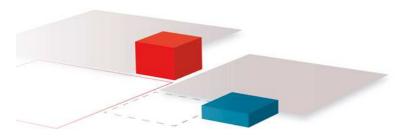


Version: 1.02 Date: 07/08/2015



Direction des Services bancaires



Transfert des avoirs en application de la Loi Eckert

Cahier des charges technique

Signature électronique



Version : 1.02 Date : 07/08/2015

Suivi des modifications

Version	Date	Auteur	Contenu
V1.00	09/06/2015	B. Touchon	Version validée et diffusée
V1.01	18/06/2015	B. Touchon	Modification de l'exemple de fichier signé
V1.02	07/08/2015	B. Touchon	Correction des contrôles CS21 et CS30.



Version : 1.02 Date : 07/08/2015

Documentation associée

Réf.	Nom du document	Descriptif		
	Banque: C048_CCH_CICLADE_CC_Techni que_Bancaire_V2.04.pdf			
00	Assurance: C049_CCH_CICLADE_CC_Techni que_Assurance_V2.04.pdf	Cahier des charges technique du projet CICLADE.		
	Teneurs de compte conservateurs : C058_CCH_CICLADE_CC_Techni que_Teneurs_De_Comptes_Conse rvateurs_V2.04.pdf			
01	XAdES 1.4.1	XML Advanced Electronic Signatures http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04 .01_60/ts_101903v010401p.pdf Référence: ETSI TS 101 903 Version 1.4.1 Date: juin 2009		
02	XAdES W3C	XML Advanced Electronic Signatures http://www.w3.org/TR/XAdES/ Date: W3C Note 20 February 2003		
03	XMLDSIG W3C	XML-Signature Syntax and Processing http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/ Date: W3C Recommendation 12 February 2002		
04	PAC-CFONB	La politique d'acceptation commune (PAC) http://www.cfonb.org/Default.aspx?lid=1&rid=122&rvid=148		



Version: 1.02 Date: 07/08/2015

Réf.	Nom du document	Descriptif
		Spécification de l'ETSI concernant les algorithmes utilisables dans le contexte des signatures électroniques avancées
05	ALGO-ETSI	http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02. 01.01_60/ts_10217601v020101p.pdf
	7,200 210.	Référence : ETSI TS 102 176-1
		Version 2.1.1
		Date : novembre 2011
		Exclusive XML Canonicalization
06	Canonicalisation exclusive W3C	http://www.w3.org/TR/xml-exc-c14n/ Date: W3C Recommendation 18 July 2002



Version : 1.02 Date : 07/08/2015

Sommaire

1.	INT	RODUCTION	6
	1.1.	Objectif de ce document	6
	1.2.	Pré requis	6
	1.3.	Rappel du besoin	7
2.	SIG	NATURE – GENERALITES	8
	2.1.	Principes généraux de XADES	8
	2.2.	Rappel des principes de la signature électronique	8
	2.3.	Définitions	9
	2.4.	Pré requis avant la transmission d'un fichier signé	10
3.	SIG	NATURE - Principes retenus dans le cadre du projet CICLADE	11
	3.1.	Documents visés	11
	3.2.	Type de signature	11
	3.3.	Signature optionnelle	12
	3.4.	Signature intégrale	12
	3.5.	Nombre de signatures sur le document	12
	3.6.	Certificats autorisés	12
	3.7.	Choix d'algorithmes	12
4.	SIG	NATURE – CONTROLES EFFECTUES PAR LA CDC	13
	4.1.	Contrôles liés à l'implémentation de la signature par la CDC dans le cadre du projet CICLADE	15
	4.2.	Contrôles liés la validation de la signature du fichier	15
	4.3.	Contrôles liés au certificat et à la chaine de certification	16
5	SIG	NATURE - Exemple	17



Version: 1.02 Date: 07/08/2015

1. INTRODUCTION

1.1. Objectif de ce document

Ce document spécifie le format de signature XAdES (XML Advanced Electronic Signatures) à utiliser, par les établissements (le(s) « Etablissement(s) ») tenus de déposer à la Caisse des Dépôts les sommes provenant des comptes bancaires inactifs ou contrats d'assurance-vie ou bons ou contrats de capitalisation en déshérence tels que définis par la loi n°2014-617 du 13 juin 2014 relative aux compt es bancaires inactifs et aux contrats d'assurance vie en déshérence, pour transférer à la Caisse des Dépôts les fichiers comportant les informations afférentes à ces comptes, contrats ou bons.

Ce format s'appuie sur les spécifications XAdES de l'ETSI (en version 1.4.1). Le présent document n'a pas vocation à redéfinir ces formats, mais à en préciser les modalités de mise en œuvre dans le contexte indiqué ci-dessus.

Le présent document vient en complément du document référencé 00 ci-dessus.

