Contrat d’Interface Remettant

Collecte DSS – Droit à Signer SOLVA2

**Correspondants Banque de France**

**Correspondant Métier**

support-s2-assurances@acpr.banque-france.fr

**Direction de l'Organisation et des Développements**

Service de Développement pour les Études, les Statistiques et la Supervision bancaire (SDESS)

OneGate-support@banque-france.fr

# Table des matières

[Table des matières 3](#_Toc137121827)

[1 Introduction 4](#_Toc137121828)

[1.1 Définition des termes 4](#_Toc137121829)

[2 Périmètre de la collecte 4](#_Toc137121830)

[2.1 Contexte 4](#_Toc137121831)

[2.2 Fréquence de remise des états 4](#_Toc137121832)

[3 Principes d’accréditation d’un remettant 4](#_Toc137121833)

[3.1 Accréditation de personnes physiques (remises U2A) 5](#_Toc137121834)

[3.2 Accréditation d’une application (remises A2A) 5](#_Toc137121835)

[4 Fonctionnement de la collecte 5](#_Toc137121836)

[4.1 Canaux de transmission 5](#_Toc137121837)

[4.2 Description de la transmission via un fichier XML 6](#_Toc137121838)

[4.2.1 Remise par fichier XML 6](#_Toc137121839)

[4.3 Spécification du fichier XML attendu en entré de OneGate 7](#_Toc137121840)

[4.4 Spécifications des champs de la têtière (Administration) 9](#_Toc137121841)

[4.5 Spécifications des champs des rapports du domaine DSS 9](#_Toc137121842)

[4.5.1 La balise <Report> 9](#_Toc137121843)

[4.5.2 La balise <Data> 10](#_Toc137121844)

[4.5.3 Description des balises <Item> du Formulaire DDAS\_SOLVA 10](#_Toc137121845)

[4.6 Exemples de fichier de remise et XSD de fichier en entré de ONEGATE 11](#_Toc137121846)

[4.6.1 Exemple de fichier XML d’entrée : 11](#_Toc137121847)

[4.6.2 XSD de fichier en sortie de OneGate : 12](#_Toc137121848)

[5 Contrôle des collectes 13](#_Toc137121849)

[5.1 Les différents niveaux de contrôles 13](#_Toc137121850)

[5.1.1 Format des restitutions 13](#_Toc137121851)

[5.1.2 Outils recommandés pour visualiser le fichier XML 13](#_Toc137121852)

[6 Annexes 14](#_Toc137121853)

# Introduction

L’objet de ce document est de fournir aux établissements déclarants et à leurs maîtrises d’œuvre, les règles de gestion et normes de transmission de données de la collecte DSS au travers du guichet OneGate.

## Définition des termes

Les termes définis ci-dessous sont utilisés dans la suite du document :

|  |  |
| --- | --- |
| Remettant | Acteur autorisé à déposer des fichiers pour lui-même ou pour le compte de tiers |
| Déclarant | Acteur assujetti à une obligation de déclaration (Mobilisateur pour l’Acte de remise et/ou le déclarant individuel pour le bordereau d’information) |
| Utilisateur BdF | Utilisateur (personne physique) accrédité au sein de la Banque de France, pour réaliser des opérations d’administration ou de suivi sur le guichet et destinataire des déclarations |

# Périmètre de la collecte

## Contexte

Le périmètre des données collectées dans le cadre de la collecte des droits à signer consiste à déclarer des signataires par déclarant et par domaine en déclarant via une interface de saisie en ligne.

## Fréquence de remise des états

Ce formulaire a une périodicité annuelle et ouverte du 01 janvier au 31 décembre avec le format YYYY-12. Il sera possible d’accéder à ce formulaire à tout moment pour le modifier (modification, réinitialisation, réouverture et fermeture du formulaire).

# Principes d’accréditation d’un remettant

La phase d'accréditation permet de vérifier si les remettants sont bien habilités par les déclarants à échanger des informations avec la Banque de France. L'accréditation à ONEGATE est une procédure obligatoire sans laquelle il n'est pas possible de remettre des déclarations à la Banque de France.

L'accréditation ne concerne que les remettants.

Les règles générales permettent d'assurer la cohérence du futur système d'information :

- Aucune remise ne sera acceptée d’un remettant non accrédité à OneGate.

