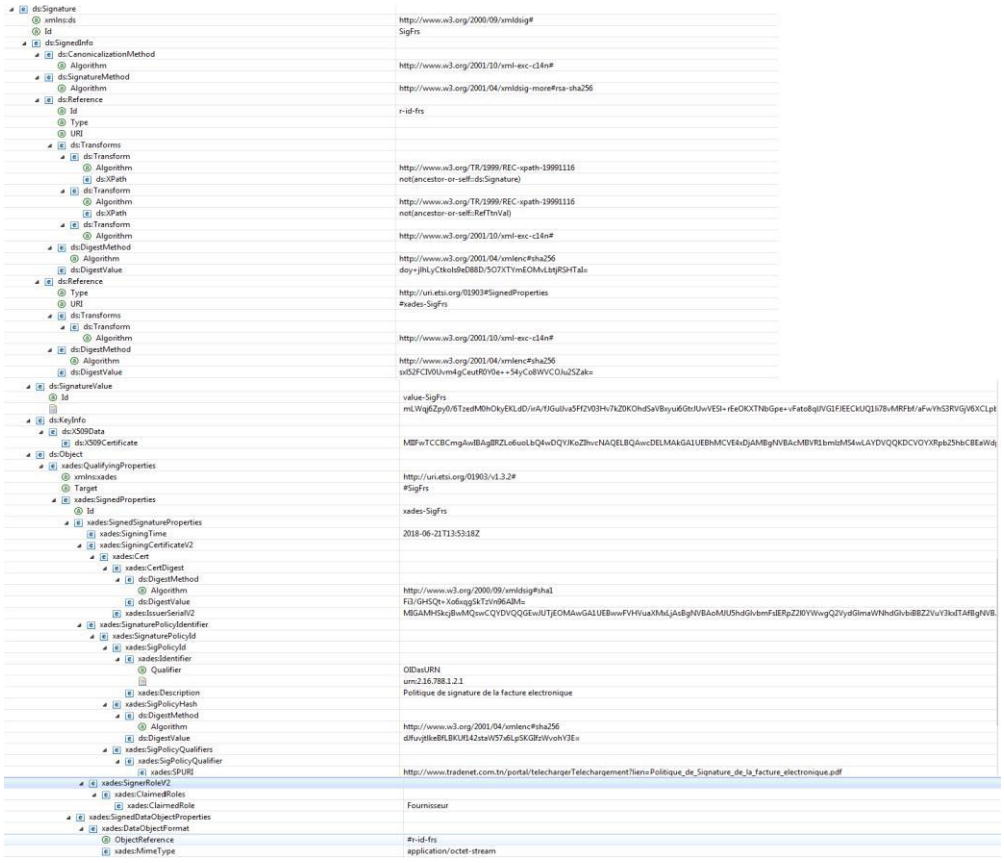

Figure 2. Structure globale de la signature XADES-B

5.1-Bloc <ds :Signature>

L'id du bloc signature **<ds :Signature>** doit contenir la valeur « SigFrs».

Figure 3. Bloc signature avec id SigFrs

5.2-Bloc <ds:SignedInfo>

Le bloc **<ds :SignedInfo>** : contient les références et les hachages des éléments signés.

Figure 4. Bloc SignedInfo

5.2.1 -Bloc <ds:CanonicalizationMethod>

Le bloc **<ds:CanonicalizationMethod >** : contient l'algorithme de canonicalisation de l'XML => La méthode exclusive de canonisation XML est utilisée (http://www.w3.org/2001/10/xml-exc-c14n#).

Figure 5. Bloc CanonicalizationMethod

5.2.2 -Bloc <ds:SignatureMethod>

Le bloc **<ds: SignatureMethod>** : contient l'algorithme de hachage pour la signature des éléments du bloc **<ds :SignedInfo>** => L'algorithme utilisé est RSA-SH256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256).

