Guide technique B2B
Acteurs Tiers

Version 1.0 du guide

Identification : ENEDIS.SGE.REF.0468
Version : 1.0
Nb. de pages : 12

Version	Date d'application	Nature de la modification	Annule et remplace
1.0	08/03/2018	Création du document	

Document(s) associé(s) et annexe(s)

- Guides d'implémentation des webservices

Résumé / Avertissement

Ce document présente l'infrastructure d'échange mise en place par le Distributeur Enedis et les contraintes techniques associées à l'utilisation du canal d'échange B2B.

Nota : les informations contenues dans ce guide sont publiées à titre d'information et ne peuvent être assimilées à des règles contractuelles. Notamment, les exemples qui y sont présents illustrent les principes généraux énoncés, mais ils ne se substituent, ni aux guides d'implémentation, ni aux XSD et WSDL (qui précisent les points d'accès aux services, etc.).

Enedis - Tour Enedis
34 place des Corolles
92079 Paris La Défense Cedex
enedis.fr

SA à directoire et à conseil de surveillance
Capital de 270 037 000 euros
R.C.S. de Nanterre 444 608 442
Enedis est certifié ISO 14001 pour l'environnement

SOMMAIRE

1. Introduction

Enedis expose aux demandeurs un ensemble de webservices. L'accès à ces services est effectué de manière sécurisée via une authentification par certificats SSL. Ce document présente l'infrastructure technique des échanges B2B à mettre en place entre le Distributeur Enedis et les acteurs de marché, permettant aux acteurs de marché d'accéder aux webservices. Les points abordés dans ce document sont :

- Les principes généraux des échanges B2B,
- Les spécificités techniques de sécurisation de ces échanges,
- L'implémentation des webservices.

1.1. Périmètre étudié

Ce document couvre les demandes au travers de l'interface B2B.

Il ne couvre pas les demandes réalisées depuis l'interface du Portail SGE.

1.2. Principes généraux

- Le canal d'échange B2B permet via les webservices, d'accéder aux informations contractuelles et techniques des points de consommation, ainsi qu'aux différentes données de mesures disponibles.

- Les informations sont échangées automatiquement entre le SI du Demandeur et le SI d'Enedis. La communication se fait de façon synchrone. Il est proposé pour des demandes unitaires à forte volumétrie.

- L'accès aux webservices de SGE nécessite la mise en place d'un mécanisme d'authentification mutuelle basé sur un échange de certificat (protocole SSL).

- L'approvisionnement du certificat est à la charge du partenaire qui doit en faire la demande auprès d'une Autorité de Certification reconnue par Enedis.

- Un seul et unique certificat client pourra être utilisé par l'acteur de marché pour l'authentification auprès de SGE pour le canal webservice.

- Les requêtes d'appel aux webservices suivent des règles de construction contenues dans les guides d'implémentation disponibles sur le portail SGE.