Il est organisé comme suit :

- le chapitre de présentation générale précise le périmètre et les grands principes de la spécification,
- le chapitre suivant contient les spécifications techniques du format, ainsi que quelques éléments techniques ayant un but didactique sur l'implémentation de la signature électronique dans le cadre des échanges avec la Caisse des Dépôts.

Ce document est commun à tous les types d'établissements, contrairement au document référencé 00 qui varie selon que l'Etablissement est un établissement bancaire, un organisme d'assurance ou un teneur de compte-conservateur.

1.2. Pré requis

L'Etablissement doit avoir pris connaissance, au préalable, du document référencé 00 ci-dessus.

Pour la bonne compréhension des éléments techniques du présent document, il est nécessaire que l'Etablissement ait une bonne connaissance des langages XML et XML Schéma (XSD), ainsi que des formats de signature électronique XML définis par le W3C : XMLDSig (cf. référence 03 ci-dessus) et XAdES (cf. référence 01 ci-dessus).

Les grands principes liés à la signature électronique, rappelés ci-dessous (cf. chapitre 2.2), sont également à maitriser.



Version: 1.02 Date: 07/08/2015

1.3. Rappel du besoin

Le besoin a été exprimé lors de l'atelier de travail, organisé par le CFONB, le 06 mai 2015, et consigné dans le compte rendu de cette réunion, diffusé le 12 mai 2015 :

Le besoin des banques est le suivant : afin de garantir l'intégrité des données de bout en bout, il est proposé de signer les fichiers dans le SI des banques dès leur constitution et avant le transfert à la CDC.

Ce besoin, de garantir l'intégrité des données du fichier déposé, entre sa création et son dépôt dans l'applicatif de la CDC, est transposable à tous les autres types d'établissements (organismes d'assurance, teneurs de compte conservateurs).



Version : 1.02 Date : 07/08/2015

2. SIGNATURE - GENERALITES

2.1. Principes généraux de XADES

Cette spécification repose sur un empilement de trois socles techniques : XML, XML-DSIG et XAdES.

XML Advanced Electronic Signatures (XAdES) est une norme conçue par l'European Telecommunications Standards Institute (ETSI) pour permettre une mise en conformité des signatures électroniques avec la Directive 1999/93/EC du Parlement Européen et du Conseil du 13 décembre 1999 sur le cadre communautaire des signatures électroniques. Cette norme offre une boite à outils permettant la mise en œuvre de signatures électroniques valables sur de longues durées.

XAdES est appliquée comme une surcouche à XML-DSIG.

La référence à utiliser dans le cadre du présent document est définie dans une note du W3C (voir [XADES-W3C] – Référence 01 ci-dessus) expliquant les différents niveaux de signature XAdES (XAdES, XAdES-T, XAdES-C) :

- Le premier niveau (XAdES) est requis
- Les autres niveaux (XAdES-T, XAdES-C, etc.) ne sont pas exploités dans la version actuelle du SI de la CDC mis en œuvre dans le cadre du projet CICLADE.

2.2. Rappel des principes de la signature électronique

Les principes de la signature électronique à maîtriser sont :

- 1) les grands concepts de cryptographie et de condensat (fonction de hachage, http://fr.wikipedia.org/wiki/Fonction_de_hachage) et leur application dans le domaine des signatures électroniques,
- 2) le concept d'indirection via condensat (voir la relation entre les balises Reference (http://www.w3.org/TR/xmldsig-core/#sec-Reference) et SignatureValue (http://www.w3.org/TR/xmldsig-core/#sec-SignatureValue)) et le concept de canonicalisation XML, qui sont des concepts fondamentaux de la norme XMLDSig (voir [XMLDSIG-W3C] Référence 02 ci-dessus) utilisée pour la signature des fichiers déposés,
- 3) L'Etablissement doit pouvoir émettre des signatures électroniques, mais également les valider et effectuer une analyse initiale en cas d'anomalie de signature.



Version: 1.02 Date: 07/08/2015

2.3. Définitions

Ce paragraphe liste les définitions propres à cette spécification. Ces définitions n'ont pas vocation à être utilisées dans d'autres contextes.

Document signé: ensemble de données, disponible sous forme d'un fichier, comprenant un contenu et une ou plusieurs signatures électroniques.

Composant d'un document: partie d'un document qui peut être disponible de manière indépendante, par exemple le contenu du document ou un sous-ensemble du document, ou encore une signature.

Contenu du document: ensemble de données initiales du document, disponible sous forme d'un fichier, pouvant faire l'objet d'une unique signature.

Signature: données garantissant l'intégrité et l'authenticité d'un composant du document. La partie du document concernée comprend la totalité du contenu du document.

Signature XML-DSIG: signature créée selon les règles du standard [XML-DSIG].

Mécanisme de hachage ou de condensation: opérations cryptographiques qui permettent à partir de données de taille quelconque d'en déduire une empreinte de taille fixe caractéristique de l'intégrité des données initiales.

Ces opérations sont conçues afin qu'il soit impossible de trouver deux jeux de données ayant même résultat.