- Si un remettant, accrédité à OneGate, remet des déclarations relatives à des déclarants pour lesquels il n’a pas été accrédité, celles-ci seront rejetées.

ONEGATE permet deux types d’accréditation:

• Une personne physique (remise U2A)

• Une application (remise A2A)

## Accréditation de personnes physiques (remises U2A)

Pour pouvoir effectuer une remise U2A il suffit d’avoir un accès (avec un identifiant et mot de passe) sur le portail ONEGATE.

Pour avoir un accès à la collecte Droits À Signer banque il faut cliquer sur « je n’ai pas de compte » sur la page ONEGATE <https://onegate.banque-france.fr> et demander une accréditation pour la collecte SOLVA.

Si le remettant a déjà un compte sur l’application ONEGATE, mais ne possède pas d’accréditations pour la collecte SOLVA, il peut alors effectuer une « extension de droits » pour cette collecte via l’onglet « Profil ».

## Accréditation d’une application (remises A2A)

ONEGATE permet les remises A2A (télétransmission automatisée d’application vers application) à travers l’envoi de fichiers déclaratifs vers le guichet. Cet envoi s’effectue à travers une application cliente qui procède à l’alimentation de SOLVA de manière automatisée.

Deux types de remises A2A sont répertoriés :

* A2A WebServices
* A2A PESIT HORS SIT

Ci-dessous la Note Technique sur les Modalités d’échanges A2A

[Notice technique modalité de remise par télétransmission](https://www.banque-france.fr/sites/default/files/media/2018/10/19/onegate-note_technique_modalites_echanges_v3.7.docx)

# Fonctionnement de la collecte

La collecte DSS fonctionne par saisie en ligne. Il est également possible de faire une remise par chargement de fichier XML en A2A ou U2A.

## Canaux de transmission

Dans le contexte de la collecte SOLVA Droits À Signer, les canaux de transmission utilisés via le guichet ONEGATE seront :

- Canal U2A – Chargement des fichiers « Clé publique du certificat » via la « Saisie en ligne »

- Canal U2A – Chargement de fichier XML

- Canal A2A – Télétransmission de fichiers XML

Le contrat d’interface remettant va spécifier le fichier XML de remise.

## Description de la transmission via un fichier XML

### Remise par fichier XML

Une remise par fichier XML comporte les données déclarées :

* Pour un seul et même déclarant,
* Pour le seul domaine DSS

L’utilisation de fichier XML donne beaucoup de souplesse aux documents qui sont remis. En effet, les données ne sont pas contenues dans des zones fixes (avec l’obligation de remplir la zone), mais dans des champs (entourés de balises XML).

Lors des contrôles effectués en réception par ONEGATE, les fichiers présentant une ou des anomalie(s) sont rejetés (règle de validation non respectée, fichier mal structuré). Ils doivent alors faire l'objet d'un nouvel envoi après correction.

#### Mode de chargement

Le mode par défaut de chargement du fichier XML est en mode "annule et remplace" : les anciennes données sont remplacées intégralement par les nouvelles. Ce mode de chargement est valable pour un déclarant, un domaine, un rapport et une période donnée.

#### Format et règle générale de codage des champs

Les règles de codage des champs constituant les enregistrements des fichiers de collecte sont à respecter strictement :

* Zone alphanumérique : tous les caractères sont autorisés et la saisie peut être en majuscule ou en minuscule ; les caractères accentués sont autorisés.
* Les champs non renseignés (i.e. valeur vide) ne devront pas apparaître dans les fichiers XML.
* En cas de modification/complément d'une information (correction), un nouveau fichier doit être adressé avec cette modification pour un déclarant, un domaine, un rapport et une période de référence.
	+ - Par défaut le fichier est envoyé en mode « annule et remplace » :

Nb : Sera consultable sur l’IHM ONEGATE que :

* + - Dans le cas d’un annule et remplace, l’image de son dernier dépôt pour un domaine/rapport/arrêté donné

## Spécification du fichier XML attendu en entré de OneGate

Chaque fichier XML de remise se compose de deux parties obligatoires :

* La têtière, qui contient les données d’administration (date de création du fichier, remettant, etc.)
* Cette partie est unique dans le fichier XML
* Le rapport incluant les données de collecte (certificat, identité du signataire, type de reporting)

Pour les remises ONEGATE, le format de fichier doit suivre les instructions ci-dessous :