2. Sécurisation des échanges

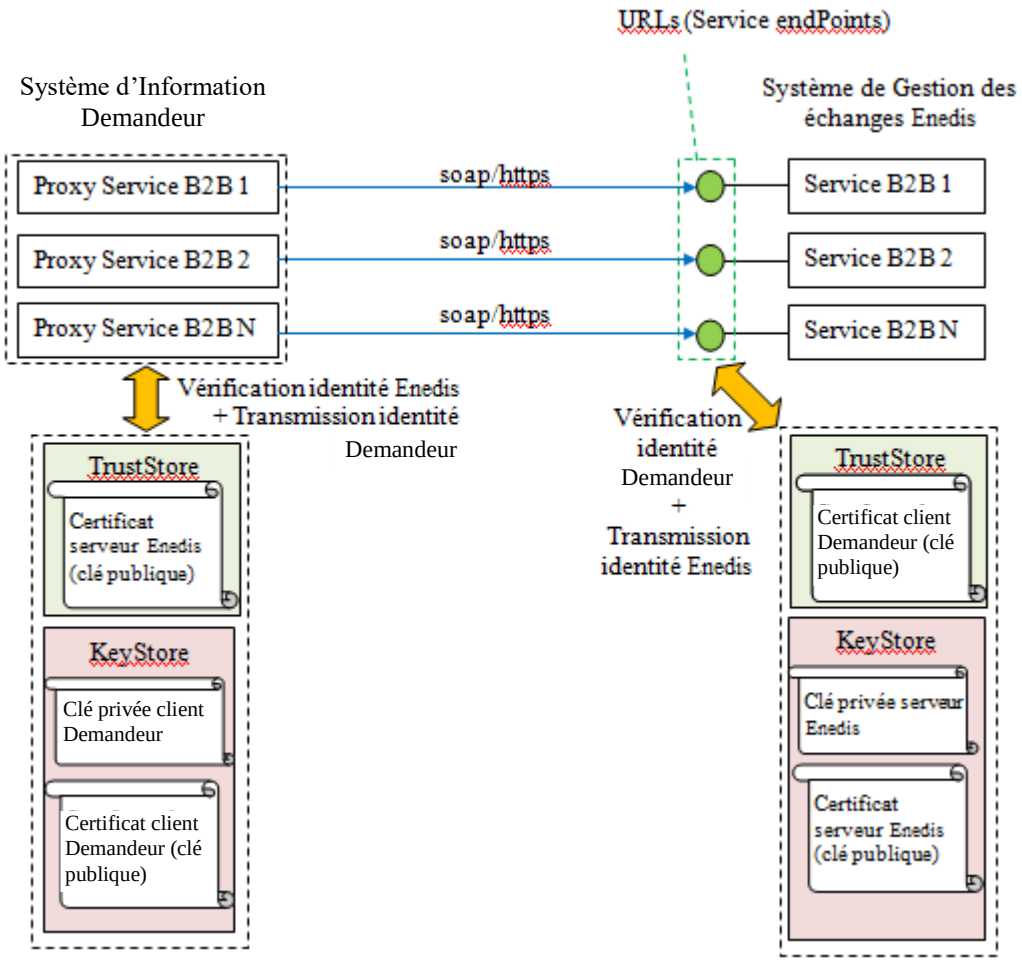
2.1. Marche à suivre

Le Demandeur se procure un certificat client auprès d'une autorité de certification reconnue par Enedis.

Le Demandeur fournit à Enedis son certificat client (clé publique) ainsi que son autorité de certification, afin que ceux-ci soient intégrés au niveau du frontal Enedis. Ceci permettra ainsi que le Demandeur soit reconnu lors des appels en webservices.

A son tour, Enedis fournit son autorité de certification, utilisée pour les échanges en B2B, ainsi que son certificat client En plus de la sécurisation des échanges, les appels effectués par les demandeurs sont tracés par Enedis.

Le schéma ci-dessous présente l'intégration mise en œuvre entre le SI d'Enedis et le SI du demandeur :



2.2. Eléments fournis par Enedis

Enedis fournit les éléments suivants aux demandeurs :

- La clé publique Enedis et son autorité de certification : ils permettent au Demandeur de vérifier l'identité d'Enedis lors de l'échange
- URLs de chaque service (service endPoints) (à retrouver dans les entêtes de la XSD de chaque webservice)
- WSDL et XSD des services B2B. Ces fichiers constituent les contrats d'interfaces des services exposés et décrivent pour chaque opération les entrées et sorties

2.3. Générer une clé privée/publique et un certificat client

Il s'agit pour le demandeur de générer un couple de clés privée/publique ainsi qu'un certificat client.

Ce certificat client doit être signé par une autorité de certification, et permet à Enedis de vérifier l'identité du demandeur. Il doit donc être transmis à Enedis une fois généré.

Ces opérations peuvent être réalisées à l'aide des utilitaires « keytool » et « openSSL ».

2.4. Importer les clés et le certificat client dans le magasin de clés (KeyStore[1])

Il s'agit d'importer dans le magasin de clés demandeur les clés générées ainsi que le certificat client.

Exemple de format possible pour un magasin de clé : JKS (Java Key Store).

2.5. Importer le certificat serveur Enedis dans le magasin de confiance (TrustStore[2])

Le certificat serveur fourni par Enedis doit être importé dans le magasin de confiance, permettant de vérifier l'identité du serveur Enedis lors des appels de services.

De la même manière que pour le magasin de clés, l'un des formats possible est le JKS.

2.6. Générer un ensemble de proxies pour les services B2B Enedis

Pour chaque WSDL fourni par Enedis, il est nécessaire de générer un proxy applicatif permettant d'appeler le service associé. Dans un contexte SI orienté objet, un ensemble de classes est alors automatiquement généré pour représenter les types manipulés en entrée et en sortie mais également l'interface du service et la classe de service proxy associée.

Ce port expose alors l'ensemble des opérations du WSDL et permet de les appeler localement au système du demandeur.

Dans le cadre d'un SI JAVA, il est recommandé d'utiliser l'utilitaire « wsimport » fourni avec le JDK.

[1] Keystore: Chaque serveur (front et back office) doit posséder un keystore. Le keystore contient des ensembles clé publique/clé privée/certificat. Ces éléments sont ses identifiants.
[2] Truststore: Chaque serveur (front et back office) doit posséder un truststore. Le truststore contient la liste de certificats de confiance

2.7. Ajouter les TrustStore et KeyStore au contexte SSL des proxies

Cette action est nécessaire pour définir un mode de transport HTTPS exploitant les certificats et clés des magasins de clés et de confiance.

