# Dossier spécifications « Webservice d'alerte »

Version v008

**19 août 2020**

# LISTE DE DIFFUSION

| Organisme ou Entreprise | Noms des Destinataires | Nombre de copies | Pour | |
|---|---|---|---|---|
| | | | Action | Information |
| ASPONE | **Dany SALMON** | 1 | | X |
| Clients | **Utilisateurs Webservices** | 1 | | X |

# SUIVI DES MISES A JOUR

SUIVI DES VERSIONS

| Version | Date | Rédacteur | Commentaires |
|---|---|---|---|
| v001 | 14 décembre 2015 | Pierre RONZY | Version initiale |
| V002 | 20 juin 2016 | Frédéric DIRSON | Ajout de la nouvelle téléprocédure DRP |
| V003 | 14 juin 2017 | Pierre RONZY | Possibilité d'utiliser le code DPAE en entrée pour les DUE |
| V004 | 20 novembre 2017 | Thomas BRUN | Ajout de la nouvelle téléprocédure EDI-OGA |
| V005 | 27 décembre 2017 | Frédéric DIRSON | Ajout de la nouvelle téléprocédure EDI-PART |
| V006 | 22 Janvier 2018 | Thomas BRUN | Ajout des alertes sur message de service de type AIS et Réception de documents |
| V007 | 28 octobre 2019 | Thomas BRUN | Authentification SSO |
| V008 | 19 août 2020 | Thomas BRUN | Amélioration du mécanisme de verrouillage des comptes |

# SOMMAIRE

# 1. INTRODUCTION

## 1.1. Le projet

Le projet a pour finalité de mettre à disposition de clients un Web Service d'alerte (WS Alert) leur permettant au travers d'une application Web développée par leur propre soin d'invoquer ce service pour :

- Activer/désactiver les alertes d'un compte
- Modifier la configuration des alertes d'un compte
- Récupérer la configuration des alertes d'un compte

## 1.2. Terminologie et abréviations

***Portail ASPOne.fr :*** portail standard ASPOne.fr. Ce portail offre des fonctionnalités d'alerte pour un compte donné à travers une application Web et un espace privé offrant les fonctionnalités suivantes :

- Modification de la configuration des alertes
- Récupération de la configuration des alertes

***Client Marque Blanche (MB) :*** c'est l'entité représentant le client ayant commandé un portail marque blanche auprès d'ASPOne.fr et qu'ASPOne.fr opère.

***Portail en marque blanche (Portail MB) :*** portail dérivé du portail ASPOne.fr, offrant tout ou partie des fonctionnalités de ce portail, généralement adapté à la charte graphique du client marque blanche et accessible à partir du portail du Client MB.

***Portail client*** : le portail standard du Client MB à partir duquel un client final accède au Portail MB.

***Prospect :*** utilisateur internaute non inscrit au portail ASPOne.fr ou à un portail MB.

***Client :*** Utilisateur inscrit à un portail MB

***Client ASPOne.fr :*** Utilisateur inscrit au portail ASPOne.fr

***Interchange :*** Un interchange comprend un ou plusieurs groupes fonctionnels contenant chacun des messages ayant la même structure. Dans le cadre des télé-procédures EDI-TDFC et EDI-TVA EDIFICAS, un interchange pourra ainsi inclure plusieurs groupes fonctionnels avec au sein d'un groupe fonctionnel plusieurs messages de type INFENT, BALANC, CONTROL mais pas une mixité de ces types.

***Télé-déclaration :*** Groupe de segments appartenant à un interchange et identifiant l'émetteur , le déclarant, le destinataire, le type de document INFENT, BALANC, URSSAF…et les données déclarées.

***Compte primaire ASPOne.fr :*** un compte primaire ASPOne.fr est l'entité informatique représentative d'un utilisateur au niveau de l'application ASPOne.fr. Il est caractérisé par un identifiant unique (GUID), un ensemble d'attributs et un nom (nom de compte) dont la dénomination complète est dans le cas d'un compte ASPOne.fr : IdCompte@aspone.fr. Cet utilisateur possède une boîte aux lettres dont le nom est IdCompte@aspone.fr.

***Compte primaire MB :*** un compte primaire MB est l'entité informatique représentative d'un utilisateur au niveau de l'application ASPOne.fr. Il est caractérisé par un identifiant unique (GUID), un ensemble d'attributs et un nom de compte dont la dénomination complète peut être de type

IdCompte@ssdom.MB.fr (ssdom.MB.fr étant un sous-domaine du domaine MB.fr géré par ASPOne.fr). Cet utilisateur possède une boîte aux lettres dont le nom est IdCompte@ssdom.MB.fr.

