



République Française Services du Premier Ministre

**DISPOSITIF DE SECURISATION DES DONNEES  
RELATIF A LA DIFFUSION DU JOURNAL OFFICIEL  
ELECTRONIQUE AUTHENTIFIE ET DES  
DOCUMENTS ADMINISTRATIFS**

## Sommaire

1. GENERALITES .....	3
1.1. Définitions .....	3
1.2. Abréviations .....	4
2. INTRODUCTION .....	5
2.1. Schéma de signature d'un document .....	6
2.2. Schéma de vérification de la signature d'un document .....	6
3. INFRASTRUCTURES DE CONFIANCE DILA .....	7
3.1. Infrastructure de diffusion .....	8
3.2. Infrastructure de Gestion de clés (IGC) .....	9
3.3. Infrastructure de signature des textes .....	10

## 1. GENERALITES

### 1.1. Définitions

Terme	Signification
Active X	Composant logiciel créé par Microsoft. Il est utilisé pour permettre le dialogue inter-programmes. Bien qu'il ait été implémenté sur de nombreuses plateformes, il est toujours majoritairement utilisé avec Windows.
Applet Java ou appliquette	Logiciel écrit en Java qui s'exécute dans la fenêtre d'un navigateur Web (Internet Explorer, FireFox, Opera, etc.) en utilisant les services d'une machine virtuelle Java.
Application utilisatrice	Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.
Autorité d'horodatage	Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du RGS).
Cachet électronique ou cachet serveur	Dans le cadre de signature électronique des textes publiés par la DILA, la signature est opérée par une machine pour le compte d'une personne morale sur ordre d'une personne physique détentrice d'un certificat personnel. Dans ce cas, le terme "signature" qui n'est défini, juridiquement, que pour les personnes physiques est remplacé par le terme cachet électronique.
Certificat électronique	Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et sa bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Codes actifs	Applet Java ou ActiveX signés. Dans le contexte de cette politique, ces codes sont utilisés pour vérifier la signature des documents signés au format XAdES avec des certificats opérés par l'AC-JO-Publication.
Composante	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie. La composante joue un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction des Infrastructures de diffusion, de signature ou d'IGC.
Contremarque de temps	Donnée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, et établissant ainsi la preuve que la donnée existait à cet instant là.
Entité	Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.
Infrastructure de gestion de clés (IGC)	Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.
Java	Langage de programmation orienté objet et indépendant de toute architecture matérielle.
Jeton d'horodatage	Voir Contremarque de temps
Machine Virtuelle Java (JVM)	Machine virtuelle indépendante de toute architecture matérielle qui permet d'exécuter les programmes écrits en Java.
Magasin à certificats	Lieu de stockage personnel des certificats. Les magasins sont le plus couramment accessibles via le navigateur Web du poste de travail. A l'installation initiale, les navigateurs contiennent un ensemble de certificats d'autorités racines ou intermédiaires dit « de confiance ». L'utilisateur peut ajouter des certificats au magasin originel sous réserve de vérifier la confiance qu'il peut leurs accorder.
OID	identificateur alphanumérique international, enregistré auprès de l'AFNOR pour la France, pour désigner de manière unique un objet ou une classe d'objets spécifique.
Porteur	La personne physique ou morale identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat. Le porteur peut être également un composant technique (routeur, serveur, application).
Produit de sécurité	Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Terme	Signification
Qualification des produits de sécurité	Acte par lequel la DCSSI atteste du niveau de sécurité d'un produit de sécurité en s'appuyant sur le schéma français d'évaluation et de certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, schéma défini par le Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
Signataire	personne physique habilitée à opérer la signature électronique des textes du JOEA ou des DA et possédant un certificat en son nom.
Signature	La signature est une marque permettant d'identifier l'auteur d'un document.
Signature électronique	La signature électronique permet, à l'aide d'un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire.
Usager	Personne physique agissant pour son propre compte ou pour le compte d'une personne morale dans ses relations avec une administration.
UTC	Échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 Pour la plupart des usages, le temps UTC est équivalent au temps solaire au méridien principal (0°). De manière plus précise, le temps UTS est un compromis entre le temps atomique particulièrement stable (Temps Atomique International – TAI) et le temps solaire dérivé de la rotation irrégulière de la terre lié au temps moyen sidéral de Greenwich (GMST) par une relation de convention.
Vérification de la signature	L'opération de vérification de la signature électronique, valide l'intégrité d'un document et l'authenticité des certificats utilisés.