Dans le cadre d'un SI JAVA, ceci peut être réalisé de manière programmatique via les API JAX-WS, ou bien en ajoutant les propriétés JVM suivantes : javax.net.ssl.keyStore / javax.net.ssl.trustStore.

2.8. Rendre paramétrable les URLs de endPoints des services

Il est préférable de permettre le paramétrage des URLS des endPoints, plutôt que d'utiliser la valeur portée par le WSDL. En règle générale, les outils de génération de proxies utilisent l'URL définie dans le WSDL.

Une surcharge est généralement possible de manière programmatique.

Dans le cadre d'un SI JAVA, il est possible d'utiliser la propriété suivante sur le port du service : BindingProvider.ENDPOINT_ADDRESS_PROPERTY.

3. Mise en œuvre des webservices

Une fois que les certificats du demandeur et d'Enedis ont bien été installés dans les SI réciproques, le Demandeur peut alors effectuer des appels vers le SI d'Enedis via les webservices proposés. L'implémentation de ces webservices doit suivre rigoureusement les instructions des guides d'implémentation mis à disposition sur le portail SGE.

Chaque guide contient :

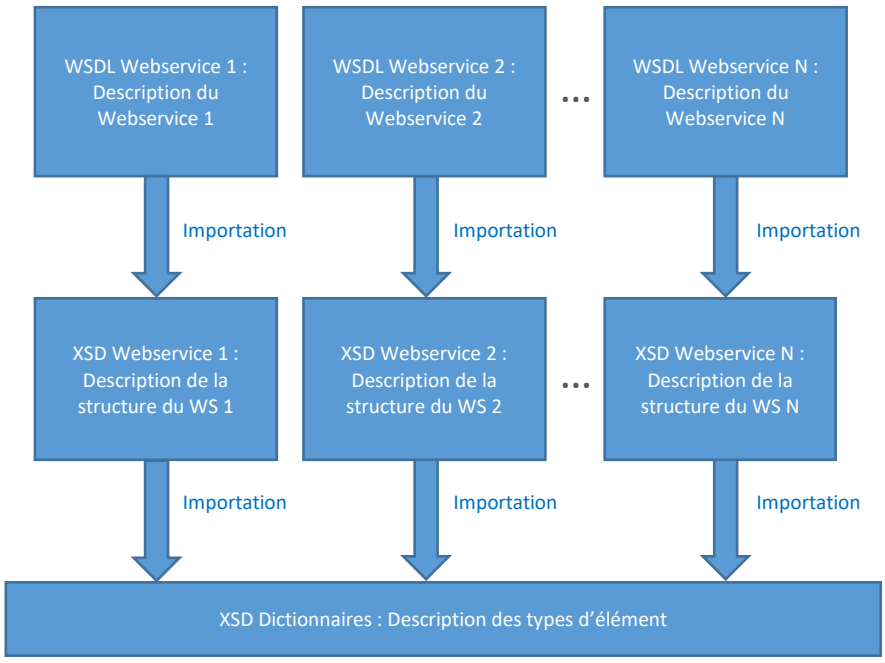
- un fichier PDF détaillant les règles SI du webservice,
- un dossier *Service* contenant la WSDL et la XSD du webservice,
- un dossier *Dictionnaire* contenant les éléments utilisés dans le webservice.

3.1. Structuration des services

Chaque appel B2B est formalisé par un message au langage XML

- Les messages sont contenus dans une enveloppe SOAP:
  - Les données fonctionnelles sont contenues dans le corps soap
  - Les données techniques sont contenues dans l'entête soap
- Les messages sont regroupés dans des fichiers pour l'interface batch
- Le codage des caractères des messages est réalisé en UTF 8

Le schéma ci-après représente la structuration des WSDL :



Les messages sont constitués de la manière suivante :

- Pour permettre l'accès B2B unitaire, les *wsdl* services importent le schéma défini dans la *XSD* service correspondantes. Ces *wsdl* contiennent donc uniquement les informations définissant les points d'accès des services (*port, binding*, etc.).
- un schéma (*XSD* service) définit les messages d'entrée et de sortie propres à chaque service métier B2B. Chacun de ces schémas importe des dictionnaires
- un schéma (*XSD* dictionnaire) regroupe l'ensemble des définitions communes de types.

