



# Plateforme Services Web ETNIC

## - Spécifications techniques

**Produit :** Plateforme Services Web ETNIC  
**Type de document :** Manuel d'utilisation  
**Révision du document :** 1.5.1  
**Date du document :** 06-02-2018

## Historique

Version	Description	Ecrit par	Date
1.0	Version initiale	Anne Nosedà Xavier Martin	22-04-2014
1.1	Ajout du mode synchrone	Xavier Martin	02-09-2014
1.2	Ajout de l'accès avec username token profile	Xavier Martin	22-04-2015
1.3	Ajout d'une section sur la configuration de SOAP-UI	Xavier Martin	26-11-2015
1.4	Section SOAP-UI étendue avec username token profile	Xavier Martin	31-03-2016
1.5	Ajout des codes d'erreur	Xavier Martin	19-07-2017
1.5.1	Correction des urls d'auto enregistrement	Xavier Martin	06-02-2018

## Objectifs du document

Ce document est destiné aux partenaires désireux d'intégrer leurs applications à celles de la Fédération Wallonie-Bruxelles en utilisant la plateforme de Services Web mise à disposition par l'ETNIC.

La plateforme est d'abord présentée de manière conceptuelle et puis définie techniquement domaine par domaine.

## Public cible

Ce document s'adresse principalement aux architectes, analystes et développeurs.

## Contacts

Pour toute question ou demande d'assistance technique veuillez contacter le helpdesk de l'ETNIC.

Support général  
Email : [support@etnic.be](mailto:support@etnic.be)  
Tél : 02 / 800 10 10



# Plateforme Services Web ETNIC

## - Spécifications techniques

### Table des matières

<b>1. PRESENTATION DE LA PLATEFORME SERVICES WEB DE L'ETNIC .....</b>	<b>3</b>
1.1. CADRE.....	3
1.2. CARACTERISTIQUES .....	3
1.3. ACCES.....	3
<b>2. COMMUNICATION.....</b>	<b>4</b>
2.1. ROUTAGE DES REQUETES.....	4
2.2. COMMUNICATION SYNCHRONE .....	4
2.2.1. <i>Architecture</i> .....	5
2.3. COMMUNICATION ASYNCHRONE .....	5
2.3.1. <i>Architecture</i> .....	5
2.3.2. <i>Service « Polling »</i> .....	6
2.3.3. <i>Exemple de messages de communication asynchrone</i> .....	6
<b>3. SECURITE .....</b>	<b>9</b>
3.1. CONNEXION SECURISEE TLS .....	9
3.2. SECURISATION DES SERVICES WEB .....	9
3.2.1. <i>UsernameToken Profile</i> .....	9
3.2.2. <i>x509Token Profile</i> .....	10
3.2.3. <i>WS-Secure Conversation Token</i> .....	10
<b>4. CONFIGURATION SOAP-UI.....</b>	<b>17</b>
4.1. UTILISATION DE SOAP-UI .....	17
4.2. INITIALISATION DU PROJET .....	17
4.3. CONFIGURATION WS-SECURITY.....	19
4.3.1. <i>Configuration x509Token Profile</i> .....	21
4.3.2. <i>Configuration usernameToken Profile</i> .....	24
4.3.3. <i>Application de WS-Security sur la requête</i> .....	26
4.4. CONFIGURATION WS-ADDRESSING .....	28



# Plateforme Services Web ETNIC

## Spécifications techniques

### 1. PRESENTATION DE LA PLATEFORME SERVICES WEB DE L'ETNIC

#### 1.1. CADRE

L'ETNIC expose des Services Web sur Internet à destination de ses partenaires informatiques désireux d'intégrer leurs applications avec les services de la Fédération Wallonie-Bruxelles.

L'ensemble des Services Web sont exposés à travers une plateforme technique répondant à diverses spécifications portant entre autre sur le protocole de communication et la sécurité.

#### 1.2. CARACTERISTIQUES

La communication se fait au choix de manière **synchrone** ou **asynchrone** à travers un canal sécurisé par **TLS**. Les Services Web dialoguent avec des messages **SOAP** en version 1.1 ou 1.2 et sont sécurisés selon la spécification **WS-Security**; l'accès se fait soit à l'aide d'un login et d'un mot de passe (UsernameToken Profile), soit en signant les messages à l'aide d'un certificat numérique (x509Token Profile). Si le certificat utilisé est celui émanant de l'eID, les spécifications **WS-SecureConversation** et **WS-Trust** sont également utilisées.

Seuls certains services web autorisent l'accès par login et mot de passe. Veuillez vous référer aux manuels respectifs de ceux-ci pour le vérifier.

Les sections suivantes de ce document décrivent en profondeur les spécifications techniques à satisfaire pour pouvoir dialoguer avec la plateforme.

#### 1.3. ACCES

Actuellement seuls des services du domaine de l'enseignement sont exposés. Pour ceux-ci, quel que soit le service adressé, le point d'accès à la plateforme est unique.

Les URLs pour les différents environnements sont les suivantes :

- Test & Qualification : <https://services-web.tq.etic.be/ecole>
- Production : <https://services-web.etic.be/ecole>

Avant de pouvoir accéder à la plateforme, vous devez dans un premier temps créer un compte Cerbère auprès de l'ETNIC. Le certificat de votre carte d'identité électronique est nécessaire pour cet enregistrement et donc un lecteur de carte. Les URLs pour s'enregistrer dans les deux environnements sont les suivantes :

- Test & Qualification : <https://www.users-acceptance.cfwb.be/IDMProv/portal/cn/GuestContainerPage/SelfRegisterID?population=EDU&eid=true&aff=WkJEVTZiVVhsUEhDL243YUQvRktWeGxnc1MremtEL20NCq>
- Production : <https://www.users.cfwb.be/IDMProv/portal/cn/GuestContainerPage/SelfRegisterID?population=EDU&eid=true&aff=Wi92ZkIvaVMvQVYrSk9TVURwWUo5Vjd2eCt6Q3IHafkNCq>



## Plateforme Services Web ETNIC

### -

## Spécifications techniques

Vous devrez alors fournir le certificat que vous utiliserez pour vous connecter aux Services Web de l'ETNIC. Vous pouvez utiliser le certificat de votre carte d'identité (l'enregistrement se fait alors via les écrans) ou bien un certificat acquis auprès d'un organisme de certification reconnu tel que GlobalSign ou Certipost. Dans ce dernier cas, vous devrez le communiquer par une autre voie à définir avec l'ETNIC.

Une fois le compte créé pour la production, vous recevrez automatiquement un email pour confirmer la création. Tandis que pour « Test & Qualification », vous devrez prendre contact directement avec l'ETNIC pour valider la création.

## 2. COMMUNICATION

### 2.1. ROUTAGE DES REQUETES

Comme l'URL d'accès est unique, quel que soit le service qui est appelé, la spécification **WS-Addressing** doit être utilisée pour adresser correctement le service demandé.

Il s'agit de remplir différentes informations dans la partie « Header » de l'enveloppe SOAP :

- Un champ **wsa:To** qui permet d'indiquer le service cible que l'on désire appeler
- Un champ **wsa:Action** qui définit la fonctionnalité que l'on désire appeler ainsi que le mode de communication à utiliser (synchrone ou asynchrone). L'ETNIC a adopté le standard suivant pour définir les actions:

```
domaine:fonctionnalité?mode=sync/async
```

Par exemple, pour le service « SIEL – Inscription », le domaine est « SIEL », la fonctionnalité « inscription » et le mode de communication est asynchrone. L'action pour l'adresser sera donc :

```
siel:inscription?mode=async
```

Les valeurs pour les champs **wsa:To** et **wsa:Action** à utiliser sont décrites dans les manuels d'utilisation spécifiques aux différents services, disponibles dans le catalogue de services SOA sur le site Internet de l'ETNIC.

- un champ **wsa:From** qui permet d'indiquer l'identité du demandeur afin de faire de l'audit, du traçage et des statistiques
- un champ **wsa:MessageID** qui permet de faire du traçage de message et de reconstituer un flux de messages (Attention dans le cas de la requête, il ne contient pas l'ID de corrélation décrit précédemment).

### 2.2. COMMUNICATION SYNCHRONE

### 2.2.1. Architecture

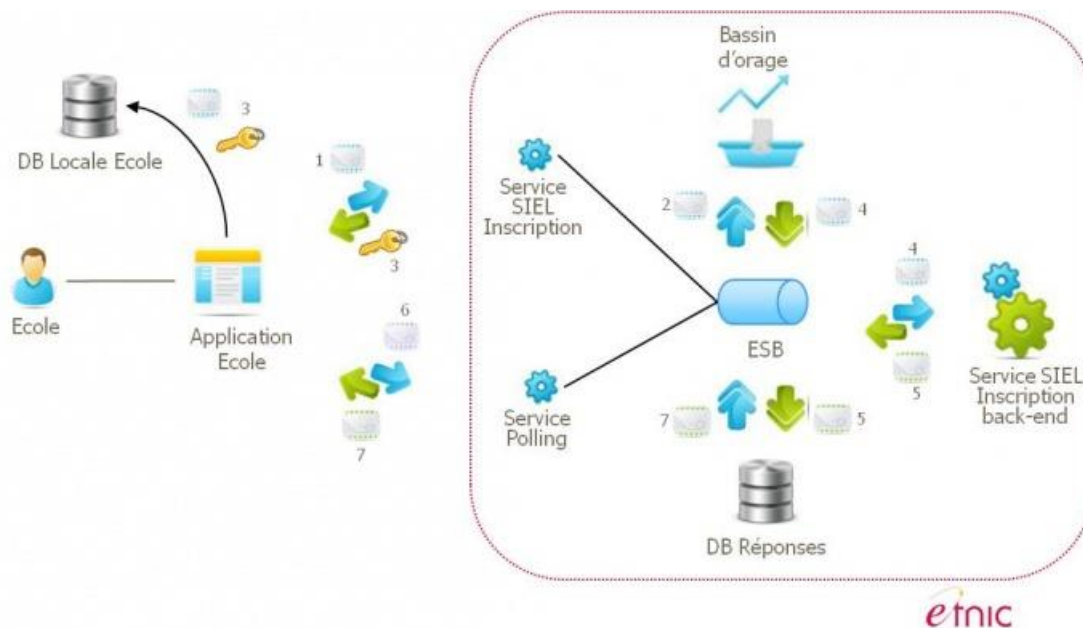
Dans le cas d'une communication synchrone, les réponses aux requêtes envoyées par le client sont directement renvoyées à ce dernier.