Données hachées: résultat obtenu par application d'un mécanisme de hachage sur des données.

Partie signée: ensemble de données qui ont été utilisées en entrée d'une opération de condensation (application d'un mécanisme de hachage) dont le résultat final (hash ou condensat) est utilisé en entrée d'un mécanisme de signature. Une partie signée peut inclure des parties signées implicitement.

Partie signée implicitement: une partie signée peut inclure des données hachées. Les données à l'origine font alors implicitement partie des données signées du fait des propriétés des mécanismes de hachage. Il est ainsi possible de signer implicitement des arborescences de données.



Version: 1.02 Date: 07/08/2015

2.4. Pré requis avant la transmission d'un fichier signé

Avant le premier envoi d'un fichier signé par un Etablissement, celui-ci doit indiquer à la CDC les éléments qui permettront de vérifier que l'autorité de certification est bien recensée.

Pour cela, l'Etablissement doit communiquer l'identifiant OID (Object Identifier) désignant cette autorité de certification

Les modalités de communication de cet identifiant seront indiquées ultérieurement sur le site déposant (CDC-Net).

A titre d'illustration, le tableau ci-dessous est extrait de la liste des autorités de certification référencées PAC niveau 1. L'OID est affiché dans la cinquième colonne du tableau.

	Liste des Autorités de Certification et Familles de certificats référencées PAC niveau 1						
Date Référencement ou du renouvellement	Date Fin de Référencement PAC	Nom du PSCE	NOM Commercial	OID	Référentiel PAC RGS versions en cours	Autres Référentiels PAC	Usage
22/05/14	16/05/16	CERTINOMIS	DEMATERIALISATION	1.2.250.1.86.2.2.1.10.1		RGS 0.98 (1)	Authentification/Signature
22/05/14	N/A	DHIMYOTIS	Certigna RGS * Pro	1.2.250.1.177.1.9.1.5	RGS v1.0		Authentification/Signature
22/05/14	N/A	CLICK AND TRUST	ADMINEO RGS	1.2.250.1.98.1.1.20.1.1.1	RGS v1.0		Authentification/Signature
22/05/14	N/A	CLICK AND TRUST	ADMINEO RGS	1.2.250.1.98.1.1.20.1.1.2	RGS v1.0		Authentification
22/05/14	N/A	CLICK AND TRUST	ADMINEO RGS	1.2.250.1.98.1.1.21.1.1.1	RGS v1.0		Signature
03/11/14	N/A	CERTINOMIS	Easy CA	1.2.250.1.86.2.3.1.1.1	RGS v1.0		Authentification
03/11/14	N/A	CERTINOMIS	Easy CA	1.2.250.1.86.2.3.1.10.1	RGS v1.0		Authentification/Signature
03/11/14	N/A	CERTINOMIS	Easy CA	1.2.250.1.86.2.3.1.2.1	RGS v1.0		Signature



Version: 1.02 Date: 07/08/2015

3. SIGNATURE - Principes retenus dans le cadre du projet CICLADE

3.1. Documents visés

Les documents visés sont les fichiers déposés tels que spécifiés dans le cadre du document référencé 00 ci-dessus.

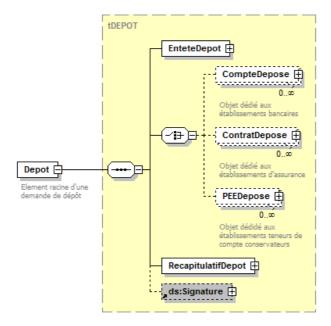
3.2. Type de signature

La signature sera enveloppée dans le document signé.

Un élément, nommé ds : Signature, a été ajouté au format d'échange décrit dans le cadre du document référencé 00 ci-dessus.

Rappel des 3 types de signatures :

- les signatures enveloppant le contenu du document,
- les signatures enveloppées dans le document (type retenu dans le cadre du présent document),
- les signatures détachées du contenu du document,





Version: 1.02 Date: 07/08/2015

3.3. Signature optionnelle

La signature reste optionnelle. L'Etablissement peut choisir de déposer un fichier signé ou non signé. Ce choix est effectué lors de l'adhésion de l'Etablissement au site déposant (CDC-Net).

Les contrôles liés au choix de cette option sont intégrés dans le document référencé 00 (voir contrôles CS00 et CS99).

3.4. Signature intégrale

La signature porte sur l'intégralité des données fonctionnelles du document, donc sur tout le contenu du document (et non seulement sur une partie du document).

3.5. Nombre de signatures sur le document

Une seule et unique signature est attendue.

3.6. Certificats autorisés

La signature pourra uniquement être réalisée à partir de certificats X509 générés par une autorité de certification recensée dans le cadre de la PAC (voir [PAC-CFONB] - Référence 03 ci-dessus).

Ces certificats peuvent être personnels (délivrés à une personne physique par l'autorité de certification) ou « serveurs » (délivrés à une personne morale par l'autorité de certification).