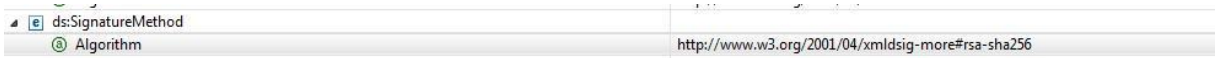

Figure 6. Bloc SignatureMethod

5.2.3 -Bloc <ds:Reference> avec id « r-id-frs»

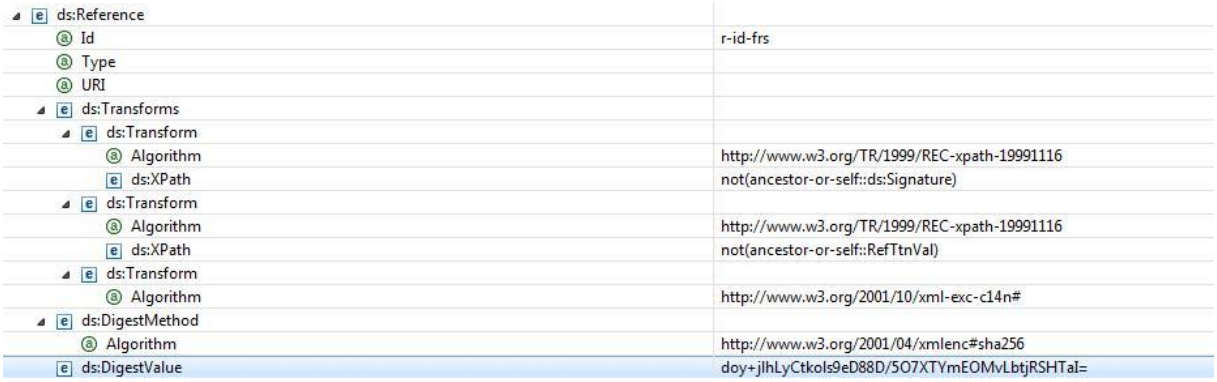

Figure 7. Bloc Reference avec id "r-id-frs"

Le bloc **< ds:Reference>** avec id « r-id-frs» contient principalement :

- Trois transformations sont appliquées avant la signature d'un message :

1- Le 1er bloc **<ds:Transform>** : Transformation XPath sur le bloc **<ds :Signature>** (le bloc est non signé).

Figure 8. 1er bloc <ds:Transform>

2- Le 2 -ème bloc **<ds:Transform>** : Transformation XPath sur le bloc **<ds :RefTtnVal>** (le bloc est non signé).

Figure 9. 2 -ème bloc <ds:Transform>

3- Le 3 -ème bloc **< ds:Transform>** : contient l'algorithme de canonicalisation de l'XML => La méthode exclusive de canonisation XML est utilisée (http://www.w3.org/2001/10/xml-exc-c14n#).

Figure 10. 3 -ème bloc < ds:Transform>

- Le bloc **< ds:DigestMethod> :** contient l'algorithme de hachage utilisé => L'algorithme utilisé est SH256 (http://www.w3.org/2001/04/xmlenc#sha256).

Figure 11. Bloc < ds:DigestMethod>

- Le bloc **< ds:DigestValue> :** contient la valeur de hachage du contenue de la facture en base64.

Figure 12. Bloc < ds:DigestValue>

5.2.4 -Bloc <ds:Reference> avec uri « #xades-SigFrs »

Figure 13. Bloc <ds:Reference> avec uri « #xades-SigFrs »

Le bloc **< ds:Reference>** avec uri « #xades-SigFrs » qui fait référence au bloc **<xades:SignedProperties Id="xades-SigFrs">** contient principalement :

- Le bloc **< ds:Transform>** : contient l'algorithme de canonicalisation de l'XML => La méthode exclusive de canonisation XML est utilisé (http://www.w3.org/2001/10/xml-exc-c14n#).

Figure 14. Bloc < ds:Transform>

- Le bloc **< ds:DigestValue> :** contient la valeur de hachage de l'élément <xades:SignedProperties Id="xades-SigFrs"> encodé en base64.

Figure 15. Bloc < ds:DigestValue>

5.3 -Bloc <ds:SignatureValue>

Le bloc **<ds:SignatureValue>:** contient la signature numérique calculée de l'élément<ds:SignedInfo> encodé en base 64..

Figure 16. Bloc <ds:SignatureValue>

5.4 -Bloc <ds:KeyInfo>

Le bloc **< ds:KeyInfo >:** contient la valeur du certificat signataire dans l'élément **<ds:X509Certificate>** encodé en base 64. Le bloc peut contenir aussi la liste des certificats de la chaine de confiance.

Figure 17. Bloc <ds:KeyInfo>

5.5 -Bloc <ds:Object>

Le bloc **< ds:Object >:** contient des éléments dont les propriétés qualifient à la fois la signature et l'objet de données signé.