## 2.3. COMMUNICATION ASYNCHRONE

### 2.3.1. Architecture

Dans le cas d'une communication asynchrone, les réponses aux requêtes envoyées par le client sont récupérées de manière différées sur un service « Polling ». Ce dernier fournit les réponses dans l'ordre des requêtes reçues.

Ci-dessous est illustrée l'architecture globale de la plateforme en prenant comme exemple le service « SIEL – Inscription ». Le cheminement des messages y est décrit.



1. Le client envoie une requête fonctionnelle
2. L'ETNIC stocke sa demande pour traitement ultérieur
3. L'ETNIC lui renvoie un ID de corrélation disponible à 2 endroits dans le message SOAP de retour. L'application cliente doit stocker cet ID :
  - o /soap:Envelope/soap:Body/ow:StatutMsg/ow:message/ow:ID
  - o /soap:Envelope/soap:Header/wsa:MessageID
4. Lorsque le back-end du service SIEL est disponible, il traite la demande
5. La réponse est stockée dans une DB côté ETNIC
6. Le client envoie une requête de polling au service dédié



## Plateforme Services Web ETNIC

### Spécifications techniques

7. L'ETNIC lui renvoie une réponse fonctionnelle (ou une SOAP Fault) avec l'ID de corrélation disponible à 2 endroits dans le message :
- /soap:Envelope/soap:Body/poll:pollingReponse/poll:message/poll:ID
  - /soap:Envelope/soap:Header/wsa:RelatesTo

Le service « Polling » renvoie toujours la réponse la plus ancienne qui n'a pas encore été récupérée à destination du demandeur.

### 2.3.2. Service « Polling »

Le service « Polling » permet de récupérer les réponses fonctionnelles aux requêtes de manière différée. Pour l'invoquer, les valeurs spécifiques des champs WS-Addressing sont les suivantes :

- **wsa:To** : `http://www.etnic.be/janus/polling`
- **wsa:Action** : `janus:polling?mode=sync`

L'unique opération est `getMessage` et ne prend pas d'argument. La réponse renvoyée correspond à la plus vieille requête de l'appelant pour laquelle la réponse n'avait pas encore été récupérée, à l'instar d'une file FIFO (*first in first out*). La réponse contient le champ l'ID de corrélation par rapport à sa requête dans le champ **wsa:RelatesTo** présent dans l'entête du message. L'application appelante doit donc faire correspondre cet ID avec les IDs qu'elle a stockés de son côté pour faire correspondre la réponse avec la bonne requête (voir schéma d'architecture au point 2.1).

Le contrat WSDL du service « Polling » se trouve en téléchargement sur la page dédiée du service dans le catalogue de services SOA de l'ETNIC.

### 2.3.3. Exemple de messages de communication asynchrone

Les en-têtes relatifs à la sécurité ont été omis de l'exemple pour des raisons de lisibilité.

#### Requête fonctionnelle :

```
<soapenv:Envelope xmlns:siel="http://www.etnic.be/janus/siel"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsa:Action>janus:dedale?mode=async</wsa:Action>
    <wsa:From>
      <wsa:Address>http://etnic.be/soapui</wsa:Address>
    </wsa:From>
    <wsa:MessageID>uuid:3164ab7f-bf5a-423b-95ba-f4e5ebddd6b0</wsa:MessageID>
    <wsa:To>http://www.etnic.be/janus/dedale</wsa:To>
  </soapenv:Header>
  <soapenv:Body>
    <ded:DedaleRequest>
      <ded:Adresse>
        <ded:Rue>reuchamp</ded:Rue>
        <ded:Numero/>
        <ded:BtePostale/>
        <ded:CodePostal>1340</ded:CodePostal>
        <ded:Localite/>
      </ded:Adresse>
    </ded:DedaleRequest>
  </soapenv:Body>
</soapenv:Envelope>
```



## Plateforme Services Web ETNIC - Spécifications techniques

```
</ded:Adresse>  
</ded:DedaleRequest>  
</soapenv:Body>  
</soapenv:Envelope>
```

### Réponse contenant l'ID de corrélation:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">  
  <soapenv:Header>  
    <wsa:To>http://etnic.be/soapui</wsa:To>  
    <wsa:MessageID>00000145279160df-246</wsa:MessageID>  
    <wsa:RelatesTo>uuid:3164ab7f-bf5a-423b-95ba-f4e5ebddd6b0</wsa:RelatesTo>  
    <wsa:From >  
      <wsa:Address>http://www.etnic.be/janus/dedale</wsa:Address>  
    </wsa:From>  
    <wsa:Action soapenv:mustUnderstand="1">janus:dedale?mode=async</wsa:Action>  
  </soapenv:Header>  
  <soapenv:Body>  
    <StatutMsg xmlns="http://www.etnic.be/janus/ow">  
      <message>  
        <ID>00000145279160df-246</ID>  
      </message>  
    </StatutMsg>  
  </soapenv:Body>  
</soapenv:Envelope>
```

### Requête de polling :

```
<soapenv:Envelope xmlns:fase="http://www.etnic.be/janus/fase"  
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">  
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">  
    <wsa:Action>janus:polling?mode=sync</wsa:Action>  
    <wsa:From>  
      <wsa:Address>http://etnic.be/soapui</wsa:Address>  
    </wsa:From>  
    <wsa:MessageID>uuid:28158767-4bb7-4b06-b7fe-a6d0b35ae884</wsa:MessageID>  
    <wsa:To>http://www.etnic.be/janus/polling</wsa:To>  
  </soapenv:Header>  
  <soapenv:Body>  
    <GetMessage/>  
  </soapenv:Body>  
</soapenv:Envelope>
```

### Réponse fonctionnelle:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"  
xmlns:soapenv12="http://www.w3.org/2003/05/soap-envelope"  
xmlns:wsa="http://www.w3.org/2005/08/addressing">  
  <soapenv:Header>  
    <wsa:To>http://etnic.be/soapui</wsa:To>  
    <wsa:MessageID>uuid:28158767-4bb7-4b06-b7fe-a6d0b35ae884</wsa:MessageID>  
    <wsa:RelatesTo>00000145279160df-246</wsa:RelatesTo>  
    <wsa:From>  
      <wsa:Address>http://www.etnic.be/janus/polling</wsa:Address>  
    </wsa:From>  
    <wsa:Action soapenv:mustUnderstand="1">janus:polling?mode=sync</wsa:Action>  
  </soapenv:Header>  
  <soapenv:Body>  
    <pollingReponse xmlns="http://www.etnic.be/janus/polling"  
xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
```



Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

## Plateforme Services Web ETNIC - Spécifications techniques

```
<message>
  <ID>00000145279160df-246</ID>
  <Suivants>0</Suivants>
  <Contenu>
    <dedale:DedaleResponse xmlns:dedale="http://www.cfwb.be/dedale"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
      <dedale:Adresses>
        <dedale:Adresse>
          <dedale:Rue>Ruelle de Reuchamp</dedale:Rue>
          <dedale:Numero/>
          <dedale:BtePostale/>
          <dedale:CodePostal>1340</dedale:CodePostal>
          <dedale:Localite>OTTIGNIES-LOUVAIN-LA-NEUVE</dedale:Localite>
        </dedale:Adresse>
      </dedale:Adresses>
    </dedale:DedaleResponse>
  </Contenu>
</message>
</pollingReponse>
</soapenv:Body>
</soapenv:Envelope>
```





# Plateforme Services Web ETNIC

## Spécifications techniques

### 3. SECURITE

#### 3.1. CONNEXION SECURISEE TLS

Les messages transitent à travers un canal HTTPS supportant le protocole TLS 1.0. Le chiffrement supporté est : ECDHE-RSA-AES256-SH

Les certificats identifiant l'ETNIC lors de la connexion SSL sont auto-signés et doivent donc être installés dans votre *Trust Store*. Vous pouvez les récupérer avec votre outil préféré tel que les navigateurs Chrome ou Firefox sur base des URL <https://services-web.tq.etic.be> et <https://services-web.etic.be>. Ou bien en faire la demande à l'ETNIC.

#### 3.2. SECURISATION DES SERVICES WEB

L'accès aux services web est sécurisé selon la spécification WS-Security en conjonction avec les profils suivant:

- **UsernameToken Profile:** un login et un mot de passe sont joints à chaque requête.
- **x509Token Profile:** un certificat numérique est utilisé pour signer. A noter que si le certificat est le certificat de signature présent sur l'eID, il n'est pas utilisé directement pour éviter d'entrer le PIN correspondant à chaque requête. Il est alors utilisé pour obtenir un token de contexte de sécurité. C'est ce dernier qui est utilisé pour signer. Ce mécanisme est basé sur les spécifications WS-SecureConversation et WS-Trust.