## 1.2. Abréviations

Les acronymes dans le présent document sont les suivants :

Sigle	Signification
AC	Autorité de Certification
DA	Document Administratif
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DILA	Direction de l'information légale et administrative
FAQ	Foire Aux Questions (Frequently Ask Questions)
IGC	Infrastructure de Gestion de Clés
JO	Journaux Officiels
JOEA	Journal Officiel Electronique Authentifié
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OID	Object Identifier
PC	Politique de Certification
PDF	Portable Document Format
PSCE	Prestataire de Services de Certification Electronique
RGS	Référentiel Général de Sécurité
RSA	Rivest Shamir Adelman
UTC	Coordinated Universal Time
X.509	Format des certificats d'identité recommandé par l'Union Internationale des Télécommunications (UIT).
XAdES	XML Advanced Electronic Signatures
XML	eXtended Markup Language

Le site des Journaux officiels ne diffuse sur l'Internet **que les textes signés**. Pour les cas où la vérification de signature ne peut être opérée sur le poste de l'utilisateur, le texte original est extrait du fichier signé sur le site de la DILA et présenté directement dans le lecteur PDF du poste de consultation.

## 2. INTRODUCTION

Ce document constitue un extrait du document décrivant le dispositif de sécurisation des données mise en place dans le cadre de la Diffusion sur l'Internet du Journal Officiel Electronique Authentifié (JOEA) et des Documents administratifs (DA).

Le JOEA est mis en ligne sur le site des Journaux officiels depuis le 2 juin 2004 (Ordonnance 2004-164 du 20 février 2004). Les DA sont mis en ligne ponctuellement depuis le 13 avril 2006.

Les textes diffusés sont signés électroniquement selon la norme européenne de signature avancée XAdES. Les certificats électroniques X509, utilisés par la DILA dans ce cadre sont opérés selon les recommandations du RGS. Les politiques de certification des autorités de certification de la DILA sont accessibles à partir de l'aide du site <http://www.journal-officiel.gouv.fr/jahia/Jahia/pid/249>

Les textes signés par la DILA reposent sur un condensat de type **SHA-1** chiffré avec une clé **RSA** d'une longueur de **2048** bits. Les documents signés sont **horodatés**. La DILA a déployé sa propre *autorité d'horodatage*.

La **signature électronique** permet d'identifier le signataire et de garantir l'intégrité d'un document électronique sur lequel le signataire manifeste son accord sur le contenu, et par analogie avec la signature manuscrite d'un document papier.

*Un dispositif de signature électronique doit :*

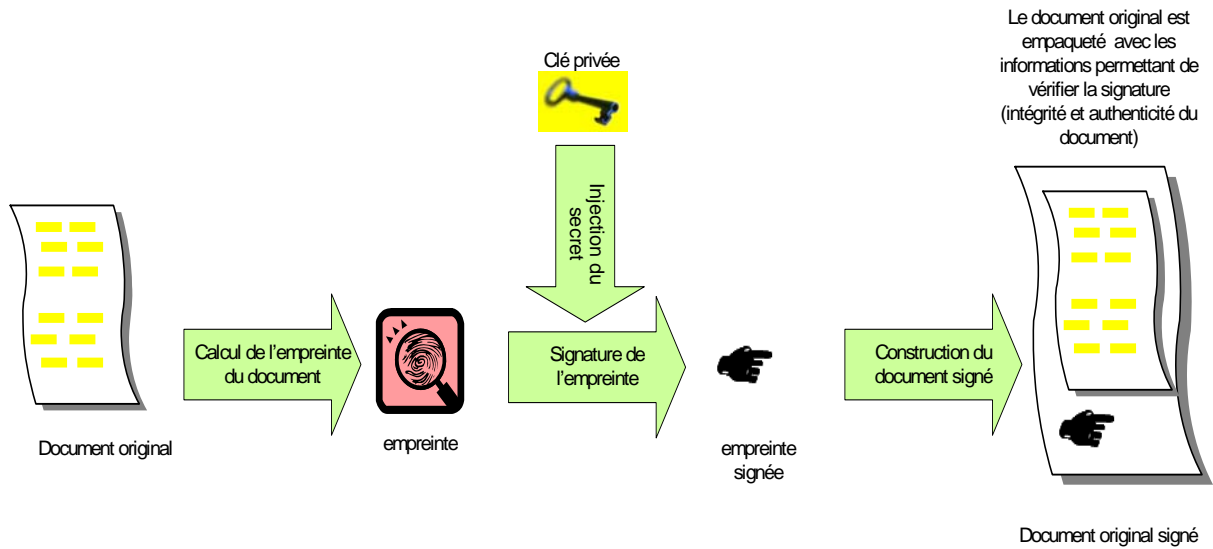
- permettre au lecteur d'un document, d'identifier la personne ou l'organisme qui a apposé sa signature ;
- garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