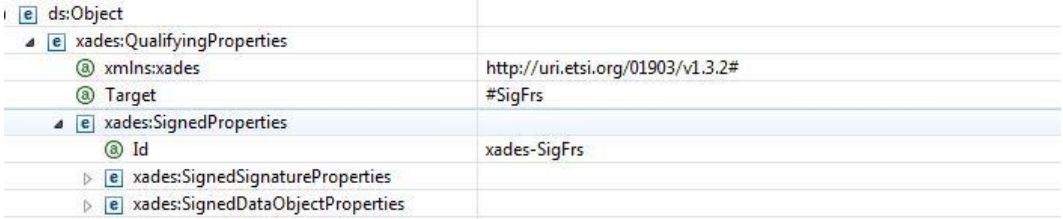

Figure 18. Bloc < ds:Object >

Le bloc **<xades:QualifyingProperties>** : contient les propriétés qualifiées d'une signature.

5.5.1 -Bloc <xades:SignedSignatureProperties>

Le bloc **<xades:SignedSignatureProperties>** : contient les propriétés signées de la signature :

Figure 19. Bloc <xades:SignedSignatureProperties>

- Le bloc **<xades :SigningTime>** : C'est la date et l'heure de la signature.

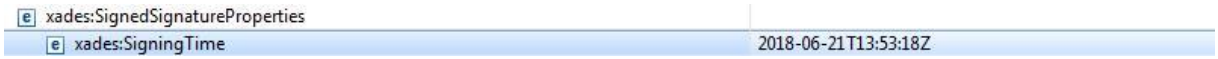

Figure 20. Bloc <xades :SigningTime>

- Le bloc **<xades:SigningCertificateV2>** : Contient deux éléments :

Figure 21. Bloc <xades:SigningCertificateV2>

- Le bloc **<xades:CertDigest>:** Contient le hachage du certificat signataire en format binaire encodé en base 64.

Figure 22. Bloc <xades:CertDigest>:

- Le bloc < **xades:IssuerSerialV2> :** Contient des informations de l'émetteur du certificat en format binaire encodé en base 64**.**

Figure 23. Bloc <xades:IssuerSerialV2 >

➢ Le bloc <**xades :ClaimedRole>** : Contient le rôle du signataire au sein de l'entreprise.

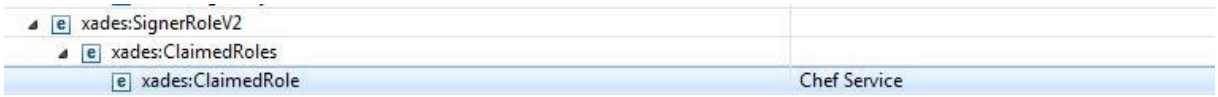

Figure 24. Bloc <xades :ClaimedRole>

➢ Le bloc <**xades:SignaturePolicyIdentifier>** : Contient la politique de signature comportant :

- Le bloc <**xades:SigPolicyId> :** Contient l'OID qui est obligatoire après prise de connaissance de la politique de signature : [Politique de signature]

Figure 25. Bloc <xades:SigPolicyId>

- Le bloc **<xades : SigPolicyHash> :** contient l'identifiant de l'algorithme de hachage et la valeur de hachage de la politique de signature encodé en base 64.

Figure 26. Bloc <xades : SigPolicyHash>

- Le bloc **<xades:SPURI>** : Url du document de la politique de signature.

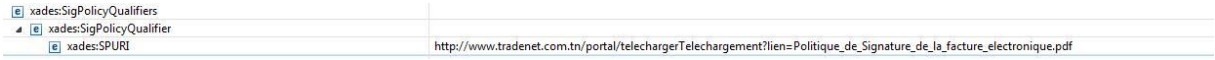

Figure 27. Bloc <xades:SPURI>

➢ Le bloc **<xades: SignedDataObjectProperties>** : contient toutes les propriétés signées qui qualifient individuellement chaque objet de données signé.