***Compte secondaire :*** un compte secondaire ASPOne.fr est l'entité informatique représentative d'un utilisateur secondaire dépendant d'un utilisateur primaire existant dont le compte a pour nom IdCP. Il est caractérisé par un identifiant unique (GUID), un ensemble d'attributs et un nom (nom de compte secondaire) dont la dénomination complète est dans le cas d'un compte ASPOne.fr : IdCompte.IdCP@aspone.fr. Cet utilisateur possède une boîte aux lettres dont le nom est IdCompte.IdCP@aspone.fr.

***Compte secondaire MB :*** un compte secondaire MB est l'entité informatique représentative d'un utilisateur secondaire dépendant d'un utilisateur primaire MB existant dont le compte a pour nom IdCP. Il est caractérisé par un identifiant unique (GUID), un ensemble d'attributs et un nom (nom de compte secondaire MB) dont la dénomination complète peut être de type IdCompte.IdCP@MB.fr (ssdom.MB.fr étant un sous-domaine du domaine MB.fr géré par ASPOne.fr). Cet utilisateur possède une boîte aux lettres dont le nom est IdCompte.IdCP@ssdome.MB.fr.

**Il ya un lien hiérarchique entre compte primaire et compte secondaire, notamment en terme de suivi : un compte primaire peut accéder au suivi des dépôts qu'on réalisés les comptes secondaires qui dépendent de lui. Alors qu'un compte secondaire n'a accès au suivi que de ses propres dépôts.**

***PED :*** partenaire EDI

Messages de service :

- ***ADS :*** Avis de dépôt signé (réceptionné suite au dépôt)
- ***ACS :*** Avis de conformité signé (réceptionné suite au traitement du portail)
- ***ARS :*** Avis de remise signé (réceptionné suite aux traitements du ou des destinataire(s)
- ***AIS :*** Avis d'information signé (réceptionné suite l'envoi d'un compte rendu / d'une réponse complémentaire du ou des destinataire(s))
- ***RCP :*** Réception de document(s) (réceptionné suite à l'envoi par un autre compte client du portail de déclaration(s) / demande(s) dont on est le destinataire)

***ICR :*** Infent Compte-rendu, compte-rendu de traitement EDI, au format EDI, généré soit par le portail MB soit par les destinataires (DGI, OGA)

***Mail client :*** adresse mail externe personnelle du client.

***BAL client :*** nom de la boîte à lettres du client inscrit au portail MB, hébergée sur le portail MB et créée lors de la création de son compte (cf. ci-dessus).

***BAL fonctionnelle :*** boîte à lettres fonctionnelle utilisée par le portail MB pour une procédure particulière :

- Pour la liasse fiscale EDI : EDI-TDFC@ssdom.MB.fr
- Pour la TVA EDI : EDI-TVA@ssdom.MB.fr
- Pour le PAIEMENT EDI : EDI-PAIEMENT@ssdom.MB.fr
- Pour la DUCS : DUCS@ssdom.MB.fr
- Pour la DADS-U : DADS-U@ssdom.MB.fr
- Pour l'AED : AED@ssdom.MB.fr
- Pour la DUE/DPAE : DUE@ssdom.MB.fr
- Pour la DSI : DSI@ssdom.MB.fr
- Pour EDI-REQUETE : EDI-REQUETE@ssdom.MB.fr
- Pour EDI-IR : EDI-IR@ssdom.mb.fr
- Pour la DSN : DSN@ssdom.mb.fr
- Pour la DRP : DRP@ssdom.mb.fr

- Pour EDI-OGA : EDI-OGA@ssdom.mb.fr
- Pour EDI-PART : EDI-PART@ssdom.mb.fr

Les boîtes en question peuvent être mutualisées avec celles du portail standard.

***Inscription :*** mécanisme permettant d'obtenir toutes les informations nécessaires à l'enrôlement ultérieur d'un utilisateur d'une marque blanche particulière

***Enrôlement :*** mécanisme permettant à partir des informations d'inscription de créer l'utilisateur sur le portail.

## 1.3. Authentification

Il existe 2 niveaux d'authentification permettant d'authentifier d'une part la marque blanche et d'autre part l'utilisateur.