A cette fin, les conditions suivantes doivent être réunies :

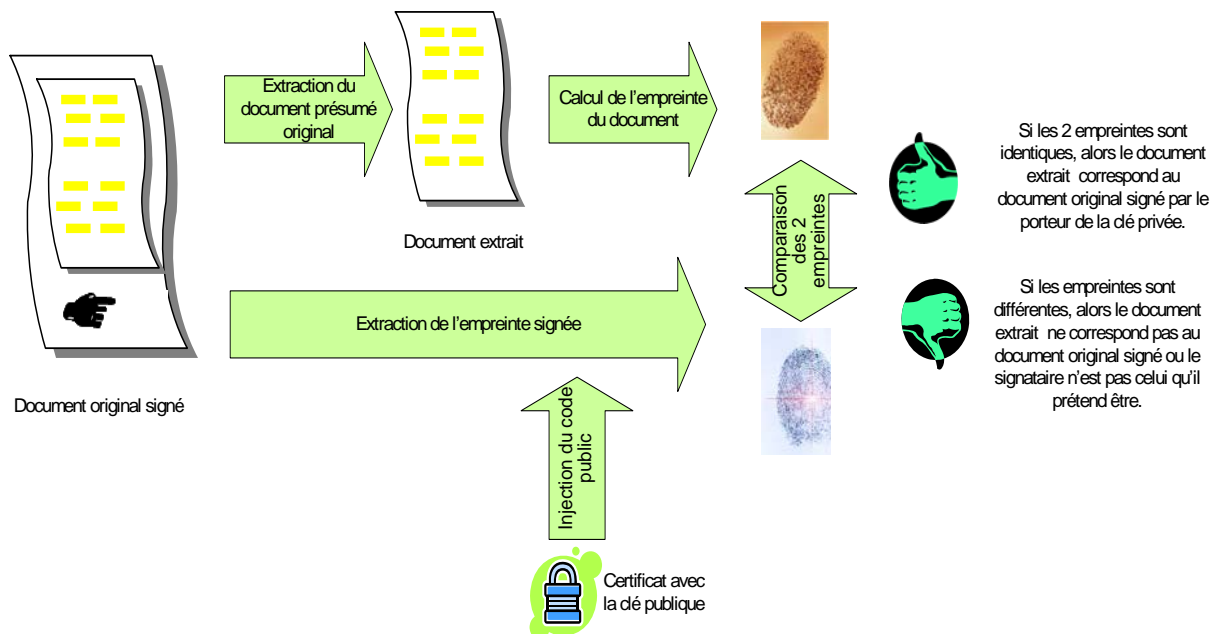
- L'identité du signataire doit pouvoir être retrouvée de manière certaine ;
- La signature ne peut pas être falsifiée ;
- Un document signé est inaltérable.

La signature numérique n'est devenue possible qu'avec la cryptographie asymétrique. Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres qui résulte de l'usage d'un procédé cryptographique répondant aux conditions définies par les lois et règlements en vigueur.