Sont donc exclus les certificats auto-générés par l'Etablissement.

Remarque : des contrôles sont prévus sur ces certificats par la CDC, notamment pour en vérifier la validité (cf. infra point 4). Les contrôles de date sont effectués à la réception du fichier par la CDC, et non à la date de génération par l'Etablissement de ce fichier.

3.7. Choix d'algorithmes

L'algorithme de création de la signature (correspondant à une signature enveloppée) est fixé à : <ds:Transforms Algorithm = "http://www.w3.org/2001/xmldsig#enveloped-signature#"/>

L'algorithme de mise sous forme canonique est fixé à :<ds:CanonicalizationMethod Algorithm = "http://www.org/2001/10/xml-exc-c14n#"/>

Commentaire [TB1]: Correctif V1.02

L'utilisation de tout autre algorithme est à proscrire.



Version: 1.02 Date: 07/08/2015

4. SIGNATURE - CONTROLES EFFECTUES PAR LA CDC

Dans le cadre du document référencé 00, il est indiqué que des contrôles seront opérés par la CDC sur les composantes de la signature du fichier (cf. chapitre 5 .4 du document référencé 00).

Ces contrôles sont listés ci-après et détaillés aux points 4.1, 4.2 et 4.3.

Contrôles spécifiques liés à l'implémentation de la signature dans le contexte CICLADE

- Format du certificat (X509)
- Conformité des algorithmes utilisés

Contrôles de la signature

- Comparaison du certificat communiqué et du certificat utilisé pour signer le fichier
- Contrôle de l'intégrité du fichier.

Contrôles certificat et chaine de certification

- validité
- usage
- liste de confiance
- autorité de certification connue



Version: 1.02 Date: 07/08/2015

Rappel des caractéristiques générales de ces contrôles

Caractéristiques générales des contrôles :

- Ils sont réalisés uniquement si le fichier est signé (présence d'une balise ds : Signature)
 Ils permettent de vérifier la validité des éléments fournis dans le cadre de la signature électronique du fichier
- · Ces contrôles sont bloquants

En cas d'anomalie :

- Le traitement est stoppé (les contrôles suivants ne sont pas déroulés)
- · Le fichier est rejeté dans sa totalité
- Le fichier est supprimé
- Un compte rendu d'anomalie précise les causes du rejet du fichier
 L'utilisateur du service est invité à corriger et à renvoyer le fichier

En l'absence d'anomalie :

- Le fichier est jugé conforme et ne sera pas rejeté.
- Les contrôles de niveau en tête sont mis en œuvre (cf. document référencé 00).



Version : 1.02 Date : 07/08/2015

4.1. Contrôles liés à l'implémentation de la signature par la CDC dans le cadre du projet CICLADE

Erreur bloquante – le format du certificat n'est pas conforme.						
Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – le certificat n'est pas au format X509, seul format supporté par la CDC. »						
Erreur bloquante – la signature du fichier n'est pas conforme car les algorithmes utilisés ne sont pas ceux qui sont spécifiés dans le présent document.						
Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – un algorithme utilisé pour générer la signature du fichier n'est pas conforme aux spécifications de la CDC ».						
Si le problème vient de l'algorithme de canonicalisation :						
Libellé complémentaire : « L'algorithme de canonicalisation à utiliser est : http://www.org/2001/10/xml-exc-c14n# »						
Si le problème vient de l'algorithme de signature :						
Libellé complémentaire : « L'algorithme de signature à utiliser est : http://www.w3.org/2001/04/xmldsig-more#rsa-sha256»						
Si le problème vient de l'algorithme de calcul d'empreinte :						
Libellé complémentaire :						
« L'algorithme de calcul d'empreinte à utiliser est : http://www.w3.org/2001/04/xmlenc#sha256»						

Commentaire [TB2]: Complément V1.02

4.2. Contrôles liés la validation de la signature du fichier

Numéro Contrôle	Libelle d'alerte
CS30	Erreur bloquante – la signature du fichier n'est pas conforme car le certificat présenté n'est pas celui qui a été utilisé pour signer le document, ou car le contenu du fichier a a été altéré.
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – le certificat présenté n'est pas celui qui a été utilisé pour signer le fichier, ou car le contenu du fichier a été altéré. ».
CS31	Erreur bloquante – la signature du fichier n'est pas conforme car l'empreinte du document transmis ne correspond pas à l'empreinte signée.
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – l'empreinte du document n'est pas identique à l'empreinte signée. »

Commentaire [TB3]: Modification V1.02



Version : 1.02 Date : 07/08/2015

4.3. Contrôles liés au certificat et à la chaine de certification

Numéro Contrôle	Libelle d'alerte
CS01	Erreur bloquante – le certificat est expiré ou n'est pas encore valide
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – le certificat utilisé est expiré ou n'est pas encore valide. ».
CS02	Erreur bloquante – le certificat utilisé est révoqué ou est suspendu.
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – le certificat utilisé est révoqué ou est suspendu. »
CS03	Erreur bloquante – l'usage du certificat n'est pas conforme.
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – l'usage du certificat utilisé n'est pas destiné à de la signature électronique. ».
CS10	Erreur bloquante – la liste de certificat de confiance (CTL) n'est pas valide, par exemple, ils ont expiré ou ils sont été révoqués.
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – la liste de certificat de confiance (CTL) n'est pas valide. ».
CS11	Erreur bloquante – l'autorité de certification n'est pas connue.
	Libellé de l'erreur : « Un contrôle de validité de la signature est en erreur – l'autorité de certification (AC) est inconnue. ».