#### *1.3.1.1. Marque Blanche*

Lors de la mise en place de la marque blanche, ASPOne attribue un couple login / mot de passe à la marque blanche et les transmet de manière sécurisée aux correspondants identifiés.

Ces identifiants permettent de générer le jeton WSSE dans l'entête SOAP de la requête générée afin d'authentifier la marque blanche et de se prémunir contre les attaques de type « Replay Attacks ».

Pour plus de détails, voir les spécifications WSSE :

https://www.oasis-open.org/committees/download.php/13392/wss-v1.1-spec-pr-UsernameTokenProfile-01.htm

#### *1.3.1.2. Utilisateur*

Les identifiants de l'utilisateur (login / mot de passe choisis à l'inscription) doivent être renseignés en clair dans l'entête du message SOAP : cependant, étant donné que nous forçons l'utilisation du protocole HTTPS, ils ne transitent jamais en clair entre votre client webservice et nos serveurs.

Pour plus de détails sur les différents types d'utilisateurs et leur hiérarchie, voir en annexe Informations sur les comptes

Afin de prévenir toutes tentatives d'attaque par force brute sur l'authentification utilisateur de nos Webservices, nous avons mis en place le mécanisme suivant : suite à l'échec d'une tentative de login, l'utilisateur est obligé d'attendre pendant un temps déterminé avant de pouvoir tenter une nouvelle authentification. Le temps d'attente entre deux tentatives est proportionnel au nombre d'échecs (le nombre d'échecs étant remis à 0 suite à une authentification réussie) avec un maximum de 30mins.

Par ailleurs, nous proposons également l'authentification des utilisateurs (sauf les administrateurs) par SSO avec le formalisme suivant en lieu et place du mot de passe :

| |
|---|
| *sso:<date>:<heure>:<jeton>* |

Date : date de génération du jeton au format AAMMJJ

Heure : heure de génération du jeton au format HHmm

Jeton : Hash SHA256 (clé partagée + login + date + heure)

Le jeton est valide durant un temps donné (paramétrable par marque blanche), nous vous conseillons de le regénérer systématiquement à chaque appel.

Exemple :

| |
|---|
| *sso:191028:1701:669118f1183616ee47cb429d9eac6308d0cbac13f0f244234955270c3489d995* |

***Attention : La clé partagée est une clé secrète propre à chaque marque blanche et fournie par ASPOne : elle doit être stockée de manière sécurisée sur vos serveurs et ne doit en aucun cas être divulguée à un tiers ou embarquée dans un logiciel client lourd diffusé chez vos clients finaux.***

Pour toute demande de mise en place d'un accès SSO, merci de contacter dev-aspone@tessi.fr

# 2. ETUDE TECHNIQUE DE MODIFICATION DE LA CONFIGURATION DES ALERTES

## 2.1. Préalables

L'utilisation du WS Alert nécessite en préalable l'existence d'un « groupe » identifiant le portail marque blanche qui va utiliser le WS Alert pour enrôlement de ses clients.

Ce « groupe » est un attribut AD et correspond à une OU Windows dans laquelle seront stockés l'ensemble des utilisateurs client du portail en marque blanche.

## 2.2. Informations pour la modification de la configuration

### *2.2.1. Les informations de saisie*

Nous avons listé ci-dessous dans un tableau toutes les informations que l'on peut saisir lors de l'inscription d'un client. Il est rappelé leur utilisation, leur type (colonne type : AN = alphanumérique, N = Numérique, A = Alphabétique, B = Booléen, Enum = Liste), leur longueur (colonne Lg : X si longueur fixe, …X si longueur maximale X) et leur caractère obligatoire ou non (colonne M : * = Obligatoire, (*) = Dépendant du type de compte).