## 2.1. Schéma de signature d'un document



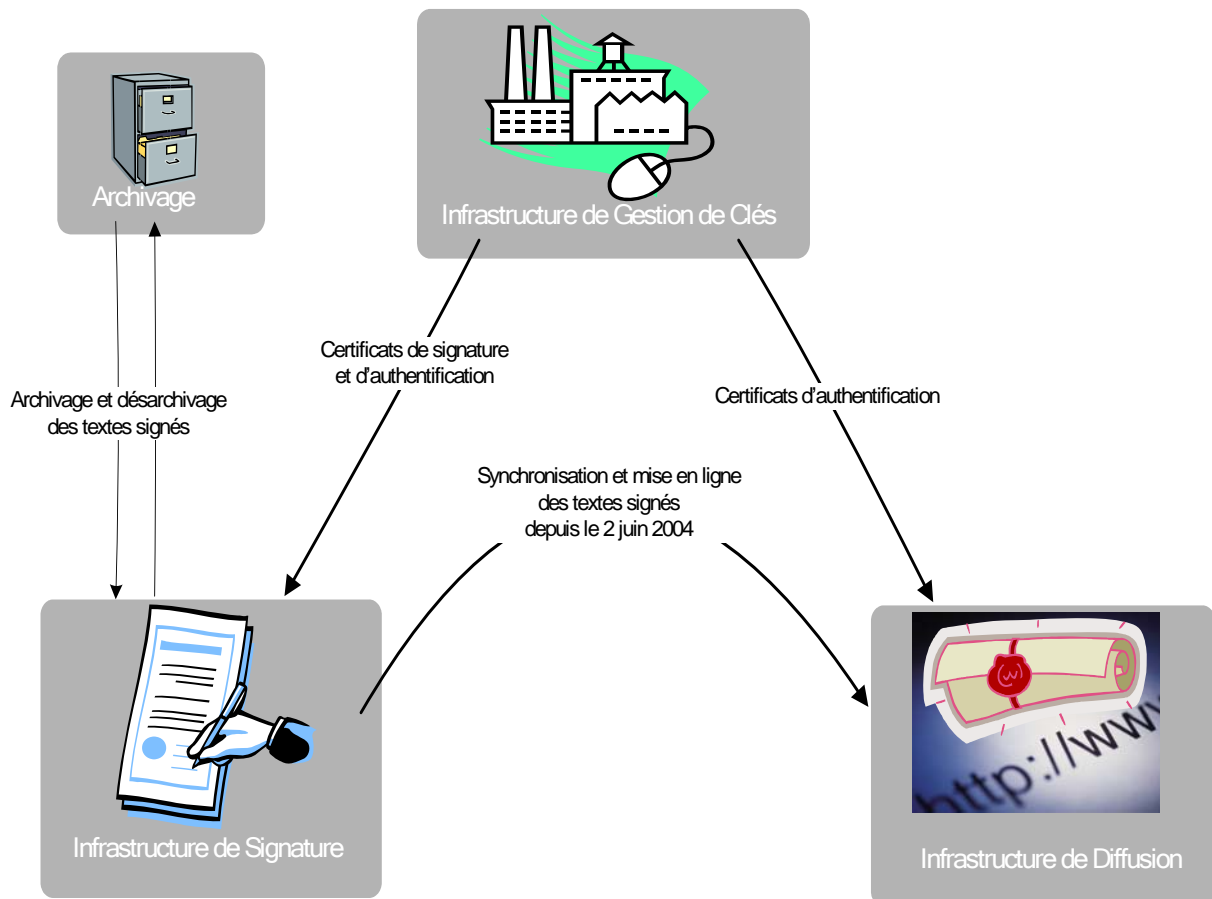
## 2.2. Schéma de vérification de la signature d'un document