##### 3.2.1. UsernameToken Profile

Cette spécification consiste à joindre un login et mot de passe dans les en-têtes WS-Security. La représentation du mot de passe doit être de type "PasswordText". Cela se spécifie dans l'attribut "Type" de la balise <wsse:Password> comme suit: <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">

##### Exemple d'un message authentifié par login et mode passe:

```
<soapenv:Envelope xmlns:ded="http://www.etic.be/services/ddle/normalisation/v2"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"><wsse:Security
xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><wsse:UsernameToken wsu:Id="UsernameToken-
7A8D1ED1FD3375EE531427794973214176"><wsse:Username>User_fake</wsse:Username><wsse:Password
Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">YU7hjlio!</wsse:Password></wsse:UsernameToken></wsse:Security><wsa:Action>dd
le:normalisationV2?mode=sync</wsa:Action><wsa:From><wsa:Address>http://etic.be/soapui</wsa:Ad
dress></wsa:From><wsa:MessageID>uuid:941b8e5c-817b-413b-8751-
d0180f4165a8</wsa:MessageID><wsa:To>http://www.etic.be/services/ddle</wsa:To></soapenv:Header
>
  <soapenv:Body>
    <ded:ObtenirDetailsAdresseRequete>
      <ded:Adresse>
        <ded:Rue>reuchamp</ded:Rue>
        <ded:Numero/>
        <ded:BtePostale/>
        <ded:CodePostal>1340</ded:CodePostal>
        <ded:Localite/>
      </ded:Adresse>
    </ded:ObtenirDetailsAdresseRequete>
  </soapenv:Body>
</soapenv:Envelope>
```



## Plateforme Services Web ETNIC

### Spécifications techniques

#### 3.2.2.x509Token Profile

La spécification x509Token Profile prévoit plusieurs possibilités pour référencer le certificat utilisé pour la signature. La méthode supportée par l'ETNIC consiste à référencer l'Issuer et le Serial Number.

Seul l'élément « Body » de l'enveloppe SOAP doit être signé.

#### Exemple d'un message signé par un certificat X509 :

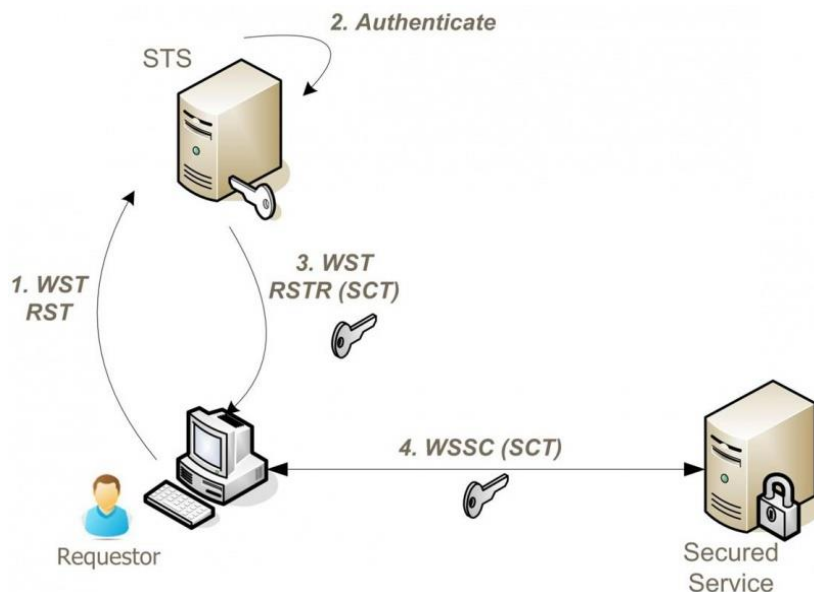
```
<soapenv:Envelope xmlns:siel="http://www.etic.be/janus/siel"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
  <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <ds:Signature Id="SIG-752" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces PrefixList="wsa siel soapenv"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:CanonicalizationMethod>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="#id-751">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="siel" xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>xC53nZkcNvpFd8vtucnvUwKPbsA=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>

    <ds:SignatureValue>hzm9/is507I5o3EZkVJ2jnbZiRSFSbFB10Y1w45mBqV2+8YRfHC1LVqafX7YLDVXTXrd1mWot1e
9+v31AiP3m5iy2+OCw7YhbXvCCCC0pbbf1/bpaeE/FE2f0sm4NZWsArpzlSEmd7DzpaiGxoMPWGxc
sefTSHHiClu0RH4Y4GERFBrHFDqDd2DMZHiugR0VxPz5QAacKeBnn68fZTK032I1+eOkyPaceuYH
YEBUEDjAfhrlchc0wKzfZuxt0dn6pBdh1U499nX2xZ4dGE37fHA0vbNRZLg/U5/b+KkKx/jEOe
9QJRSs/CKAONMfFcuZJnpZ+lbJoXT9UIK1jdUA==</ds:SignatureValue>
    <ds:KeyInfo Id="KI-EAF95CB2EABEB3293D13643957589981127">
      <wsse:SecurityTokenReference wsu:Id="STR-EAF95CB2EABEB3293D13643957589981127">
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>CN=WSJanusTEST_BULL001</ds:X509IssuerName>
            <ds:X509SerialNumber>1243600900</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
        </ds:X509Data>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="id-751" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd"> ...
</soapenv:Body>
</soapenv:Envelope>
```

#### 3.2.3.WS-Secure Conversation Token

Dans le cadre de l'utilisation du certificat de la carte d'identité électronique belge, il n'est pas envisageable de signer avec celui-ci car il impose de demander son code PIN à l'utilisateur pour chaque requête à signer avant envoi. C'est pourquoi un système de Security Token Service (STS) a été mis en place. Celui-ci peut être appelé via le standard WS-Trust afin de récupérer un jeton (token). C'est ce jeton qui servira à signer les requêtes suivantes jusqu'à son expiration.

Voici le schéma de ce principe :



1. **WST RST (WS-Trust Request Security Token)** : Le client envoie une requête de demande de token au serveur STS.

### Exemple de requête :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Id-18871350">
    <wst:RequestSecurityToken xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
      <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
      <wst:TokenType>http://schemas.xmlsoap.org/ws/2005/02/sc/sct</wst:TokenType>
    </wst:RequestSecurityToken>
  </soapenv:Body>
</soapenv:Envelope>
```

### 2. Authenticate

L'authentification auprès du STS se fait via Mutual SSL, dont le fonctionnement est décrit ci-dessous :





Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

## Plateforme Services Web ETNIC

### Spécifications techniques

```
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>D6F+imMesLRFAAjilmq3vYoJouA=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#id-2-d8b6db1a929f7c149819ec183c1548e1">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <ds:DigestValue>gw+8vQiLAmKyo10z1ShXlarhPRE=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>b1qcN4cWaPd7mPDnFUUXTbZgFoXEREj6Fja8QVOPPSH1DZtKQf59IVlJczMvZH3Jdglv6bWEWd0
KuBtsSniZQ4FyS4Qjx49oOGU14AOr5y0kKRoGyiDZRxMjaQzH+mYOJjH55c9ZbtHtg2pIKxkuXHxjos31RL6Y6s/12SB2q
/rNlWVD2eJSVWok5DSSoCmPRAqTYe8Jq83BcgAMMPbLFICoibcmiCsn3kpUWPmMgQcElaE89QCRwrRGXLD95r/nE4ujNBb
dHt7h1bcSMxiu8EFEmgt4DdvFB6IF6vKf7jMILs+4qPCI5Z31YHs2MxrNw5HnkM/dj+7puFXZh8C6sQ==</ds:Signatur
eValue>
  <ds:KeyInfo>
    <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <wsse:Reference URI="#id-0-b6b68eb710c70f895b1d2541064060c5"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"/>
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</soap:Header>
<soap:Body wsu:Id="id-1-254d82d66e9957c180e856d1bf0109f6" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <wst:RequestSecurityTokenResponse xmlns:wsc="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <wst:RequestedSecurityToken>
      <wsc:SecurityContextToken>
<wsc:Identifier>http://www.layer7tech.com/uuid/5d49793febfbbec46c5644fa0b05702f2be8cc9b</wsc:I
dentifier>
      </wsc:SecurityContextToken>
    </wst:RequestedSecurityToken>
    <wst:RequestedProofToken>
      <wst:BinarySecret
Type="http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey">gBndC3Zqhu6NiDBtM849Y7F4b89Pnd
302MKwQ9tYXZI=</wst:BinarySecret>
    </wst:RequestedProofToken>
    <wst:Lifetime>
      <wsu:Expires>2014-02-19T12:09:43.113Z</wsu:Expires>
    </wst:Lifetime>
  </wst:RequestSecurityTokenResponse>
</soap:Body>
</soap:Envelope>
```

4. **WSSC (SCT)** (*Ws-SecureConversation (Security Context Token)*): Les échanges avec le service sont maintenant sécurisés car signés par le token X.509 obtenu du serveur STS.

#### Exemple de requête envoyée avec le SCT :

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <soapenv:Header>
```



Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

## Plateforme Services Web ETNIC

### Spécifications techniques

```
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="true">
  <wsc:SecurityContextToken xmlns:wsc="http://schemas.xmlsoap.org/ws/2005/02/sc">

<wsc:Identifiant>http://www.layer7tech.com/uuid/5d49793febfbbec46c5644fa0b05702f2be8cc9b</wsc:I
dentifiant>
  </wsc:SecurityContextToken>
  <wsc:DerivedKeyToken xmlns:wsc="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="derivedKeyId-1">
  <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
    <wsse:Reference
URI="http://www.layer7tech.com/uuid/5d49793febfbbec46c5644fa0b05702f2be8cc9b"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"/>
      </wsse:SecurityTokenReference>
      <wsc:Offset>0</wsc:Offset>
      <wsc:Length>20</wsc:Length>
      <wsc:Nonce>avVNfpeBDmnPscPZ9Mu6ww==</wsc:Nonce>
    </wsc:DerivedKeyToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-2">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
        <ds:Reference URI="#id-3">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>6w9ZxQHZRgU2IeZs1YRb01NZTAM=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>PAAK5JUht+dPs/pgwmYYezogg=</ds:SignatureValue>
      <ds:KeyInfo Id="KeyId-3DF323081E1D4D392B13928045869761">
        <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="STRId-3DF323081E1D4D392B13928045869762"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
          <wsse:Reference URI="#derivedKeyId-1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"/>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wsse:Security>
  ...
</soapenv:Header>
<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="id-3">
  ...
</soapenv:Body>
</soapenv:Envelope>
```

### 4. CODES D'ERREUR

Les SOAP Fault techniques renvoyées par la plateforme sont identifiées par des codes catégorisés par type d'erreur :