Version : 1.02 Date : 07/08/2015

5. SIGNATURE - Exemple

Cet exemple vise à concrétiser l'ajout de la balise ds :Signature dans un fichier déposé. Il se base sur un fichier de la famille de dépôt « 02 » qui correspond aux établissements bancaires.

```
<?xml version="1.0"?>
<Depot xmlns="http://www.caissedesdepots.fr/schema/eckert/deposant">
        <DeposantFonctionnel>0015021
/DeposantFonctionnel>
<NombreDepots>2
/NombreDepots>
                  <DeviseDepots>EUR</DeviseDepots>
<MontantDepots>2000</MontantDepots>
                  <DateHeureGeneration>2015-01-15T17:00:52
         </EnteteDepot>
         <CompteDepose:
                  Compte RefContrat="FR0000122220222112" TypeRefContrat="NUMERO_CONTRAT" TypeCompte="01"
                  NatureCompte="101" CodeDevise="EUR">
                           <Solde>1000</Solde>
                           <DateDepartDecheance>1987-04-26
                           <FaitGenerateurInactivite>DATE_DERNIERE_OPERATION_CLIENT/FaitGenerateurInactivite>
                  </Compte>
                  <PartiePrenante TypePersJuridique="P.PHYS" TypePartiePrenante="TITULAIRE">
<IdentitePartiePrenante>
                                    <PersonnePhysique>
                                             <Sexe>H</Sexe>
                                             <Nom>DUPONT</Nom>
                                             <NomDUsage>MARGOT</NomDUsage></Prenom>Florantine</Prenom>
                                             <LieuNaissance>PARIS</LieuNaissance>
<Nationalite>FR</Nationalite>
                                             <CapaciteJuridique>MINNEMAN</CapaciteJuridique>
                                             <DateDeces>2005-01-05</DateDeces>
<CommuneDeces>Paris</CommuneDeces>
                                             <PaysDepartementDeces>FRANCE/PaysDepartementDeces>
                                    </PersonnePhysique>

IdentitePartiePrenante>
                           <BlocAdresse>
                                    <LigneAdresse1/>
                                    <LigneAdresse2/>
                                    <LigneAdresse3>18 rue Berthollet</LigneAdresse3>
                                    <LigneAdresse4/>
                                    <CodePostal>94110</CodePostal>
                                    <Localite>ARCUEIL</Localite>
<PaysISO>FR</PaysISO>
                           </BlocAdresse
                  </PartiePrenante>
                  <LibelleAffaire>Le libelle
                  </LibelleAffaire>
         </CompteDepose>
        <CompteDepose>
                  Compte RefContrat="FR0000122220222113" TypeRefContrat="NUMERO_CONTRAT" TypeCompte="01"
                           NatureCompte="101" CodeDevise="EUR">
                           <Solde>1000</Solde>
                           <DateDepartDecheance>1987-04-26</DateDepartDecheance>
<FaitGenerateurInactivite>DATE_DERNIERE_OPERATION_CLIENT 
/FaitGenerateurInactivite>
                  <PartiePrenante TypePersJuridique="P.MORALE" TypePartiePrenante="ENTREPRISE">
                           <IdentitePartiePrenante>
                                   <PersonneMorale>
                                             <Denomination>MARGOT COMPAGNIE/Denomination>
                                    </PersonneMorale>
                           </ld>
IdentitePartiePrenante>

                  </PartiePrenante>
```