### 3. INFRASTRUCTURES DE CONFIANCE DILA

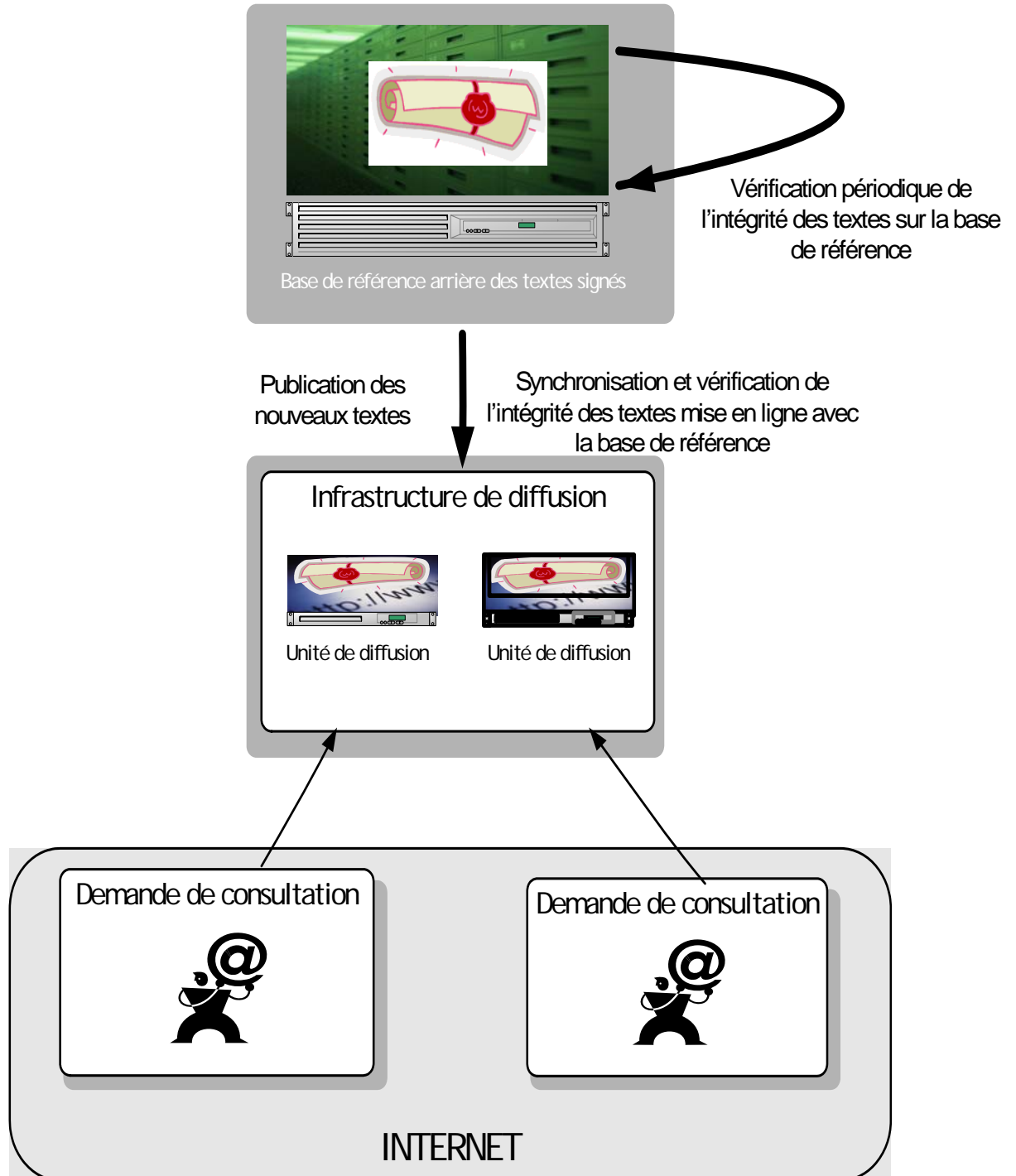
La consultation des textes signés sur le site de la DILA, s'appuie sur :

- Une Infrastructure de diffusion ;
- Une Infrastructure de Gestion de Clés, à partir de laquelle les certificats sont opérés ;
- Une Infrastructure de signature des textes qui héberge le *dispositif de création de signature*.