Avertissements :

- **La définition des éléments est faite de manière à permettre tous les cas valides. Il est donc compréhensible que celle-ci soit la plus tolérante possible du point de vue des valeurs et occurrences acceptées afin de ne pas bloquer les messages conformes aux contrôles XSD.**
- **Les contraintes supplémentaires propres à chaque webservice sont consignées dans les guides d'implémentation des différents webservices. Ceux-ci restent la référence en la matière.**
- **La transmission de balises vides n'est pas autorisée, ceci entraînant un rejet des demandes.**

3.2. Structuration des messages

3.2.1. Exemple de message de demande

Nota : à titre d'exemple, grâce au logiciel SoapUI, il est possible de générer des demandes type d'un webservice en important la WSDL présente dans le fichier *Service* de son guide d'implémentation.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/
xmlns:v1="http://www.enedis.fr/sge/b2b/technique/v1.0"
xmlns:v11="http://www.erdf.fr/sge/b2b/services/commandersouscription/v1.1">
  <soapenv:Header>
    <v1:entete>
      <version>1.1</version>
      <infoFonctionnelles>
        <pointId>14141414141414</pointId>
      </infoFonctionnelles>
      <infoDemandeur>
        <loginDemandeur>homologation@demandeur.fr</loginDemandeur>
      </infoDemandeur>
    </v1:entete>
  </soapenv:Header>
  <soapenv:Body>
    <v11:commanderSouscription>
      <demande>
        <donneesGenerales>
        ...
        </donneesGenerales>
      </demande>
    </v11:commanderSouscription>
  </soapenv:Body>
</soapenv:Envelope>
```

Bloc <soapenv:Envelope> : contient le message global

Bloc <sopenv:Header> : entête du message contenant les informations techniques

Bloc <entete> :

- Le namespace est décrit dans le guide de chaque WS
- les éléments à remplir sont décrits dans le guide chapeau B2B pour chaque WS

Bloc <sopenv:Body> : corps du message contenant les informations fonctionnelles

Bloc du service métier appelé : les conditions d'utilisation des balises sont décrites dans le guide d'implémentation du webservice appelé

3.2.2. Exemples de message de retour

3.2.2.1. Message de succès

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/>
  <soapenv:Header>
  <v1:acquittement xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:v1="http://www.enedis.fr/sge/b2b/technique/v1.0">
        <resultat code="SGT200">Succès</resultat>
        <infoFonctionnelles>
            <pointId>98800004366006</pointId>
        </infoFonctionnelles>
  </v1:acquittement>
  </soapenv:Header>
  <soapenv:Body xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <v1:consulterMesuresDetailleesResponse xmlns:v1="http://www.enedis.fr/sge/b2b/technique/v1.0">
        ...
        </v1:consulterMesuresDetailleesResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

Bloc <soapenv:Envelope> : contient le message global

Bloc <sopenv:Header> : entête du message contenant les informations techniques

Bloc du service métier appelé : les balises de retour sont décrites dans le guide d'implémentation du webservice appelé

3.2.2.2. Message d'erreur

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/>
 <soapenv:Body>
   <soapenv:Fault>
         <faultcode>soapenv:Server</faultcode>
         <faultstring>Une erreur technique est survenue</faultstring>
    <detail>
          <v1:erreur xmlns:v1="http://www.enedis.fr/sge/b2b/technique/v1.0">
           <resultat code="SGT500">Une erreur technique est survenue</resultat>
           <infoFonctionnelles>
              <pointId>98800004366006</pointId>
           </infoFonctionnelles>
           <infoDemandeur>
              <loginDemandeur>homologation@demandeur.fr</loginDemandeur>
           </infoDemandeur>
          </v1:erreur>
    </detail>
   </soapenv:Body>
 </soapenv:Fault>
</soapenv:Envelope>
```

Bloc <soapenv:Envelope> : contient le message global

Bloc <sopenv:Fault> : synthèse de l'erreur retournée

Bloc du détail de l'erreur retournée

- Contient les données fonctionnelles supplémentaires
- les codes retour sont décrits dans l'annexe des codes retour du Guide Chapeau

3.3. Gestion des versions des webservices

Plusieurs versions d'un même webservice peuvent co-exister en production. Lorsqu'une nouvelle version est exposée par Enedis (impliquant une modification de la xsd), l'ancienne version du service reste ouverte et utilisable pendant environ un an (sauf exception).

Exemple :

- La version du webservice est précisée à la fin de l'url d'appel :

  https://sge-b2b.enedis.fr/ConsultationMesures/v1.0

- la version du service utilisée lors d'une demande doit également être transmise à travers l'entête soap du message :

```
<entete>
    <version>1.0</version>
    <infoFonctionnelles>
…
</entete>
```

3.4. Traçabilité

L'ensemble des échanges réalisés entre les Partenaires et le système SGE est tracé. Les informations suivantes sont tracées :

- La date et l'heure de la demande
- L'adresse IP du serveur
- Le partenaire réalisant la demande (acteur du marché, login utilisateur)
- Le webservice appelé
- Le PDL associé à la demande
- Le message original de demande et message de la réponse
- Le numéro de session (services conversationnels)