Version : 1.02 Date : 07/08/2015

```
<PartiePrenante TypePersJuridique="P.PHYS" TypePartiePrenante="TITULAIRE">
<IdentitePartiePrenante>
                                                <PersonnePhysique:
                                                                 <Sexe>H</Sexe>
                                                                 <Nom>VINCENT</Nom>
                                                                NomDUsage>BENJAMIN</NomDUsage>

<pre
                                                                 <LieuNaissance>PARIS</LieuNaissance>
<Nationalite>FR</Nationalite>
                                                                 <CapaciteJuridique>MINNEMAN</CapaciteJuridique><DateDeces>2005-01-05/DateDeces>
                                                                 CommuneDeces>Paris
CommuneDeces
                                                                 <PaysDepartementDeces>FRANCE
PaysDepartementDeces>
                                                 </PersonnePhysique>

IdentitePartiePrenante>
                                 <BlocAdresse>
                                                 <LigneAdresse1/>
                                                 <LigneAdresse2/>
                                                 <LigneAdresse3>18 rue Berthollet</LigneAdresse3>
                                                 <LigneAdresse4/>
                                                 <CodePostal>94110</CodePostal>
                                                 <Localite>ARCUEIL</Localite>
                                                 <PaysISO>FR</PaysISO>
                                </BlocAdresse>
                 </PartiePrenante>
 </CompteDepose
<RecapitulatifDepot>
<NombreDepots>2</NombreDepots>
</RecapitulatifDepot>
<ds:Signature Id="Signature_1434469620581" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds.SignedInfo Id="Signature_1434469620581-SignedInfo">
<ds:SignedInfo Id="Signature_1434469620581-SignedInfo">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference_URI=""Id="Signature_1434469620581-Reference-0">
                                 <ds:Transforms>
                                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                 </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>3SAT4Tuu44eeS1QHwCNAs8smCDX2f4oNULhaDV6SEwc=</ds:DigestValue>
                </ds:Reference>
                 <a href="ds:Reference URI="#Signature_1434469620581_SignedProperties">ds:Reference URI="#Signature_1434469620581_SignedProperties"</a>
                 Type="http://uri.etsi.org/01903#SignedProperties">
                                <ds:Transforms>
                                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                 </ds:Transforms>
                                <ds:DigestValue>9Q4s7mBuDTJXBQmxN92vw71bzGEtlVE4e9NuybIQ1Cc=</ds:DigestValue>9
</ds:SignedInfo>
<ds:SignatureValue
"de="Signature_1434469620581_Value">p7XX0Vfrkc5GE32etQooHZz3B3MZ+4C3CtKqy7LYYFRGPO8haRswZU/s27bnep9zPcC9LwWCxcRU8HaJ93fOn4r/bLEEF9ZAMguDpBojeBllT/zl/ymjNAyhinAl9+jdHzG3B7a4mri9GiXdx28qdgKBety5rG2DDfo4XXIcHQ8
PDYugruPQM5lbZFnLjfks/900d9qhrLnJhuB0Z9j7Md2u04rRX3zX5HYSY06Vh6M2P0l9x9JXBXRob7/PhChic4hf8VTgjoBX7gHJF0pAs+RQsrzAiDQYSWXXvyxYh3l7H+uTTm7BxSJsqir5ykE57y/wc0lnfMUFdnliAR2Z3g==
</ds:SignatureValue>
<ds:KeyInfo>
                                <ds:X509Certificate>MIID9DCCAtygAwlBAgISESEpuu1MAoettIA+0tzMV76AMA0GCSqGSlb3DQEBCwUAM
FkxCzAJBgNVBAYTAkZSMRowGAYDVQQKExFDQUITU0UgREVTIERFUE9UUzEXMBUGA1UECxMOMDA
wMiAxODAwMjAwMjYxFTATBgNVBAMTDENEQyAtIFJBQ0iORTAeFw0wOTExMTcwMDAwMDBaFw0xOTE
xMTcwMDAwMDBaMFkxCzAJBgNVBAYTAkZSMRowGAYDVQQKExFDQUITU0UgREVTIERFUE9UUzEXM
                                xmi tswinDawinbaainfxxczaJBgivbay i AkzswirkowGAYDVQQRExFDQUITOUGgREV i IERFUE90UZEAW BUGA1UECxMOMDAwMiAxODAwMjAwMjYxFTATBgNVBAMTDENEQyAtIFJBQ0IORTCCASIwDQYJKoZIhv cNAQEBBQADggEPADCCAQoCggEBALD56Uai/ND5iExk+AUPQWHQ3HHyj5YFrW8fsvqYSY2WyYRk8ibx 3ocBCdB26jon0LbppjGlL1phelGonaJrw4H67t0PLV48ohOu9//ArG/kqqiRTicutfPrf/UFVzBbhRFatALCqrKdeMd oRYa7am7l0IApPBXv4F2Oht6jLfDLHaDObNyFbbpkuQWVyxwWonsWLW47dKEJS727bKxoauWiInH5I7gnJs
```