### 3.1. Infrastructure de diffusion

- La disponibilité des textes mis en ligne est assurée par la redondance des supports de diffusion (accès internet et serveurs de diffusion) ;
- L'intégrité des textes est vérifiée périodiquement sur les serveurs de diffusion.



- Les textes *PDF* (*JOEA*, *DA*) sont signés (au format *XAdES*) et horodatés (*Contremarque de temps*). Ils sont diffusés de manière permanente et gratuite (24h/24 et 7j/7). Les certificats de signature et d'horodatage sont émis par L'AC JO Publication ;

- La vérification de signature est :
  - soit **synchrone** sur le poste de travail de l'*Usager*.  
Dans ce cas le poste doit être autorisé à télécharger et exécuter des codes actifs, de type *Active X* ou *Applet Java*. Les codes DILA sont signés avec un certificat émis par L'AC JO Codes.  
  
Le lancement et les mises à jour des codes actifs sont automatisés. En cas de dysfonctionnement, des *FAQ* sont accessibles à partir de la page de recherche du JOEA : <http://www.journal-officiel.gouv.fr/frameset.html>
  - soit **périodique** sur le site de diffusion.  
Dans ce cas le poste de l'utilisateur doit disposer d'un lecteur de fichier PDF. Adobe met à disposition son Reader en téléchargement libre et gratuit sur son site : <http://www.adobe.fr/products/acrobat/readstep2.html>
- Les **pré-requis** nécessaires à l'exécution d'une vérification de signature synchrone sont :
  - Avoir de disponible sur son poste travail, un lecteur *PDF* de type Adobe Reader ou équivalent ;
  - Avoir installé les certificats Racine, Publication et Codes dans le *magasin* de son navigateur ;
  - Avoir autorisé sur son poste et en téléchargement à partir du site de la *DILA*, l'affichage de fenêtre de type publicitaire et l'exécution de l'*Active X* ou de l'*Applet Java* signée.

Pour les *Usagers* utilisant l'*Applet* :

- Avoir de disponible sur son poste de travail une machine virtuelle java.

Pour les *Usagers* dont le poste de travail appartient à un réseau d'entreprise ou équivalent :