#### Routage

Code d'erreur	Zone	Message FR	Message EN	Remarque
ROUT-0101	Client	Impossible de récupérer les informations de routage WS-Addressing ('action', 'to', 'from', 'msgId', ... manquants?)	Cannot retrieve WS-Addressing routing information ('action', 'to', 'from', 'msgId', ... missing?)	
ROUT-0103	Client	La règle de routage n'a pas pu être trouvée : veuillez vérifier les paramètres 'action', 'to' et 'mode'	Routing rule not found : please check your 'action', 'to' and 'mode' parameters	Le service indiqué dans les paramètres WS-A est inconnu
ROUT-0201	Client	Vous utilisez un port HTTP erroné pour l'envoi de vos requêtes	Wrong HTTP port	
ROUT-0202	Client	Vous utilisez un port HTTPS erroné pour l'envoi de vos requêtes	Wrong HTTPS port	
ROUT-1000	Server	Erreur technique de routage	Routing technical error	
ROUT-1001	Server	Erreur technique du fournisseur de service	Service provider technical error	Le backend (interne ou externe) a un problème
ROUT-1002	Server	Erreur technique de routage: il y a un problème avec la plateforme asynchrone	Routing technical error: there is an issue with the asynchronous platform	

#### Sécurité

Code d'erreur	Zone	Message FR	Message EN	Remarque
SECU-0102	Client	L'authentification a échoué : aucune information de sécurité reçue (WSS X509 ou WSS UsernameToken)	Authentication failed : no proven X509 certificate or username token found	Ni le user / mot de passe, ni le certificat n'ont été utilisés
SECU-0103	Client	L'authentification via la technique 'WSS UsernameToken' a échoué: utilisateur ou mot de passe invalide	WSS UsernameToken Authentication failed: invalid username or password	
SECU-0104	Client	L'authentification via la technique 'WSS X509' a échoué auprès du LDAP	WSS X509 Authentication failed against LDAP	Le certificat n'est pas reconnu
SECU-0200	Client	L'autorisation d'accès a échouée : vous utilisez un niveau de sécurité non défini par le service: \${securityLevelVerified}	Autorisation failed : security level not supported by the service: \${securityLevelVerified}	
SECU-0300	Client	Utilisation du protocole SSL obligatoire	SSL required	
SECU-0301	Client	STS: L'authentification a échoué	STS: User not authenticated	
SECU-0302	Client	Le service de génération de token de sécurité ne supporte que les requêtes de type 'Issue' et les token de type 'sct'	SecurityTokenService only support RequestType : 'Issue' and TokenType : 'sct'	Relatif à l'authentification par eID
SECU-1000	Server	L'authentification a échoué : erreur technique	Authentication failed : technical error	
SECU-1001	Server	Erreur technique de sécurité	Security technical error	
SECU-1100	Server	L'authentification a échoué : votre compte est désactivé	Authentication failed : your account is disabled	
SECU-1101	Server	L'autorisation d'accès a échoué : vous n'avez pas les profils de sécurité requis	Autorisation failed : incorrect security profile	Les autorisations n'ont probablement pas encore été accordées

#### Validation



Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

## Plateforme Services Web ETNIC

### Spécifications techniques

Code d'erreur	Zone	Message FR	Message EN	Remarque
VALI-0100	Client	La validation XSD du message de requête a échoué : <code>#{schema.failure}</code>	Validation of request message failed : <code>#{schema.failure}</code>	
VALI-0101	Client	La requête reçue n'est pas au format SOAP	Request is not a SOAP Message	
VALI-0200	Client	La taille de la requête que vous avez envoyée ( <code>#{request.size}</code> ) excède la limite autorisée ( <code>#{limit}Kb</code> )	Size of request exceed <code>#{limit}Kbytes</code> : <code>#{request.size}</code>	<code>#{limit}</code> = limite actuelle (10Mb)
VALI-1000	Server	Erreur technique de validation	Validation technical error	
VALI-1100	Server	La validation XSD du message de réponse a échoué : <code>#{schema.failure}</code>	Validation of response message failed : <code>#{schema.failure}</code>	<code>#{schema.failure}</code> indique l'erreur précise à l'intérieur du xml. Malheureusement, c'est l'erreur brute du parseur STAX qui est remontée sur laquelle nous ne pouvons pas prendre la main. Le texte à ce endroit sera donc toujours en anglais et très orienté JAVA.

#### Transformation

Code d'erreur	Zone	Message FR	Message EN	Remarque
TRAN-1100	Server	La transformation XSL du message a échoué	Transformation of msg failed	
TRAN-1101	Server	Erreur technique sur le traitement de la réponse	Technical error on response processing	

#### Polling

Code d'erreur	Zone	Message FR	Message EN	Remarque
POLL-0100	Client	Vous avez trop de messages en attente de lecture : <code>#{jdbcCount.found}</code> , veuillez d'abord effectuer des requêtes de polling	You have too many messages waiting : <code>#{jdbcCount.found}</code> , please poll first	
POLL-1000	Client	Erreur technique de polling	Polling technical error	



### 5. CONFIGURATION SOAP-UI

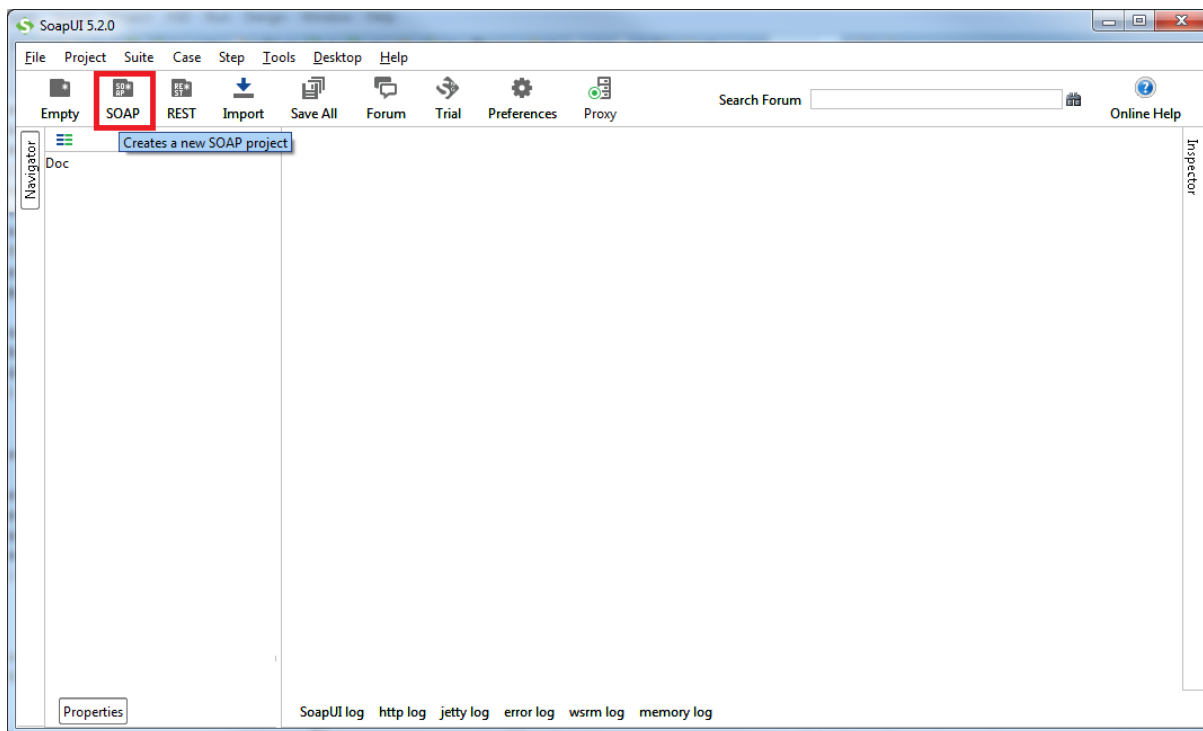
#### 5.1. UTILISATION DE SOAP-UI

Il est possible de tester les services web de l'Etnic grâce à l'application SOAP-UI. Il existe une version gratuite disponible sur le site: <http://www.soap-ui.org>

Cette section décrit les configurations particulières pour interagir avec les services web exposés par l'ETNIC.

#### 5.2. INITIALISATION DU PROJET

Tout d'abord, au lancement de l'application, vous devez créer votre projet de test en cliquant sur l'icône "SOAP" comme indiqué ci-dessous.