Figure 28. Bloc <xades: SignedDataObjectProperties>

7-Exemple complet du bloc <ds :Signature>:

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Id="SigFrs"> <ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference Id="r-id-frs" Type="" URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116"> <ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116"> <ds:XPath>not(ancestor-or-self::RefTtnVal)</ds:XPath>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/> </ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>doy+jlhLyCtkols9eD88D/5O7XTYmEOMvLbtjRSHTaI=</ds:DigestValue>
</ds:Reference>
<ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-
SigFrs"> <ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/> </ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>sxl52FCIV0Uvm4gCeutR0Y0e++54yCo8WVCOJu2SZak=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue Id="value-SigFrs">
mLWqj6Zpy0/6TzedM0hOkyEKLdD/irA/fJGulJva5Ff2V03Hv7kZ0KOhdSaVBxyui6GtrJUwVESl+rEeOKXTNbGpe+vFato8qlJVG1FJEECkUQ1li7
8vMRFbf/aFwYhS3RVGjV6XCLpbUoUmX8+KU4DBRBalZph3Z+AuC65J2A2XoYc0UfX+FwQCw1yx8MF3KR9IBiXeOY9E9tNS8LI/aoAE/9GDeh
wCWWRXz18J9/4maueGtxeB2xoTRq1qp2FLxcgiZtBmauics0ijvoQNr2UmwfmRjYprw/pmNeunroFMyLU/4t8QNrPAkMVI6A5+2kcoOCYfgQ
MNP4mqIzdszg==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIFwTCCBCmgAwIBAgIIRZLo6uoLbQ4wDQYJKoZIhvcNAQELBQAwcDELMAkGA1UEBhMCVE4xDjAMBgNVBAcMBVR1bmlzMS4wLAYDVQ
QKDCVOYXRpb25hbCBEaWdpdGFsIENlcnRpZmljYXRpb24gQWdlbmN5MSEwHwYDVQQDDBhUblRydXN0IFF1YWxpZmllZCBHb3YgQ0EwH
hcNMTcxMDE4MTQzMDQ4WhcNMTkxMDE4MTQzMDQ4WjBkMQswCQYDVQQGEwJUTjEZMBcGA1UECgwQVFVOSVNJRSBUUkFERU5FV
DEQMA4GA1UEBAwHQk9VWklESTEPMA0GA1UEKgwGSEFCSUJBMRcwFQYDVQQDDA5IQUJJQkEgQk9VWklESTCCASIwDQYJKoZIhvcNAQ
EBBQADggEPADCCAQoCggEBAMV7EUmFMqHZm+iB1iOXKBbKu0C41X/IqyxalRyX+9sVDmFekXepGcjnsIST5ZQcq+vhl/HUW7aevub15wm6
6QAwLF35X55w305yZNK3Vx1EmCF040/22UyXKxJRxXKWmYYfZzli6UKk0mFiRKULvFt/2pYehF1q121uvvb+/9Wk1sDt2Vrp67MYvMowoKS
s/reDs83rvARGk+H3ydAs9++FINvIott0gryYyLtPxOZ75Ur4Gk15PePZTGDnzzGCgZM8VhZo8zeN+6FgK8QNlyEYfD7bbeKVu4wMl1xZfld4My
MGOtsw16KUqi23cpQ+BjnTNR4fxRUIpEGjqkgliPMCAwEAAaOCAekwggHlMDYGCCsGAQUFBwEBBCowKDAmBggrBgEFBQcwAYYaaHR0cD
ovL3ZhLmNlcnRpZmljYXRpb24udG4wHQYDVR0OBBYEFP3zo4J4TSsNDURUM7plRXGyiGkbMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAUcyQoJfoi9pKpFYOkLLPNxsu0A1YwLAYDVR0gBCUwIzAJBgcEAIvsQAECMAwGCmCGFAECBgEKAQEwCAYGBACPegECMEYGA1UdHwQ/
MD0wO6A5oDeGNWh0dHA6Ly9jcmwuY2VydGlmaWNhdGlvbi50bi90bnRydXN0cXVhbGlmaWVkZ292Y2EuY3JsMA4GA1UdDwEB/wQEA
wIGwDApBgNVHSUEIjAgBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQBgjcUAgIwKQYDVR0RBCIwIIEeaGFiaWJhLmJvdXppZGlAdHJhZGV
uZXQuY29tLnRuMIGABggrBgEFBQcBAwR0MHIwCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGATBHBgYEAI5GA
QUwPTA7FjVodHRwOi8vd3d3LmNlcnRpZmljYXRpb24udG4vcHViL3Bkcy10dW50cnVzdGdvdmNhLnBkZhMCZW4wDQYJKoZIhvcNAQELBQ
ADggGBALcTGocPDIp7DBQ6pGFNVhw9a1F0U3agYngyPRGkXf8lSHqxA8oZw8vrxEIkTpDG/EKVhmf2VOA/aKaKlSyaBIzKiEvLKncrQRbTJ71S
XnC1DW5Szr94EQRSzXbtQwGtB5ENWWliGcDVOaUN8rnZO00orkDJMZy7t9vMFi3ZosKNybCSNceemySBKZiSqUXqzB1+bYEPRQHV2rXoLXj
PIzUdgY1UnmQZ2R2t0itxaDNPcQVIb4zgQwWfLwAhkJyuG9bT+l4pXH+V0Fy5ti3GrVs0b7xF4VfQP3tj9LxIhAJ2eVeSUAA7tEWMCVbwp6Ob
2E9F3hQPVQHj6BGc6HyWsA8k/ON60ZjnE0kaddnMRp8P5E+Ruj9VhFgSmAK6WbxuUclFEZGzDGoDbxiF7M/W7wNaXouazGe65KdJ45YnFp
sQvvj2Zi7RusFLNQ0aCH8YWsUH1NK4CfyPwn+hnMhaWO1ipCKJJEEhKrB7UjymFO6DobULnPw/qKQcEMJDx1wZ3A==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
<ds:Object>
<xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#SigFrs">
<xades:SignedProperties Id="xades-SigFrs">
<xades:SignedSignatureProperties>
<xades:SigningTime>2018-06-21T13:53:18Z</xades:SigningTime>