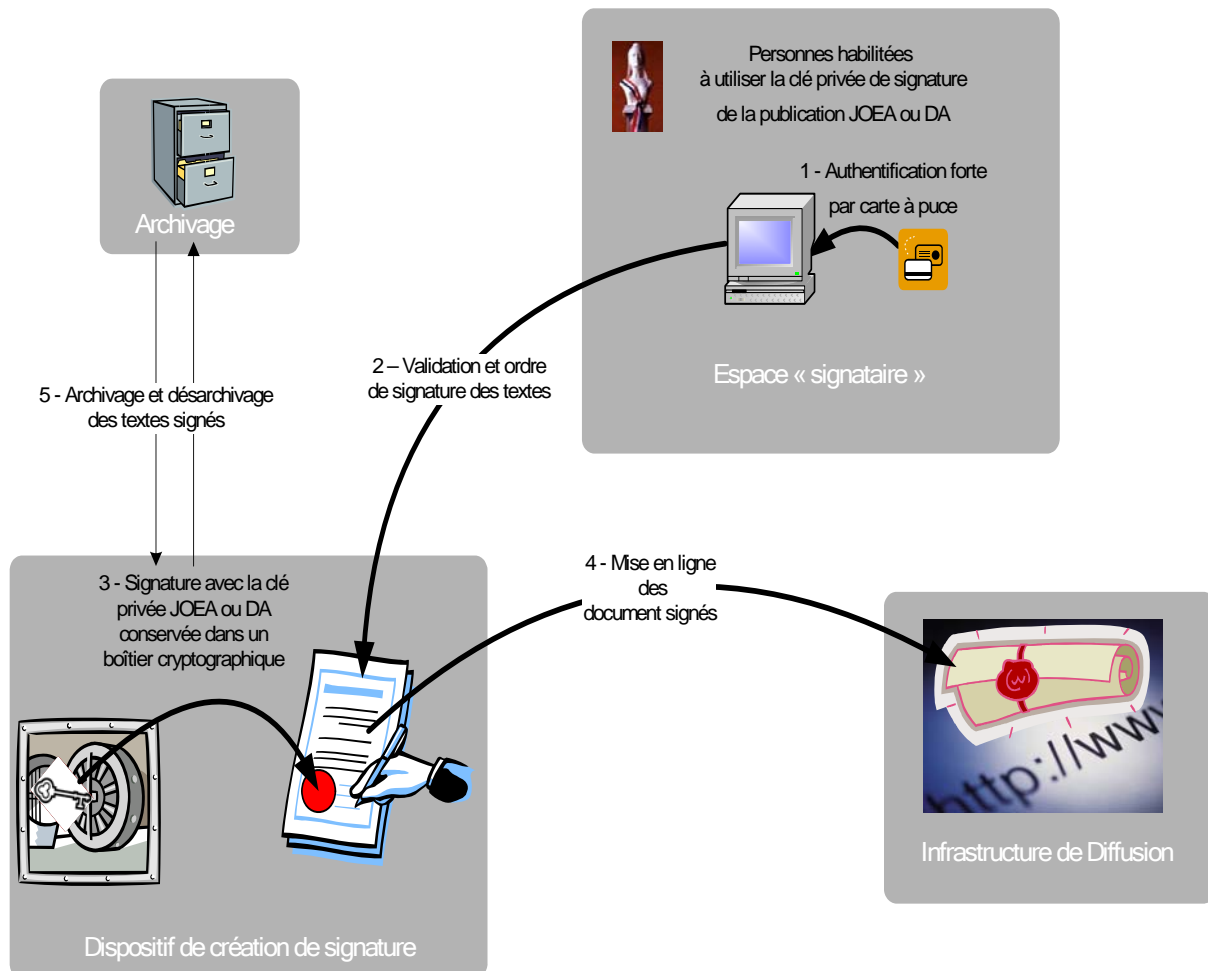
- S'assurer que l'un des 2 types de *codes actifs* : *Active X* ou *Applet Java*, est autorisé en téléchargement à partir du site de la *DILA* et en exécution sur le poste de travail.
- Les listes de révocation des certificats sont disponibles sur le site de la *DILA* et mis à jour régulièrement :
  - [http://igc.journal-officiel.gouv.fr/crl/AC-DILA-Racine/crl\\_acDILA\\_Racine.crl](http://igc.journal-officiel.gouv.fr/crl/AC-DILA-Racine/crl_acDILA_Racine.crl)
  - [http://igc.journal-officiel.gouv.fr/crl/AC-DILA-Publication/crl\\_acDILA\\_Publication.crl](http://igc.journal-officiel.gouv.fr/crl/AC-DILA-Publication/crl_acDILA_Publication.crl)
  - [http://igc.journal-officiel.gouv.fr/crl/AC-DILA-Codes/crl\\_acDILA\\_Codes.crl](http://igc.journal-officiel.gouv.fr/crl/AC-DILA-Codes/crl_acDILA_Codes.crl)
- Les certificats utilisés sont disponibles sur le site de la *DILA* :
  - <http://igc.journal-officiel.gouv.fr/crt/AC-DILA-Racine.crt>
  - <http://igc.journal-officiel.gouv.fr/crt/AC-DILA-Publication.crt>
  - <http://igc.journal-officiel.gouv.fr/crt/AC-DILA-Codes.crt>

### 3.2. Infrastructure de Gestion de clés (IGC)

La *DILA* est son propre *PSCE* et s'est dotée d'une *Infrastructure de gestion de clés* pour opérer les certificats dont elle a besoin pour la diffusion des ces publications. Cette *IGC* s'appuie sur les recommandations du RGS. Les politiques de certification de ses *AC Racine*, *Publication* et *Rôles* sont accessibles sur le site de la *DILA*.

### 3.3. Infrastructure de signature des textes

Le schéma ci dessous synthétise l'infrastructure mise en place pour la signature (*cachet serveur*) des textes :



- Le dispositif de création et de stockage des clés de signature s'appuie sur un carte cryptographique *qualifiée* ;
- Le logiciel de signature est en cours de *qualification*.