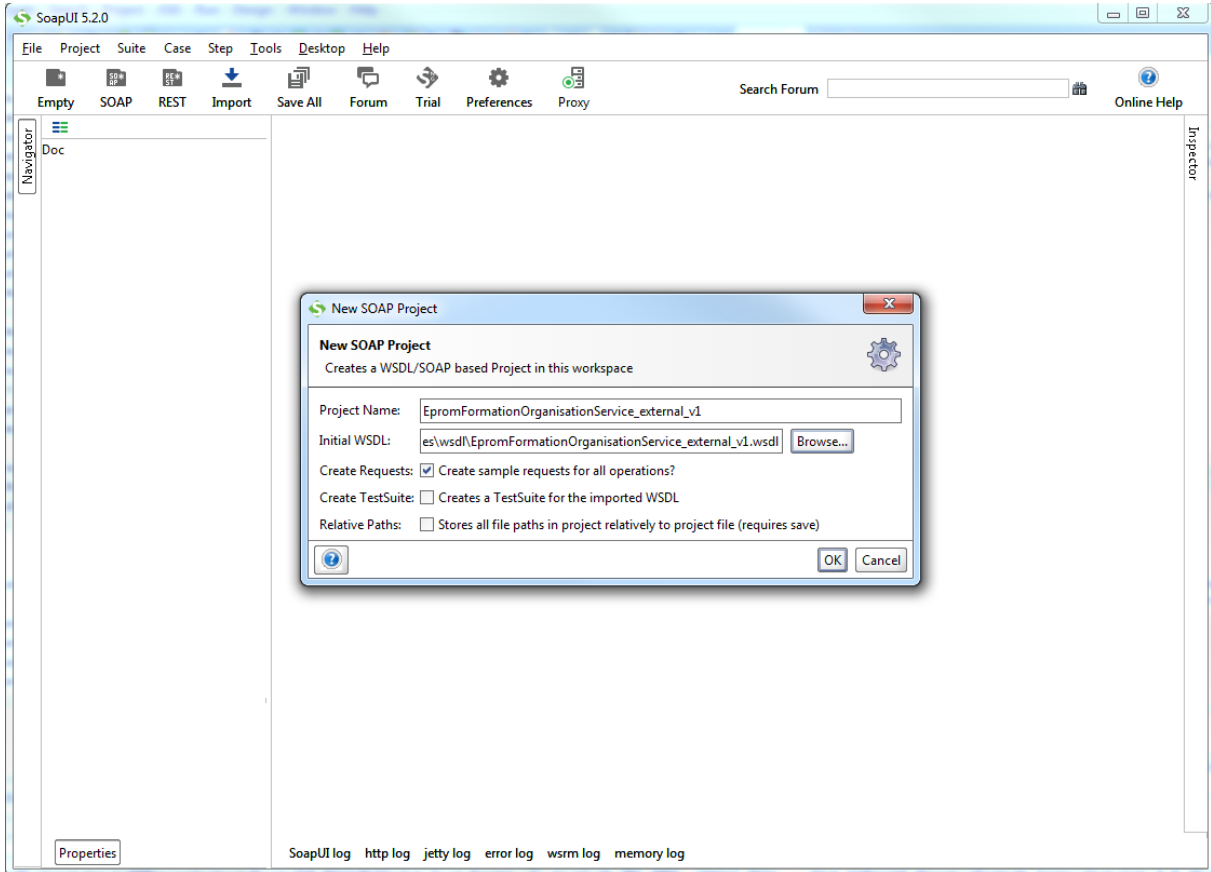


Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

# Plateforme Services Web ETNIC

## Spécifications techniques

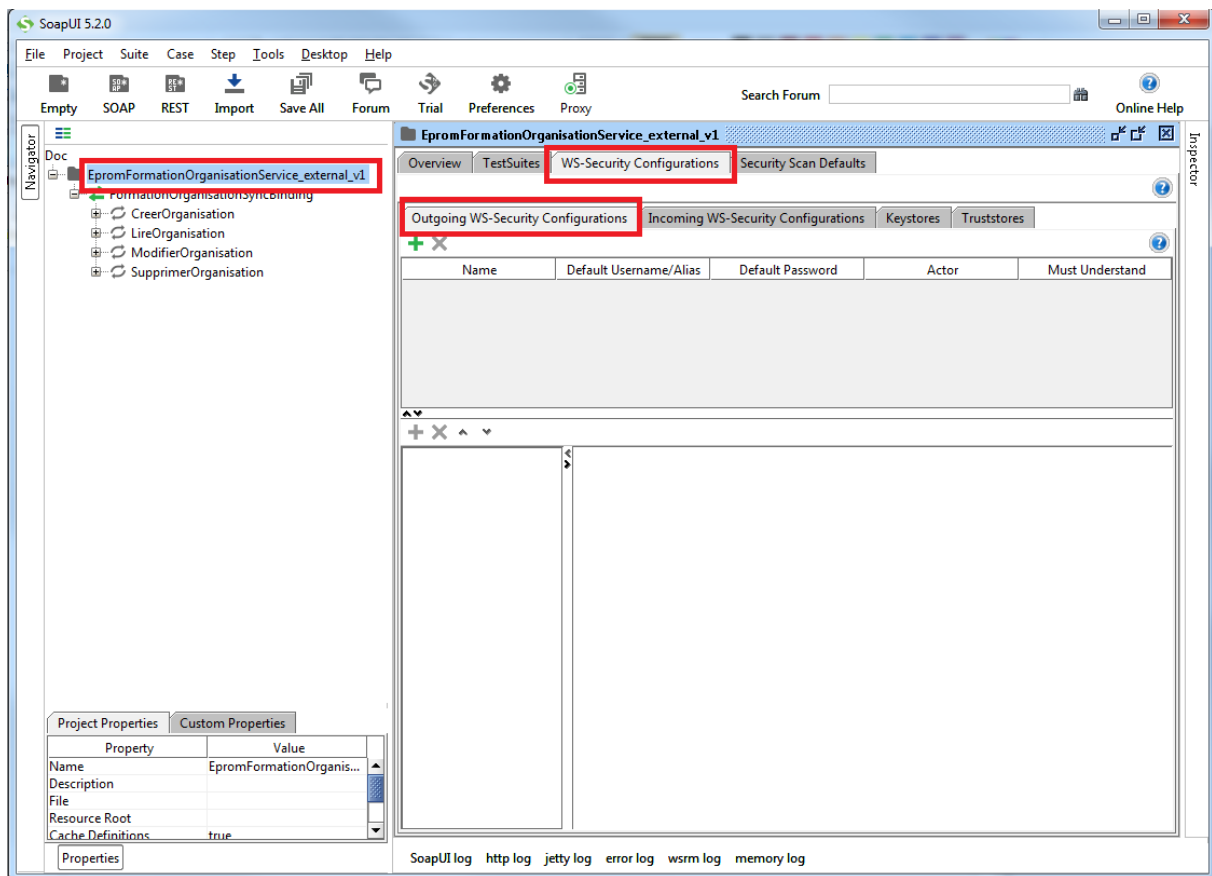
Ensuite vous indiquez le contrat WSDL décrivant le service web que vous allez tester:



### 5.3. CONFIGURATION WS-SECURITY

Pour configurer SOAP-UI afin d'utiliser WS-Security que ce soit en *username Token Profile* ou *x509Token Profile*, vous devez suivre les étapes suivantes:

Tout d'abord, double-cliquez sur le nom de votre projet dans la colonne de gauche. Cela ouvrira une fenêtre dans la partie droite de l'écran. Dans ce fenêtre cliquez sur l'onglet WS-Security Configurations et le sous-onglet "Outgoing WS-Security Configurations".