Les données collectées au format XML sont enveloppées par la balise <DeclarationReport> contenant :

* La balise <**Administration**> correspond à la têtière ONEGATE
* La balise <**Report**> correspond au rapport contenant données de la collecte

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><**DeclarationReport** xmlns="http://www.onegate.eu/2010-01-01"><**Administration** creationTime="AAAA-MM-JJTHH:MM:SS.CCC+GMT"><From declarerType="LEI">XXXXXXXXXXXXXXXXXXXX</From><To>BDF</To> <Domain>DSS</Domain><Response feedback="true"> <Email>mail\_emetteur@xxxx.fr</Email> <Language>FR</Language></Response>**</Administration>**<**Report** date="AAAA" code="DSS" close="true" >*<Data form="* DDAS\_SOLVA*">**<Item>**Données XML**</Item>**</Data>*</**Report**>*…*</**DeclarationReport** |

*Format de fichier*

## Spécifications des champs de la têtière (Administration)

Le tableau suivant présente le détail des différents champs de la têtière :

|  |  |  |
| --- | --- | --- |
| Champs | Obligatoire (O) Facultatif (F) | Description |
| <creationTime> | F | C’est l’attribut de la balise <Administration qui reprend la date de création du fichier (Exemple: 2016-08-25T11:03:09.488). Ce champ peut être généré automatiquement par l’application émettrice. |
| <From> | O | Cette balise représente le déclarant. Pour la collecte DSS le code LEI est la seule valeur possible (donnée alphanumérique de longueur 20). |
| <To> | O | Identifiant qui caractérise le guichet ONEGATE. La valeur est fixe : « BDF». |
| <Domain> | O | Représente le code de la collecte auquel l’instance fait référence. Ses valeurs sont sur trois caractères. Pour la collecte DSS le code est «DSS » |
| <Response> | O | Contient l’adresse de l’émetteur et le langage de l’avis de dépôt. Une balise à « true » ou « false » indique respectivement si le destinataire souhaite être informé ou non par e-mail dès réception par le guichet du fichier.Dans le cas de l’utilisation de la valeur « false », les balises <Email> et <Language> ne doivent pas apparaître au sein des balises <Response>. La balise <Email> peut contenir uniquement une seule adresse mail.**Recommandation**: il est recommandé d’utiliser une adresse email générique dédiée aux échanges avec ONEGATE. |

## Spécifications des champs des rapports du domaine DSS

Le domaine « Droit à signer Solva2» (DSS) contient 1 seul rapport : DSS

### La balise <Report>

La balise <Report> correspond au nom du rapport des données à collecter pour une date d’arrêté donnée. Elle contient plusieurs attributs :

#### Rapport DSS:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Propriétés | TYPE(\*) | Libelle affiché | Longueur maximum | O/F | Commentaires |
| Code | AN | DSS | / | O | Le code rapport est: « DSS» |
| Date | DATE | Date d’arrêté | / | O | La date de déclaration correspond à la date d’arrêté. Elle doit être sous le format « AAAA ». |

### La balise <Data>

Les différents rapports contiennent les formulaires définis par la balise <Data>. Cette balise contient les attributs suivants :

#### Formulaire DDAS\_SOLVA:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Propriétés | TYPE(\*) | Libelle affiché | Longueur maximum | O/F | Commentaires |
| form | AN | Déclaration des droits à signer SOLVA2 | / | O | Le code formulaire est: « DDAS\_SOLVA» |

