BANQUE DE FRANCE
DIRECTION DE L'ORGANISATION ET DES DÉVELOPPEMENTS
SDESS

GUICHET ONEGATE

Note technique sur les accréditations à ONEGATE
- Utilisateurs externes de la collecte ELAL -
Septembre 2010

1. Contenu du document

Le présent document fournit les informations nécessaires à une demande d'accréditation à ONEGATE :

- Une description de la procédure à suivre
- Les formulaires de demande d'accréditation

Une demande d'accréditation peut se faire pour deux types d'utilisateurs :

- **Une personne physique (remise U2A)**
- **Une application (remises A2A WebServices et remise A2A PESIT HORS SIT)**

Dans la suite du document les notions ci-dessous seront utilisées :

Déclarant	Personne morale assujettie aux déclarations de données à transmettre via ONEGATE
Demandeur	Personne physique qui effectue la demande d'accréditation via un formulaire pour des utilisateurs devant accéder à l'application ONEGATE
Utilisateur	Utilisateur de l'application ONEGATE

2. Demande d'accréditation de personnes physiques

2.1. Accréditation à l'application ONEGATE

Un utilisateur accrédité à ONEGATE se connectera au guichet à l'aide d'identifiants de connexion gratuits : un Login et un mot de passe. Il pourra alors, au travers de pages Web, effectuer des opérations de dépôt et de suivi de fichiers de données.

L'accréditation à ONEGATE peut se faire sur les deux environnements suivants :

- l'environnement de Production
- l'environnement d'Homologation (Tests Externes)

Voici le document à compléter pour obtenir vos identifiants de connexion à la plateforme :

accred_u2a_elal.doc

Il est composé des cadres suivants :

- **Demandeur :**
  Informations sur la personne effectuant la demande d'accréditation. Nous n'imposons aucune contrainte sur le statut de la personne effectuant la demande.
- **Accréditer des personnes physiques :**
  Noms des personnes auxquelles vous souhaitez donner accès à l'application pour effectuer des dépôts de fichiers déclaratifs ou en assurer le suivi.
  Si le demandeur souhaite aussi obtenir un accès à l'application, il doit préciser son nom dans le cadre.
  Les utilisateurs doivent renseigner leur login uniquement s'ils ont déjà un compte sur ONEGATE pour une autre collecte (exemple : SURFI)

  Remarque :
  Un utilisateur a le choix d'être accrédité à différents domaines de la collecte, à savoir :
  - M_CONTRAN (MCO)
  - M_TITTRAN (MTI)

Le formulaire devra être envoyé à **la Cellule Support ONEGATE** : onegate-support@banque-france.fr

Après accréditation dans l'application, l'équipe support transmettra au demandeur les identifiants et mots de passe des utilisateurs accrédités.

Remarque :
Un même utilisateur qui serait accrédité pour plusieurs établissements (à l'exception du cas particuliers des réseaux) devra transmettre autant de formulaires que d'établissements pour lesquels il est autorisé à intervenir, mais se verra attribué un login/mot de passe unique.

3. Demande d'accréditation pour une application (remise A2A)

Dans le cadre de ONEGATE, il vous est possible d'utiliser la remise A2A (télétransmission d'application vers application) pour l'envoi de vos fichiers déclaratifs vers le guichet.

Pour cela, vous devez disposer d'une application cliente pouvant effectuer des envois de fichiers vers ONEGATE de manière automatisée.

Deux types de remises A2A sont répertoriés :
- A2A WebServices
- A2A PESIT HORS SIT (PACIFIC)

Remarque :
Ce mode de remise est une possibilité de ONEGATE et est donc facultatif.

3.1. Accréditation à la remise A2A WebServices

ONEGATE offre la possibilité aux Déclarants d'automatiser le dépôt d'un fichier de données par le biais d'une application utilisant les WebServices. Ce canal est appelé A2A WebServices.

Avant de pouvoir utiliser ce dernier, il est nécessaire que le Déclarant dispose d'un certificat permettant l'authentification de l'application réalisant le dépôt auprès de la Banque de France.

Remarque :
Le certificat d'authentification logiciel est uniquement nécessaire dans le cadre de l'authentification d'une application.

3.1.1. Cas 1 : Vous souhaitez obtenir un certificat d'authentification logiciel

3.1.1.1. Demande de certificat

La Banque de France est une Autorité de Certification. Elle peut donc fournir un certificat d'authentification payant, à un Déclarant.