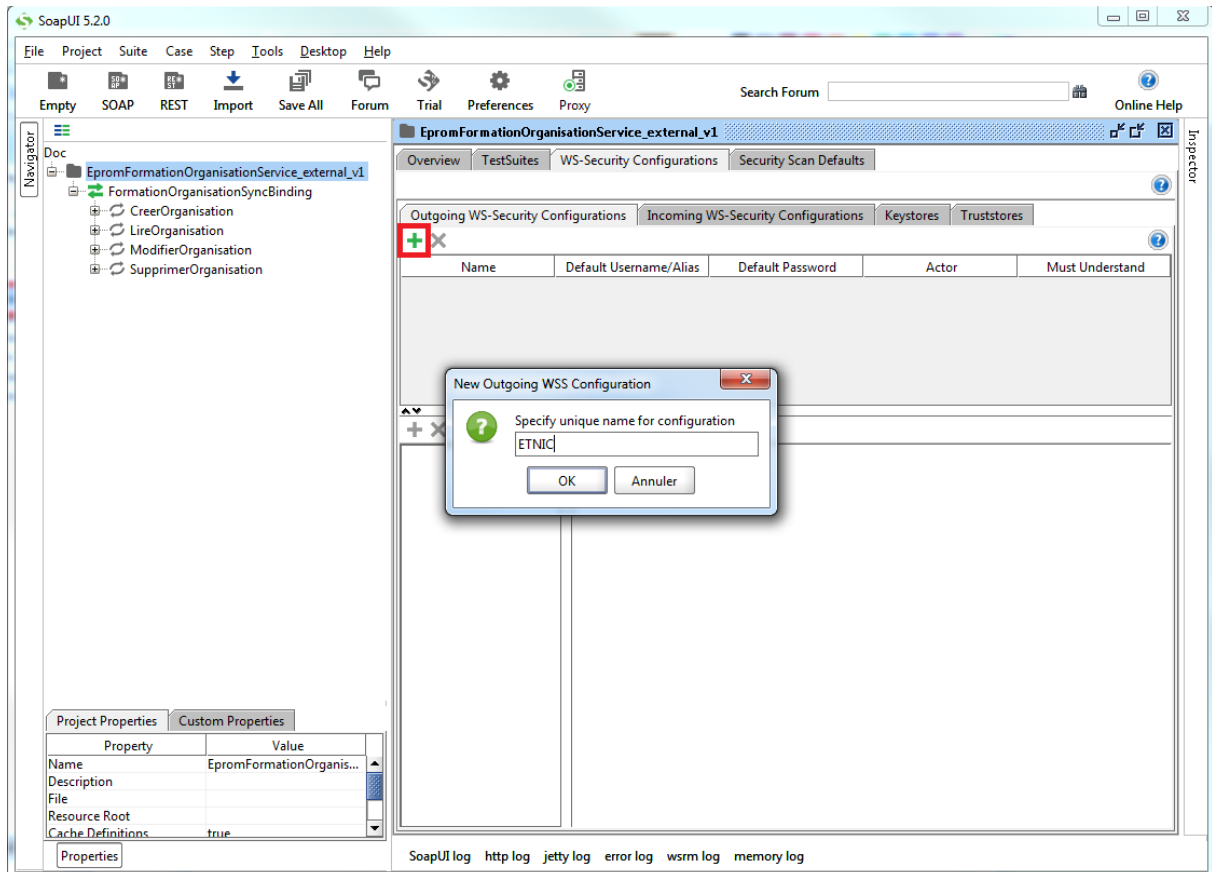


Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

# Plateforme Services Web ETNIC

## Spécifications techniques

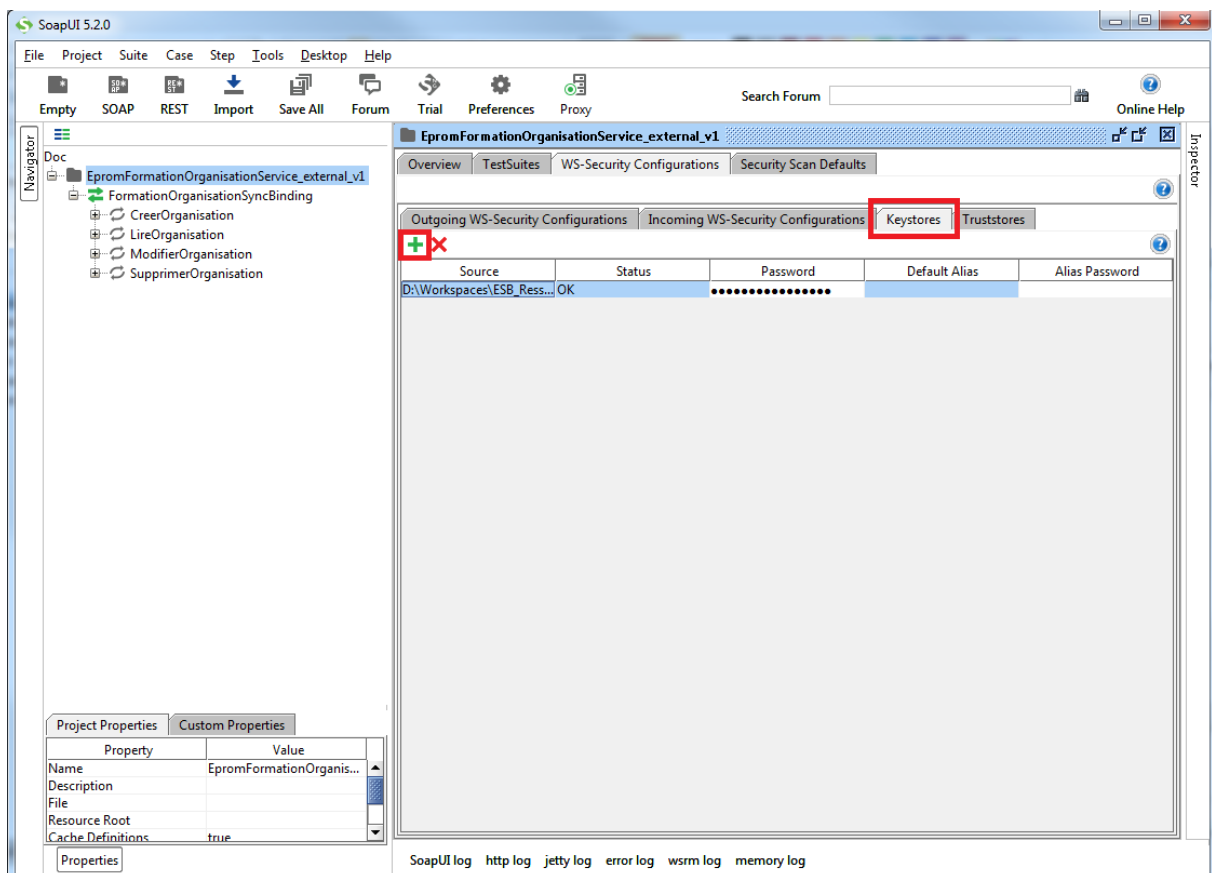
Cliquez sur l'icone "+" pour créer un alias pour une nouvelle configuration. Entrez le nom que vous désirez. Pour l'exemple, nous l'appellerons "ETNIC".



### 5.3.1. Configuration x509Token Profile

Pour configurer SOAP-UI afin de signer vos requêtes à l'aide du certificat que vous détenez, veuillez suivre les étapes suivantes:

Cliquez sur le sous-onglet "Keystore" et ajoutez un nouveau keystore via l'icone "+". Le fichier à ajouter est soit un fichier suffixé par .jks ou .p12. Tapez son mot de passe s'il est protégé.

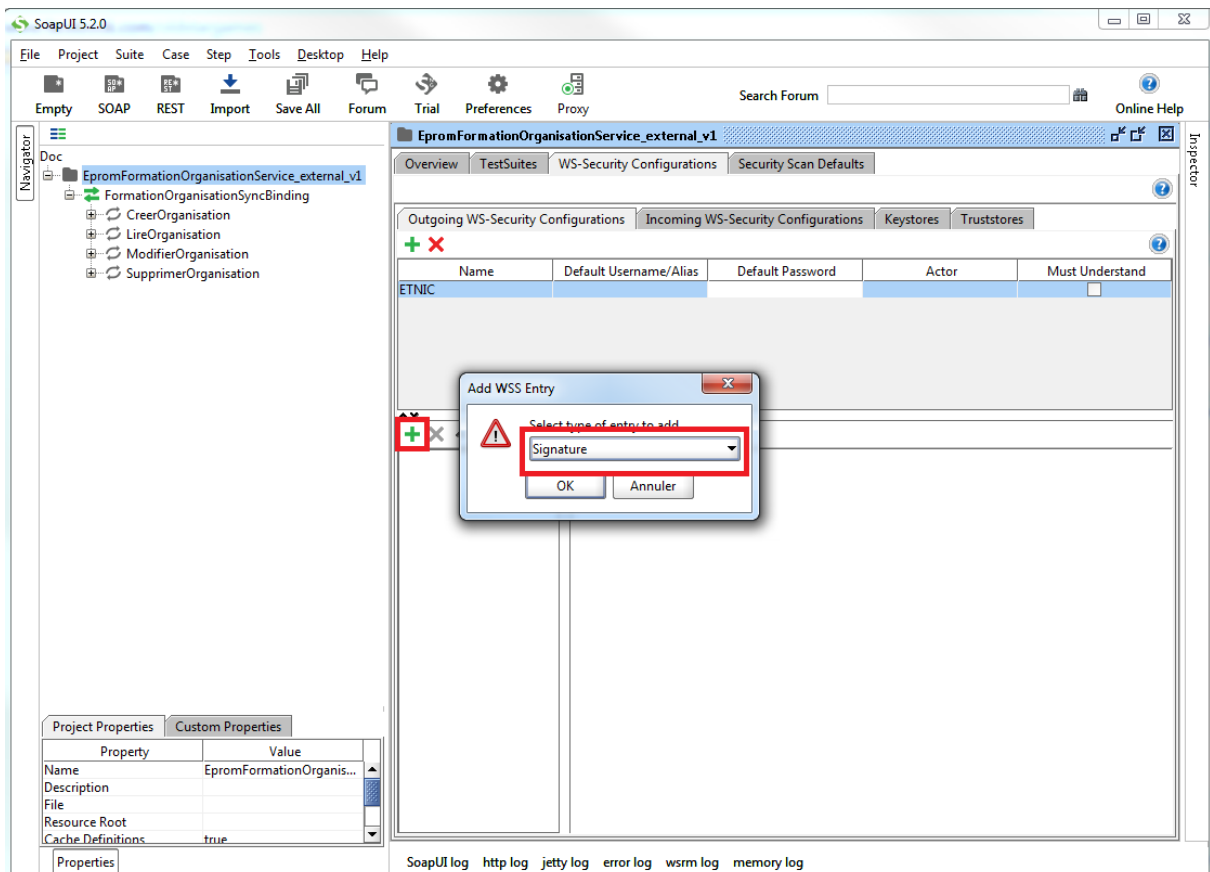




Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

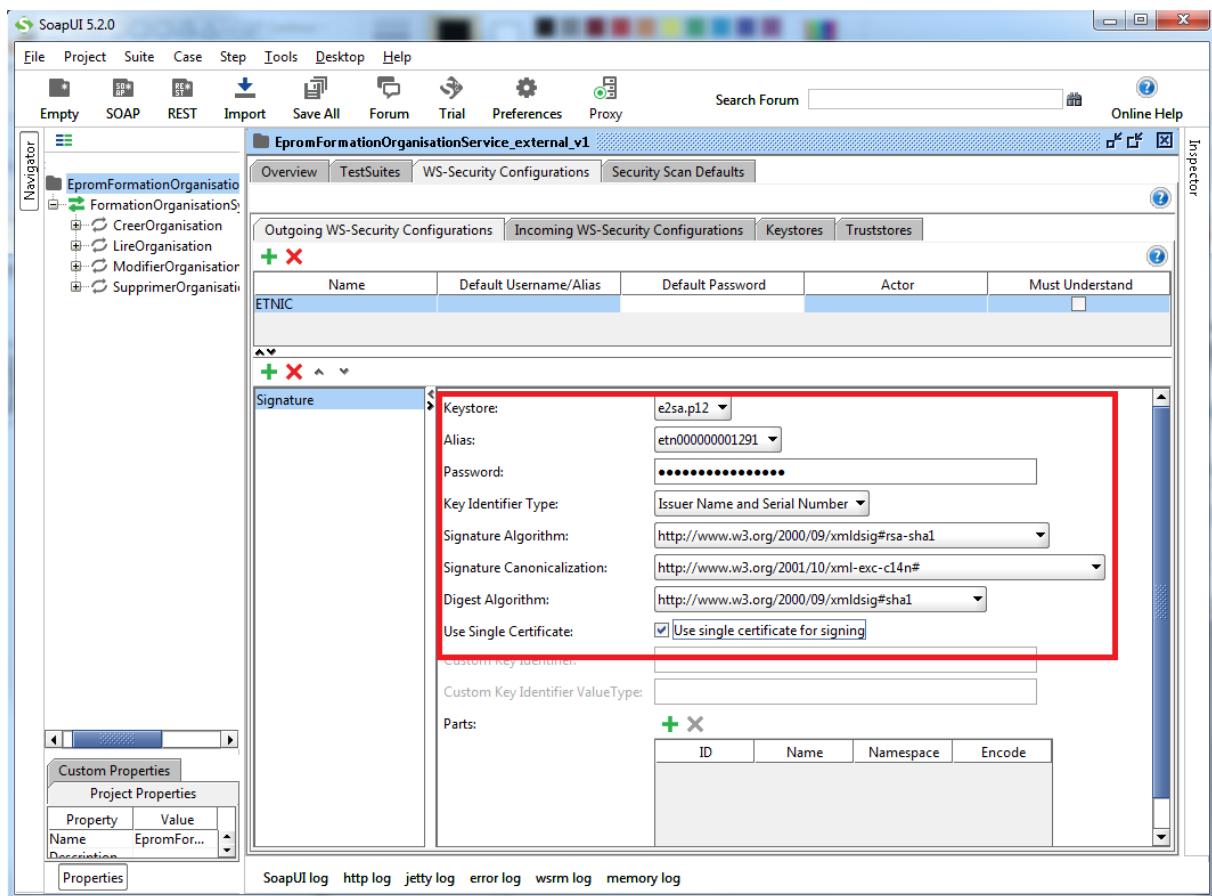
## Plateforme Services Web ETNIC - Spécifications techniques

Sélectionnez la configuration "ETNIC" que vous venez d'ajouter et cliquez sur l'icône "+" qui apparaît dans une colonne plus bas. Une pop-up apparaît vous invitant à choisir le type de configuration que vous désirez introduire. Choisissez "Signature".