<xades:SigningCertificateV2>
<xades:Cert>
<xades:CertDigest>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Fi3/GHSQt+Xo6xqgSkTzVn96AIM=</ds:DigestValue>
</xades:CertDigest>
<xades:IssuerSerialV2>
MIGAMHSkcjBwMQswCQYDVQQGEwJUTjEOMAwGA1UEBwwFVHVuaXMxLjAsBgNVBAoMJU5hdGlvbmFsIERpZ2l0YWwgQ2VydGlmaWN
hdGlvbiBBZ2VuY3kxITAfBgNVBAMMGFRuVHJ1c3QgUXVhbGlmaWVkIEdvdiBDQQIIRZLo6uoLbQ4=
</xades:IssuerSerialV2>
</xades:Cert>
</xades:SigningCertificateV2>
<xades:SignaturePolicyIdentifier>
<xades:SignaturePolicyId>
<xades:SigPolicyId>
<xades:Identifier Qualifier="OIDasURN">urn:2.16.788.1.2.1</xades:Identifier>
<xades:Description>Politique de signature de la facture electronique</xades:Description>
</xades:SigPolicyId>
<xades:SigPolicyHash>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>dJfuvjtlkeBfLBKUf142staW57x6LpSKGlfzWvohY3E=</ds:DigestValue>
</xades:SigPolicyHash>
<xades:SigPolicyQualifiers>
<xades:SigPolicyQualifier>
<xades:SPURI>
http://www.tradenet.com.tn/portal/telechargerTelechargement?lien=Politique_de_Signature_de_la_facture_electronique.pdf
</xades:SPURI>
</xades:SigPolicyQualifier>
</xades:SigPolicyQualifiers>
</xades:SignaturePolicyId>
</xades:SignaturePolicyIdentifier>
<xades:SignerRoleV2>
<xades:ClaimedRoles>
<xades:ClaimedRole>Fournisseur</xades:ClaimedRole>
</xades:ClaimedRoles>
</xades:SignerRoleV2>
</xades:SignedSignatureProperties>
<xades:SignedDataObjectProperties>
<xades:DataObjectFormat ObjectReference="#r-id-frs">
<xades:MimeType>application/octet-stream</xades:MimeType>
</xades:DataObjectFormat>
</xades:SignedDataObjectProperties>
</xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
</ds:Signature>

8- Validation de la signature

Pour la vérification de la signature, vous pouvez utiliser l'outil en ligne de l'ETSI : Outil checker. Il faut envoyer un email à Plugtests@etsi.org avec objet : **ETSI Signature Checker** en précisant votre nom et prénom avec le nom de votre entreprise comme la figure ci-dessous.