### Description des balises <Item> du Formulaire DDAS\_SOLVA

#### Description des balises <Item> de la section « Déclaration des droits à signer SOLVA2 »

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Balise XML | Description | TYPE(\*) | LONG-UEURMAX | Obligatoire (O)Facultatif(F) | COMMENTAIRES |
| CERTIFICAT | Fichier | AN | / | O | Nom du fichier avec une extension en .cer |
| NOM | Nom du titulaire du certificat  | AN | / | O | / |
| PRENOM | Prénom du titulaire du certificat | AN | / | O | / |
| DOMAINE\_S2P | Solvabilité 2 Prudentiel (S2P) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_BLA | Blanchiment Assurance (BLA) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_ SBS | Collectes Bureautiques Signées (SBS) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_ SNX | RAN (SNX) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_ CCA | Commissaires aux comptes Assurance (CCA) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_ RPX | Collectes xbrl ORPS (RPX) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_ RPS | Collectes Bureautiques ORPS Signées (RPS) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| DOMAINE\_ DBA | Collecte bureautique Blanchiment (DBA) | AN | / | O | Liste déroulante avec deux choix - Oui- Non |
| Documents | / | / | / | O | La balise <Documents></Documents> permet d’encapsuler le fichier de signature chargé. Elle contient la balise <Doc prop="CERTIFICAT"> </Doc> |
| <Doc prop=<"CERTIFICAT"> | Fichier  | AN | / | O | Ce champ contiendra le fichier clé publique (préalablement exporté en base 64) encapsulé en base 64\* du certificat personnel de la personnePrécisions en annexe 2. |

\*pour précision, il est nécessaire d’insister sur le fait que l’export de la clé publique en base 64, et l’encapsulation nécessaire en base 64 afin d’être intégré dans la balise XML sont deux actions indépendantes.

## Exemples de fichier de remise et XSD de fichier en entré de ONEGATE

### Exemple de fichier XML d’entrée :

Exemple de demande d’habilitation à signer avec le modèle de signature détachée associée.





### XSD de fichier en sortie de OneGate :



# Contrôle des collectes

Les contrôles sont effectués d’une part, par le guichet ONEGATE, à la réception des documents, pour vérifier l’intégrité physique et la conformité des fichiers et des données transmis, d’autre part par le service gestionnaire de la collecte au sein de la Banque de France. Les éléments de contrôles liés à l’intégrité physique, la conformité et la structure des fichiers ainsi qu’au référentiel sont retransmis aux remettants *via* le guichet ONEGATE. Les contrôles des données métiers sont également retransmis via le guichet ONEGATE sous forme de Compte Rendu de Collecte (CrC).

Pour limiter au minimum les rejets, il est nécessaire que les contrôles soient effectués également par les remettants lors de l'élaboration des fichiers.

Les contrôles sont précisés pour chacun des rapports.

## Les différents niveaux de contrôles

Les contrôles sont de quatre types :

* Contrôles de **conformité** du fichier (exemple : contrôle de conformité XML)

Le non-respect entraîne un rejet systématique du fichier remis.

* Contrôles de **structure** (exemple : par rapport à un schéma XSD pour un fichier XML)

Le non-respect entraîne un rejet systématique du fichier remis.

* Contrôles de **référentiel** (exemple : vérification d’une donnée par rapport à un référentiel, contrôle d’un champ obligatoire). Le non-respect des contrôles de référentiel est bloquant et entraîne un rejet du fichier remis.
* Contrôles de **format** (exemple : tous les montants sont exprimés sans décimale et strictement positifs ; contrôle de doublons)

Des contrôles métiers sur la qualité des données (contrôle de cohérence temporelle) ne seront pas bloquants mais entraîneront des comptes rendus d’anomalies adressés aux remettants.

Ces contrôles étant partagés entre le guichet ONEGATE et l’application du service gestionnaire de cette collecte (« métier »), plusieurs comptes rendus sont susceptibles d’être restitués. Les comptes rendus de traitement ONEGATE sont déposés sur le guichet ONEGATE.

### Format des restitutions

L’accusé de réception et compte-rendu du guichet sont envoyés à l’adresse e-mail mentionnée dans le fichier XML uploadé.

### Outils recommandés pour visualiser le fichier XML

Il est recommandé d’utiliser  Notepad++ <http://notepad-plus-plus.org/fr/> (logiciel libre et gratuit) pour visualiser les fichiers.

# Annexes

Annexe 1 : Liste des abréviations

|  |  |
| --- | --- |
| Abréviation | Signification |
| N | Numérique |
| AN | Alphanumérique |
| O | Obligatoire |
| F | Facultatif |

Annexe 2 : Précision sur l’encapsulation en base 64 d’un fichier.

Ci-dessous le contenu d’un fichier avec l’unique chaine de caractères suivante :

|  |
| --- |
| <Exemple> |

L’encapsulation en base 64 de ce fichier donne le résultat ci-dessous :

|  |
| --- |
| PEV4ZW1wbGU+ |

C’est ce résultat d’encapsulation en base 64 du fichier de clé publique du certificat (elle-même exportée en base 64) qui doit être intégré dans la balise XML <Doc prop="CERT"> correspondante.