Dans la partie droite de la fenêtre de configuration, remplissez les paramètres comme suit:

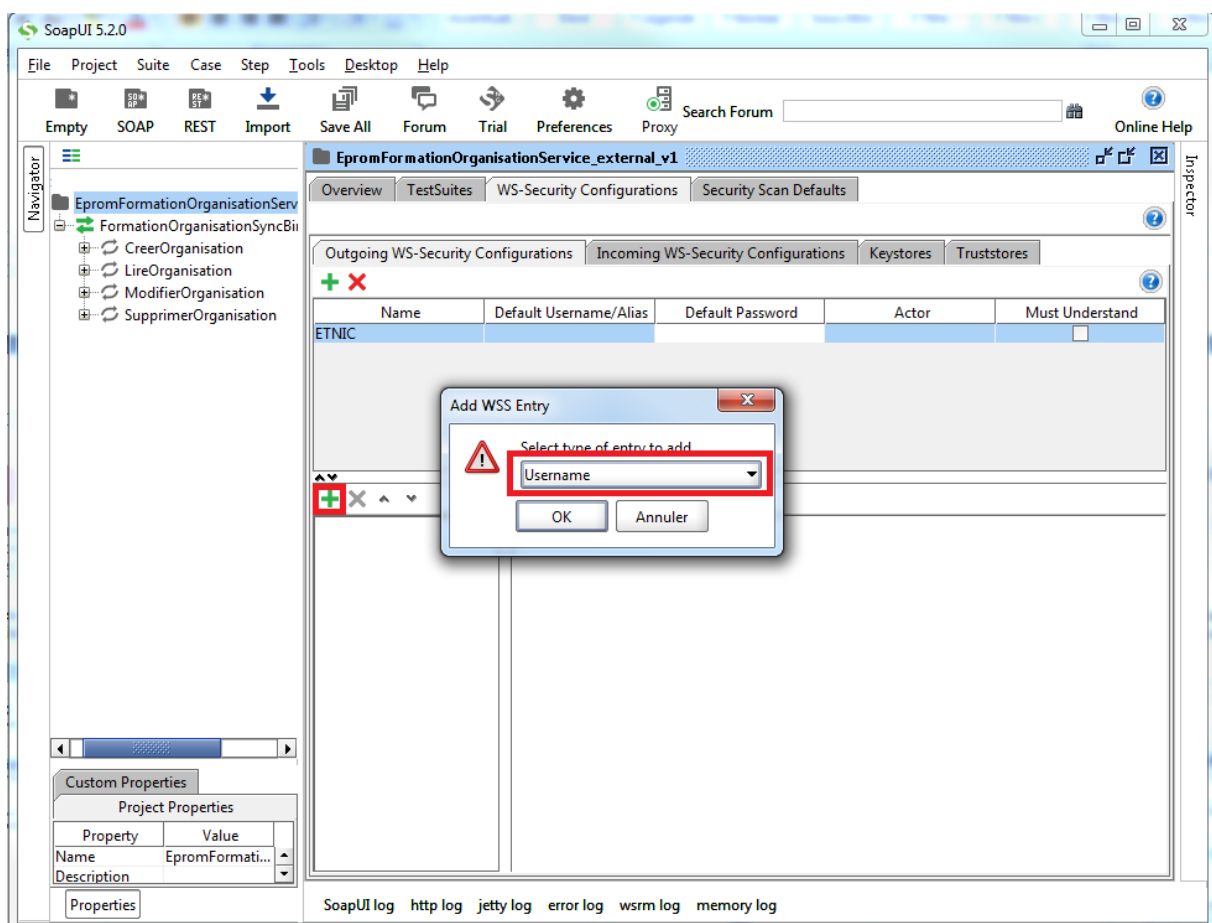
- Keystore: Sélectionnez votre keystore
- Alias: Sélectionnez l'alias de l'entité à authentifier (généralement, il n'y a qu'un choix)
- Password: Entrez le mot de passe du keystore s'il est protégé
- Key Identifier Type: Issuer Name and Serial Number
- Signature algorithm: <http://www.w3.org/2000/09/xmlsig#rsa-sha1>
- Signature Canonicalization: <http://www.w3.org/2001/10/xml-exc-c14n#>
- Digest Algorithm: <http://www.w3.org/2000/09/xmlsig#sha1>
- Use Single Certificate: Coché



### 5.3.2. Configuration usernameToken Profile

Pour configurer SOAP-UI afin de vous authentifier avec un identifiant et un mot de passe, veuillez suivre les étapes suivantes:

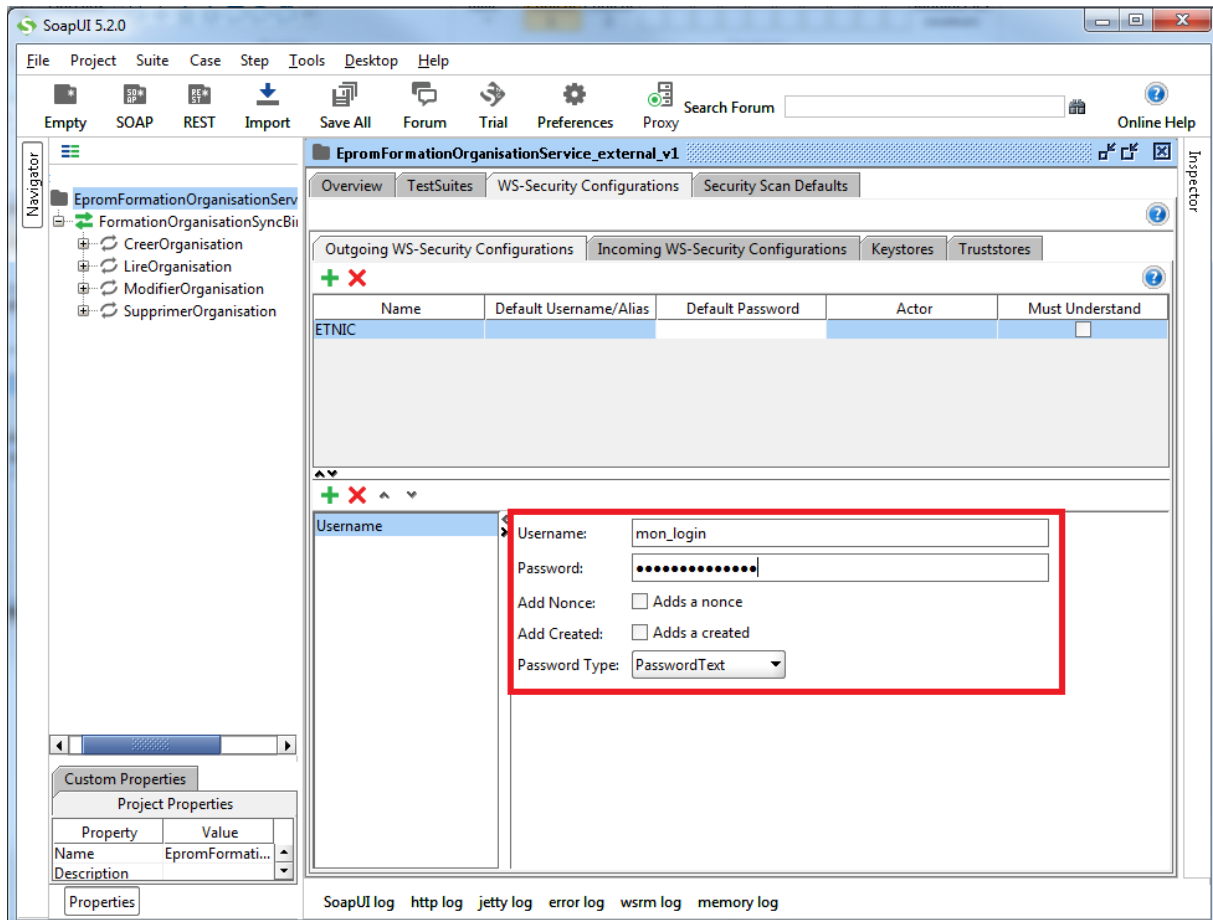
Sélectionnez la configuration "ETNIC" que vous venez d'ajouter et cliquez sur l'icône "+" qui apparaît dans une colonne plus bas. Une pop-up apparaît vous invitant à choisir le type de configuration que vous désirez introduire. Choisissez "Username".