| Nom | Utilisation | Type | Lg / Enum | M |
|---|---|---|---|---|
| *Infos générales* | | | | |
| **Nom du compte** | **Sert à identifier le compte à modifier** | **AN** | **…9** | **N** |
| alertActive | Indique si les alertes sont activées ou non pour ce compte | B | | |
| *Option* | | | | |
| sendAdmin | Booléen permettant de préciser si l'admin souhaite recevoir les alertes des comptes qu'il gère. | B | | |
| secondaryAccountAlert | Booléen permettant de préciser si le compte primaire souhaite recevoir les alertes de ses comptes secondaires | B | | |
| mails | Cette zone va permettre de préciser la liste complète des adresses mails des destinataires. Les mails déjà paramétrés seront remplacés (dans la limite de 3) | AN | …250 | |
| mailsToAdd | Cette zone va permettre de rajouter des adresses mails (dans la limite de 3). | AN | …250 | |
| mailsToDelete | Cette zone va permettre de supprimer des adresses mails (dans la limite de 3). | AN | …250 | |
| *Multiple paiement* | | | | |
| sendMultiplePaiement | Alerte pour les multiples paiements (utile pour les clients abonnés à TVA ou PAIEMENT | B | | |
| *Notification* | | | | |
| sendTest | Booléen permettant de préciser si on envoie des alertes pour les flux de tests passé via un compte réel. | B | | |
| *TeleprocedureAlert* | | | | |
| teleProcedure | Nom de la téléproédure | Enum | TDFC, TVA, | * |

| | | | | |
|---|---|---|---|---|
| | | | PAIEMENT, DADS-U, DUCS, DUE, DPAE, AED, DSI, REQUETE, IR, DSN, DRP, OGA, PART | |
| *MessageService* | | | | |
| actif | Booléen indiquant si l'on souhaite envoyé une alerte | B | | * |
| type | Type de réponse pouvant déclencher une alerte | Enum | ACS, ARS, AIS, RCP | * |
| delai | Si pas de rejeu détecté, délai d'alerte en jour (uniquement pour les messages négatifs) | N | ..2 | * |
| Positif | Booléen indiquant si cela concerne une alerte sur retour négatif (ACS, ARS) ou positif (ARS, AIS, RCP) | B | | * |

#### *2.2.2. Paramétrages*

Les informations ci-dessus sont paramétrables.

La Marque Blanche peut présenter l'ensemble des informations qu'elle désire faire saisir par le client. Les informations obligatoires peuvent être masquées ou présentées pré-remplies et non modifiables ou présentées pour saisie. Une information typiquement masquée ou pré-remplie et non modifiable est le « Nom du compte » dont la valeur peut être définie entre la Marque Blanche et ASPOne.fr, afin notamment de simplifier le SSO ou d'éviter des doublons.

#### *2.2.3. Les contrôles*

Des contrôles clients sont réalisés en ligne.

- Vérification de la saisie des champs obligatoires et des champs dépendants du type de compte
- Contrôle de validité des champs numériques et alphanumériques est assurée ainsi que la longueur des champs.

### 2.3. Informations retournées par le portail ASPOne

En cas de succès on obtiendra en retour le détail complet de la configuration des alertes.

Toutes les téléprocédures auxquelles le compte est abonné sont remontées, mais on ne retourne que les MessageService qui sont actif.

# 3. ETUDE TECHNIQUE RECUPERATION DE LA CONFIGURATION DES ALERTES

## 3.1. Informations pour la récupération de la configuration

La seule information à fournir est le nom du compte.

## 3.1. Informations retournées par le portail ASPOne

En cas de succès on obtiendra en retour le détail complet de la configuration des alertes de la même manière que pour la modification.

# 4. ANNEXES

## 4.1. Message de service

Les ADS, ACS et ARS sont communs à toutes les téléprocédures.

### *4.1.1. AIS*

Les AIS (Avis d'Information Signé) concernent uniquement les téléprocédures suivantes :

| Téléprocédure | Type d'information |
|---|---|
| DUCS | Compte Rendu d'exploitation (CRE) |
| AED | Attestation Employeur Rematérialisée (AER) |
| DSN | Compte Rendu OPS<br>AER POLE-EMPLOI<br>… |
| REQUETE | Liste des locaux |
| OGA | Réponse FEC<br>Réponse Pièce Libre EPS<br>Réponse Pièce Libre ECCV<br>Réponse Question(s) ECCV |

Les autres téléprocédures ne font pas l'objet d'information / réponse complémentaire de la part de leurs destinataires.

### *4.1.2. RCP*

Les RCP (Réception de documents) concernent uniquement les téléprocédures / types de compte destinataire suivants :

| Téléprocédure | Type de compte |
|---|---|
| TVA | OGA<br>Tiers-Déclarant |
| TDFC | OGA<br>Tiers-Déclarant<br>Entreprise |
| PAIEMENT | OGA<br>Tiers-Déclarant |
| IR | GPA |
| OGA | Tiers-Déclarant<br>Entreprise |

Les autres téléprocédures ne sont pas concernées puisqu'elles sont à destination d'organismes, les comptes clients du portail ne peuvent donc pas en recevoir.