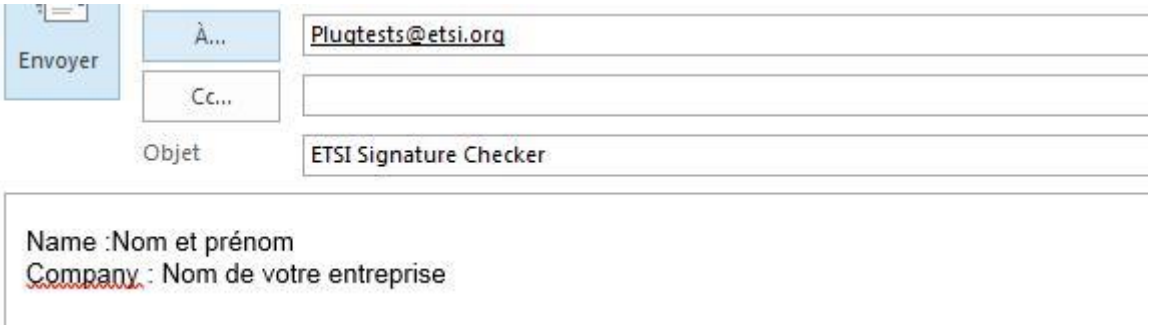

Figure 29. : ETSI Signature Checker

NB : Un email de réponse sera transmis par ETSI contenant votre login et mot de passe pour accéder à l'outil.

Pour valider la signature de votre message xml il suffit de suivre les étapes suivantes :

1. Choisir **XAdes Checker** du menu à gauche.

Figure 30. Xades Cheker

2. Choisir l'option **"ETSI EN 319 132-1 v1.1.1 Building Blocks and Baseline"**.

Figure 31.Option ETSI EN 319 132-1 v1.1.1

3. Parcourir votre message xml en utilisant le bouton « choisir fichier ».

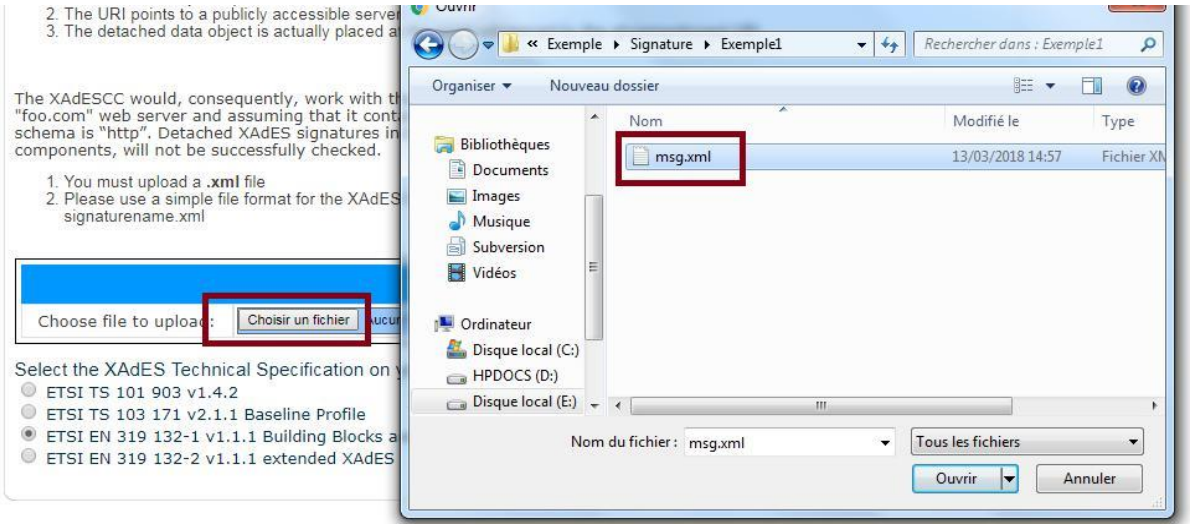

Figure 32. Ajout fichier XML

4. Cliquer sur le bouton « Upload ».

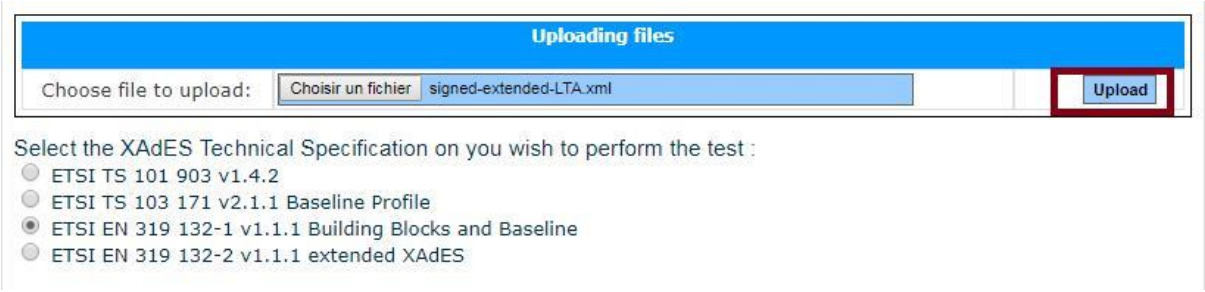

Figure 33. Clique sur le bouton "Upload"