Pour ce faire, voici les deux formulaires de demande à compléter :

ONEGATE_Demande_Certificat_A2A_Web

Ils doivent ensuite être transmis à la **Cellule Support ONEGATE** : onegate-support@banque-france.fr

Après traitement de votre demande, vous recevrez de la Banque de France le lien vers l'interface de récupération de votre certificat. En vous connectant à cette dernière, vous pourrez récupérer les clés publiques et privées de votre certificat :

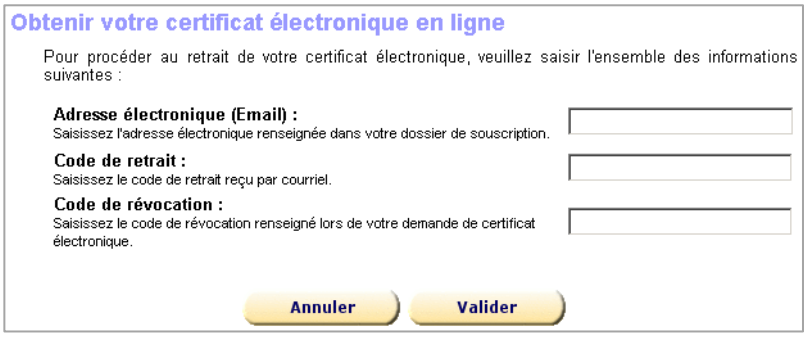

Figure 1 : Interface de récupération d'un certificat

La clé publique devra être fournie au moment de votre demande d'accréditation à l'application ONEGATE. Le format de fichier attendu est un fichier plat avec l'extension « .cer ». Ce format est celui issu du retrait en ligne.

3.1.1.2. Demande d'accréditation

La procédure à suivre est similaire à celle pour accréditer une personne physique (cf. point 2.1).
Le Demandeur devra renseigner le formulaire d'accréditation ci-dessous :

Formulaire_accreditation_A2A.doc

Dans la partie « **Accréditer des applications (Remise A2A WebServices)** » du formulaire, veuillez renseigner les informations suivantes :

- Désignation de l'application cliente (c.à.d. le nom de l'application)
- Insérer la clé publique de votre certificat d'authentification

Après traitement de votre demande, la Cellule Support ONEGATE vous transmettra des identifiants de connexions qui vous permettront de suivre vos dépôts sur le guichet.

3.1.2. Cas 2 : Vous disposez d'un certificat d'authentification

Un certificat d'authentification simple émis par une Autorité de Certification reconnue par la CFONB est suffisant pour utiliser le mode de remise A2A WebServices de ONEGATE.

Attention :
Ce certificat doit être différent de celui que vous utilisez pour signer électroniquement vos fichiers déclaratifs. En effet, ces deux utilisations différentes d'un même certificat pourraient entrer en conflit.

Pour votre information, voici la liste des Autorités de Certification (AC) référencées pour les échanges entre établissements et sphère financière :

AC référencée	Famille de certificat	Point de contact de l'AC
Banque de France	Certificat d'Authentification	e-mail : certificats@banque-france.fr
BNP Paribas Authority Entreprise	Net Identity	e-mail : claudine.huard@bnpparibas.com
Crédit Agricole CA Certificat	CA Certificat	e-mail : support.ca-certificat@ca-cedicam.fr
Crédit Agricole Interne	e-badge	Service non commercialisé
CNCE interne	CE Certification (ATOS Mediacert)	Service non commercialisé
Chambersign	Fiducio	e-mail : commercial@chambersign.tm.fr
Certinomis	CertiPoste, classe 3+	e-mail : service.commercial@certinomis.com
LCL	Authentys Entreprise	e-mail : contact@certification.lcl.fr
Click & Trust Banque Populaire	Mercantéo	e-mail : contact-commercial@click-and-trust.com
Natixis	CES@MOR	e-mail : cesam@natixis.fr
Société Générale	SG TRUST SERVICES	e-mail : support@sgtrustservices.com
Caisse des Dépots	Legalia	e-mail : cedric.clement@caissedesdepots.fr

Figure 2 : Liste des AC reconnues par la Banque de France

Si votre certificat d'authentification simple suit les conditions énoncées ci-dessus, référez vous au point 3.1.1.2 pour accréditer votre application à ONEGATE.
Dans le cas contraire, il vous faut suivre la procédure décrite au point 3.1.

3.2. Accréditation à la remise A2A PESIT HORS SIT (PACIFIC)

Pour les sociétés disposant **déjà** d'une connexion PESIT HORS SIT avec la Banque de France, il est possible de la réadapter pour l'envoi de données vers ONEGATE

Pour ce faire, voici le formulaire à retourner à la **Cellule Support ONEGATE** :

ONEGATE_PESIT.DOC

Pour les **nouveaux** utilisateurs souhaitant mettre en place le canal PESIT HORS SIT, veuillez contacter la Cellule Support ONEGATE pour mise en œuvre de la procédure.

Pour toute information complémentaire sur la remise A2A, vous pouvez vous reporter à la Note Technique sur les Modalités d'échanges A2A.