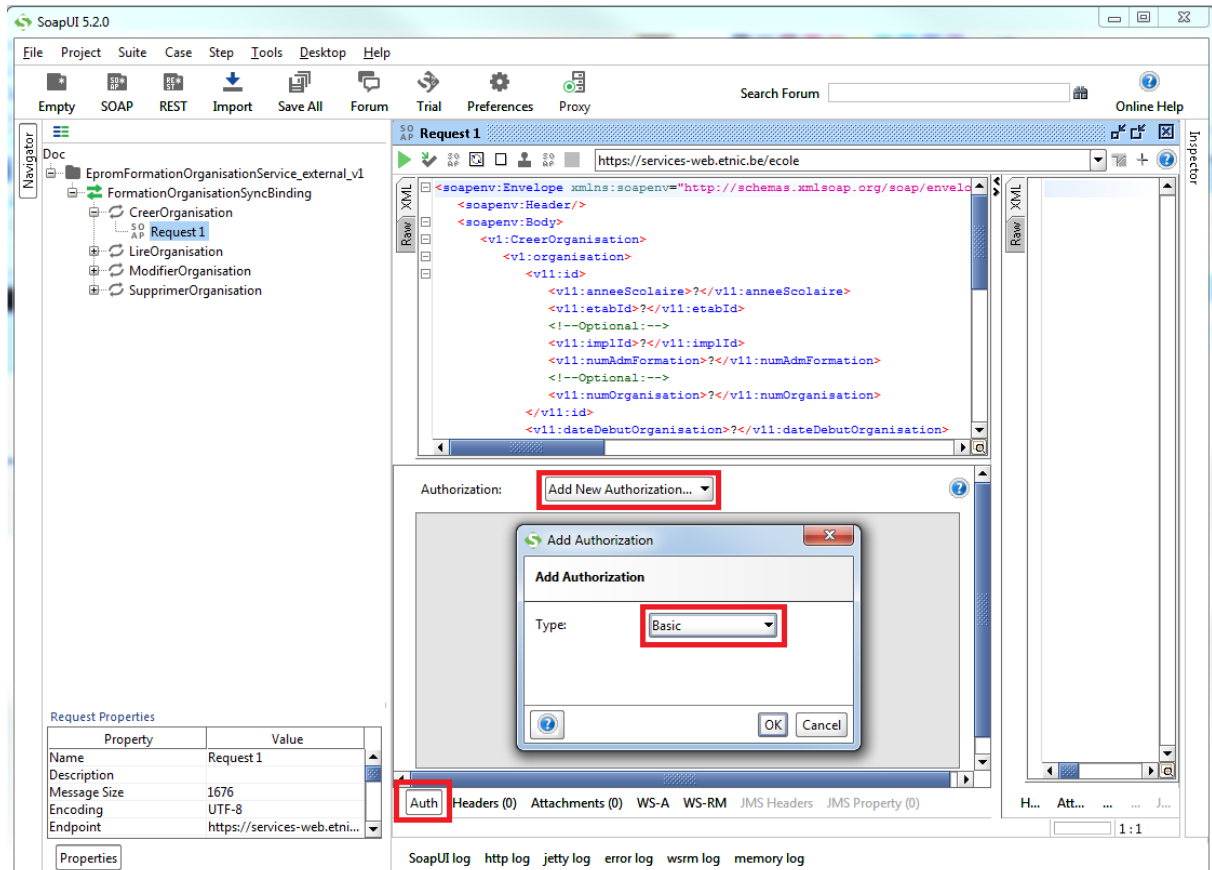
Dans la partie droite de la fenêtre de configuration, remplissez les paramètres comme suit:

- Username: votre identifiant
- Password: votre mot de passe
- Add Nonce: décoché
- Add Created: décoché
- Password Type: PasswordText



### 5.3.3. Application de WS-Security sur la requête

Dans la fenêtre de test d'une requête, cliquez sur l'onglet "Auth" en bas de la fenêtre. Choisissez "Add New Authorization" dans la fenêtre qui vient d'apparaître et "Basic" dans la pop-up suivante.





Bâtiment 'Le Zénith'  
Boulevard du Roi Albert II, 37  
1030 Bruxelles

## Plateforme Services Web ETNIC

### Spécifications techniques

Sélectionnez l'alias de votre configuration dans le champ "Outgoing WSS". Dans notre exemple, il s'agit d'"ETNIC". Le reste des champs doit rester vide.

The screenshot shows the SoapUI 5.2.0 interface. The main window displays a SOAP request configuration for 'Request 1' at the endpoint 'https://services-web.etnic.be/ecole'. The XML body of the request is as follows:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body/>
  <v1:CreerOrganisation>
    <v1:organisation>
      <v1:id>
        <v1:anneeScolaire?</v1:anneeScolaire>
        <v1:etabId?</v1:etabId>
        <!--Optional:-->
        <v1:implId?</v1:implId>
        <v1:numAdmFormation?</v1:numAdmFormation>
        <!--Optional:-->
        <v1:numOrganisation?</v1:numOrganisation>
      </v1:id>
      <v1:dateDebutOrganisation?</v1:dateDebutOrganisation>
    </v1:organisation>
  </v1:CreerOrganisation>
</soapenv:Body>
</soapenv:Envelope>
```

The 'Authorization' section is set to 'Basic'. The 'Outgoing WSS' dropdown menu is highlighted with a red box and contains the value 'ETNIC'. The 'Incoming WSS' dropdown is empty. The 'Request Properties' table at the bottom left shows the following details:

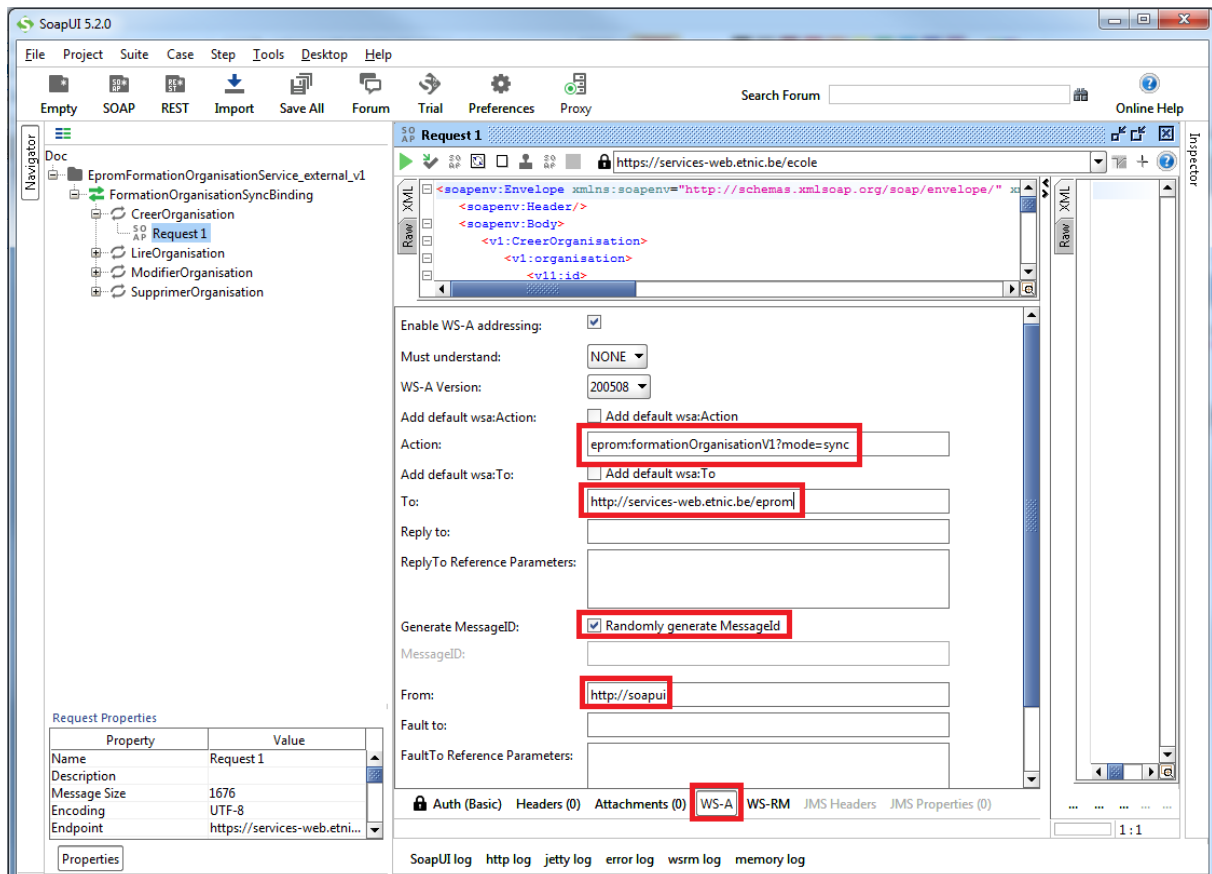
Property	Value
Name	Request 1
Description	
Message Size	1676
Encoding	UTF-8
Endpoint	https://services-web.etni...

### 5.4. CONFIGURATION WS-ADDRESSING

Dans la fenêtre de test d'une requête, cliquez sur l'onglet "WS-A" en bas de la fenêtre. Remplissez les champs suivants comme suit:

- Enable WS-Addressing: Coché
- Action: Introduisez l'"action" du service web à tester indiquée dans le manuel d'utilisation du dit service.
- To: Introduisez l'url "to" du service web à tester indiquée dans le manuel d'utilisation du dit service.
- Generate MessageId: Coché
- From (facultatif): Indiquez ici une uri à votre convenance assez parlante pour vous identifier. (par exemple: http://ecole-X/soap-ui)

Vous êtes maintenant prêt à ouvrir une connexion avec l'ETNIC et effectuer des tests.



The screenshot shows the SoapUI 5.2.0 interface with the 'Request 1' configuration window open. The 'WS-A' tab is selected at the bottom. The configuration fields are as follows:

- Enable WS-A addressing:
- Must understand: NONE
- WS-A Version: 200508
- Add default wsa:Action:  Add default wsa:Action
- Action:  (highlighted with a red box)
- Add default wsa:To:  Add default wsa:To
- To:  (highlighted with a red box)
- Reply to:
- ReplyTo Reference Parameters:
- Generate MessageId:  Randomly generate MessageId (highlighted with a red box)
- MessageID:
- From:  (highlighted with a red box)
- Fault to:
- FaultTo Reference Parameters:

The 'Request Properties' table at the bottom left shows:

Property	Value
Name	Request 1
Description	
Message Size	1676
Encoding	UTF-8
Endpoint	https://services-web.etni...

The 'WS-A' tab is highlighted with a red box at the bottom of the configuration window.