5. Cliquer sur le lien généré comme montre la figure ci-dessous :

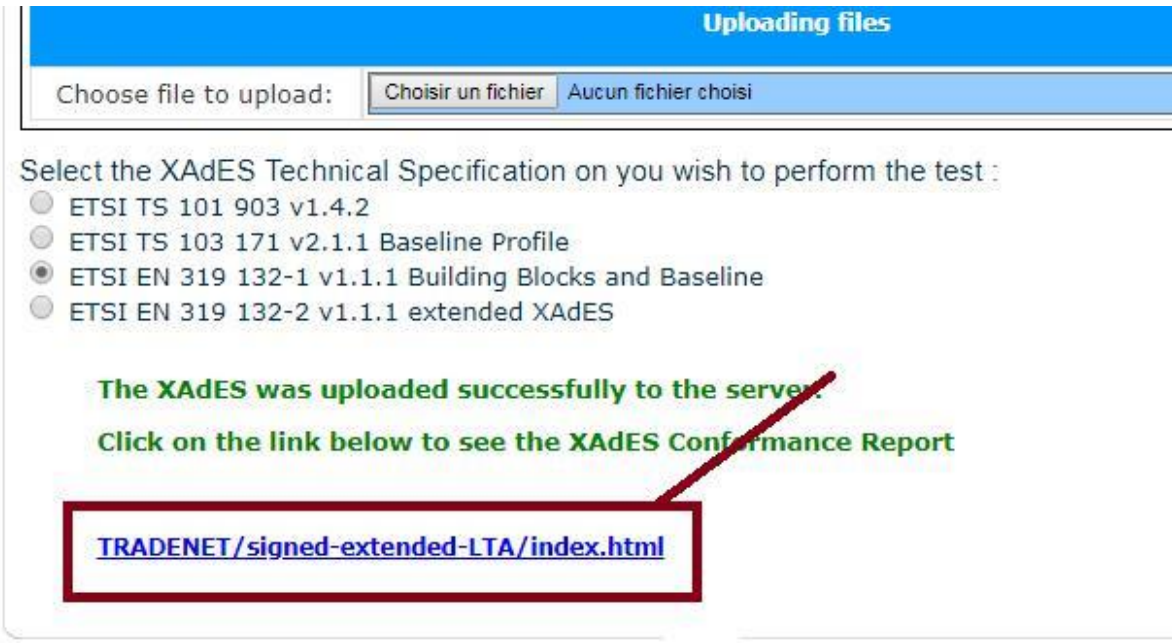

Figure 34. Clique sur le lien généré

6. Cliquer sur le lien « XAdES-signature-1 » comme montre la figure ci-dessous :

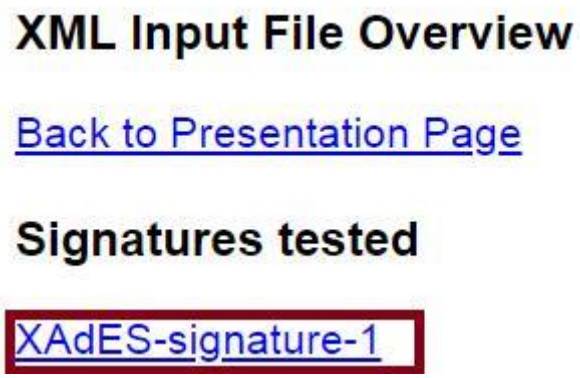

Figure 35 Clique sur"XAdES-signature-1".

7. Cliquer sur le lien « Errors and Warnings» pour voir les erreurs s'il y en a comme montre la figure ci-dessous :

Figure 36. Clique sur "Errors and Warnings"

9- Remarques

- Utilisation du jdk 1.7 update 25.

- L'encodage utilisé est UTF-8 pour l'XML.

- Eviter les caractères spéciaux.

- Il faut utiliser le format unpretty (le message XML doit être en une seule ligne) juste avant de signer le document facture électronique.