Version: 1.02 Date: 07/08/2015

dlJ/Tx2FY9Fy5tjgPxyA+IcHJp9xLdKM65jbX0r7e2e8lAbfdkROmJAKMcbEQYvtR/oPAzddOJ/ez9wZyYuPGu7RcJIAKvSzMpIdXcnr2wWMmkYSXBM8CAwEAAaOBtTCBsjAPBgNVHRMBAf8EBTADAQH/ME8GA1UdlARI MEYwRAYEVR0gADA8MDoGCCsGAQUFBwlBFi5odHRwÓi8vaWdjLXBjLmNhaXNzZWRlc2RlcG90cy5mci9wyy1yYWNpbmUucGRmMA4GA1UdDwEB/wQEAwlBBjAdBgNVHQ4EFgQUeNMzBOlq7ZQJKhXhDE4z+fL3 B30wHwYDVR0jBBgwFoAUeNMzBOIq7ZQJKhXhDE4z+fL3B30wDQYJKoZlhvcNAQELBQADggEBADgOVs EPdLua4DERFYFtsPRMVw6JxOtxRFh2AaTLAsZpO29HBNMEg/sZM6sZdgPlNApFRtl9gQn2qFaWEABY6NaCsbqSkuGbAF47SivJMmYQDY2LnN5S1i7SK2PmhNHY/BQSUt6K7B5Au8OYxGC5dHjxYaOSZufcNrs7rwWI z+Cdu/CuM6OaRo56KECjWQfKYt2cM3HFQm6xuyk8lz40togfTUoOaCclznQLaNeEvYqnFchmHsAasttZFB4cw53KagxUFGESlNXpC//Yr93r6AEeYwM6RCvt2RcvZl9SQ0x7owsLPTEgEdFRDOQKPNtvuQHf3wP+CoqSD Hc3/mdStPc=</ds:X509Certificate:

cds:X509Certificate>MIIEijCCA3KgAwlBAglSESGvbpbamFVB+KLxEmEeUNg5MA0GCSgGSlb3DQEBCwUA MFkxCzaJBgNVBAYTAkZSMRowGAYDVQQKExFDQUITU0UgREVTIERFUE9UUzEXMBUGA1UECxMOMDAwMiAxODAwMiAwMjYxFTATBgNVBAMTDENEQyAtIFJBQ0iORTAeFw0wOTExMTcwMDAwMDBaFw0xOT EXMTUWMDAwMDBaMFoxCzAJBgNVBAYTAkZSMRowGAYDVQQKExFDQUITU0UgREVTIERFUE9UUzEX MBUGA1UECxMOMDAwMiAxODAwMjAwMjYxFjAUBgNVBAMTDUNEQyAtlEZJREVMSUEwggEiMA0GCSqGSlb3DQEBAQUAA4IBDwAwggEKAoIBAQDgGBsNwxsfaCvzFLtirqPOzkyxZtpw7SwDQ5/Mb/Tq9KnaUVmkb sXwcvqZs90yzSK/rpe0tdzeYycQqgbjrsGB6uBU1YjJq4KkduX6Csh89bqBQsWTmCN2BnMUuUu35+Aj1Xlkdiz jz0BOu3ymlpA4/uswXSVC1LbrMSrqzD48T50ZRdBEghEycR1YnL3QZk1iREJSp5gB5BTnJeDGJxojLjWTA3x KPH2EagEzbK+dswWA1DMVwQSbQj/VK+O0Cbs3mCvc1P7ucWCQYjZKReXEnKBFdSqPfeF73f3pAMhvnlODpc6FMojK2n173/r0KDhgOvBejHMSGl044gBvk0SVAgMBAAGjggFJMllBRTBLBggrBgEFBQcBAQQ/MD0wO WYIKWYBBQUHMAGGL2h0dHA6Ly9pZ2Mtb2NzcC5jYWlzc2VkZXNkZXBvdHMuZnlvb2NzcC1yYWNpbmUvMBIGA1UdEwEB/wQIMAYBAf8CAQAwTwYDVR0gBEgwRjBEBgRVHSAAMDwwOgYlKwYBBQUHAgEWLmh0dHA6Ly9pZ2MtcGMuY2Fpc3NlZGVzZGVwb3RzLmZyL3BjLXJhY2luZS5wZGYwQQYDVR0fBDowODA2oD SgMoYwaHR0cDovL2lnYy1jcmwuY2Fpc3NIZGVzZGVwb3RzLmZyL2NkYy9yYWNpbmUuY3JsMA4GA1UdDwEB/wQEAwlBBjAdBgNVHQ4EFgQUB8pYWkuqTQ7ea/LRWXMwlaOSpjMwHwYDVR0jBBgwFoAUeNMzBO Iq7ZQJKhXhDE4z+fL3B30wDQYJKoZlhvcNAQELBQADggEBAJ7wnGmld+dlzQ9Co9TTqww0YvXSJOARQN Z9st/bNsIcnrkRzQmI+rVeuc5NyiauwQ/S1Qq4MBz9XACadKuQzpgx6Jqn1BWSydqricB2id8OuGYzByUw5fv+ BgulyqZuOvCnVEnP2/1iXyzLXhfMVH8c9LNG7A4TJoq739iOGOcY+mw4ukkAgSTj6QS5GEfJB6UakJSknSzAQ0FEfH8yWhJvOaeWTDuGaBgYiVtD+pzorWWccGHZKPX+PsSYrujEpd9eUpFsL7wq6zj26aChDYfVGPN wWK+ce8h5yFc7jsoTQduEoRQWODY0wqafPD0SoRq3nK69zupAcQn0dQHDeY=

</ds:X509Certificate:

<ds:X509Certificate>MIIFDDCCA/SgAwlBAgISESfoACiM11V+x4IJr240yAIVMA0GCSqGSlb3DQEBCwUAMF oxCzaJBgNVBAYTAkZSMRowGAYDVQQKExFDQUITU0UgREVTIERFUE9UUzEXMBUGA1UECxMOMDAwMiAxODAwMjAwMjYxFjAUBgNVBAMTDUNEQyAtlEZJREVMSUEwHhcNMTMwNDI0MDgzNDMzWhcNMTY wNDI0MDgzNDMzWjBYMQswCQYDVQQGEwJGUjEZMBcGA1UEChMQSU5GT1JNQVRJUVVFIENEQzEX MBUGA1UECxMOMDAwMiA3NzU2NjU0MzMxFTATBgNVBAMTDFRoYW5obGFtIENBTzCCASIwDQYJKoZI hvcNAQEBBQADggEPADCCAQoCggEBAK5L3/5b+FVTW3bWCWggvRa7/fqUB9EUeLDDIXNk/d9qewKGSKWI33fnI+wW6UP6JUFLKhF/paHbcrQdZ47S1Xyf72O5tuyrkkpHI4PV+aPwBVwltZnqElvb1Aop2eZRiEYolWRE 5V4xlH8j/ibGsKiMnso7amDpiH0uxrGqCVqFM7W4DTd96TgBJ0WTCOx4gxQjUV7r7afHkCSP7f4LcR88BkeGt LnURsWgZAvrTD8ZyAEwVsqVTGbG9o+FU6Gy9kVLMA7MvCJrGcJD9yy5v2XV+lpCd0mjAs8LRldmGsESffy Ya6sWVTUjiuxQT8RHGDDoNAK16o6s5amObRl4p1ECAwEAAaOCAcwwggHlMAwGA1UdEwEB/wQCMAA wTAYIKwYBBQUHAQEEQDA+MDwGCCsGAQUFBzABhiBodHRwOi8vaWdiLW9ic3AuY2Fpc3NIZGVzZGVw b3RzLmZyL29jc3AtZmlkZWxpYS8wDgYDVR0PAQH/BAQDAgeAMB8GA1UdJQQYMBYGCCsGAQUFBwMC BgorBgEEAYI3FAICMFYGA1UdIARPME0wSwYKKoF6AQUBAQEEAjA9MDsGCCsGAQUFBwIBFi9odHRwOi8vaWdjLXBjLmNhaXNzZWRlc2RlcG90cy5mci9wYy1maWRlbGlhLnBkZjBCBgNVHR8EOzA5MDegNaAzhjFo dHRwOi8vaWdjLWNybC5jYWlzc2VkZXNkZXBvdHMuZnlvY2RjL2ZpZGVsaWEuY3JsMF0GA1UdEQRWMFS gMAYKKwYBBAGCNxQCA6AiDCBUaGFuaC1MYW0uQ2FvQGNhaXNzZWRlc2RlcG90cy5mcoEgVGhhbmgt TGFtLkNhb0BjYWlzc2VkZXNkZXBvdHMuZnlwHQYDVR00BBYEFFQkwf84EnB+LZyyxPlWqGLkNTxTMB8GA1UdlwQYMBaAFAfkWFpLqk0O3mvy0VlzMJWjkqYzMA0GCSqGSlb3DQEBCwUAA4lBAQA81lT4lz4M5lM9 1HYbdWLzUkuQpialO0P43nw0Z25OPZtoUSmEpY8uSqsX1JcmtEkkKEEpxFwp3iU6kYTpDG3nOsoLjUriHwC xZGssJz7u+ImEkrR8HWGiTbY1tgoz9mbixrkjEiCyl3nd/7dJoj0L8rWcYyDmn4if+rtZe1yEng5q9xO5aCyx+oZQOm63TcfKJzG5ua78CYH6VyJ+Jky4BVaRAtDp06PysSrV7CkZzjsQBilZZW+tM9xdtbXiJzcJpgzg27Apdz0AlixX

```
</ds:X509Data>
</ds:KevInfo>
<ds:Object>
          <xades:QualifyingProperties Target="#Signature 1434469620581" xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">
          <xades:SignedProperties Id="Signature_1434469620581_SignedProperties">
          <xades:SignedSignatureProperties>
                     <xades:SigningCertificate>
                                <xades:Cert>
                                           <xades:CertDigest>
                                                     ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>TOAWNxk08ZmDUOPgT/IE9MykUZHq64PtAngBRUE/j0k=</
                                                     ds:DigestValue>
                                           </xades:CertDigest>
                                           <xades:IssuerSerial</p>
```



Version : 1.02 Date : 07/08/2015

<ds:X509lssuerName>CN=CDC - FIDELIA,OU=0002 180020026,O=CAISSE DES DEPOTS,C=FR</ds:X509lssuerName><ds:X509SerialNumber>1494488254867317863082760636668308999375189</ds:X509SerialNumber>