

Guide technique de configuration d'*Adobe Acrobat DC*
et d'*Adobe Reader DC* pour signature avec
Entrust Entelligence Security Provider

Direction générale des registres et de la certification
du ministère de la Justice

Mise en garde

Selon l'environnement technologique utilisé, le fonctionnement du logiciel peut différer de celui décrit dans ce document. Il est donc fortement recommandé de vérifier d'abord les exigences techniques requises, puis, si l'environnement technologique de l'utilisateur diffère de celui indiqué dans le présent document, de communiquer avec le Service de soutien informatique du Service de certification du ministère de la Justice (MJQ).

Note

Ce document comporte plusieurs noms composés de mots ou d'expressions qui constituent des marques de commerce. Afin d'alléger le texte et d'en faciliter la lecture, les symboles « ^{MC} », « TM », « ^{MD} » ou « [®] » ne sont pas mentionnés à la suite de ces mots ou expressions.

Service de certification
Direction des registres et de la certification
Ministère de la Justice
1, rue Notre-Dame Est, bureau 7.35
Montréal (Québec) H2Y 1B6

Site Web : www.infocles.justice.gouv.qc.ca
Courriel : services@infocles.justice.gouv.qc.ca
Téléphone : 418-643-5140, option 2 (Québec et les environs)
1-866-536-5140, option 2 (sans frais)
Télécopieur : 514 864-2346

Table des matières

1. Introduction	4
2. Systèmes d'exploitation, logiciels requis et préalable	4
3. Installation des certificats racines (<i>root</i>)	4
4. Configuration d' <i>Adobe Reader DC</i> ou d' <i>Adobe Acrobat DC</i>	7

1. Introduction

Ce document décrit les étapes à suivre pour la configuration d'*Adobe Acrobat DC* ou d'*Adobe Reader DC*, pour la signature et la vérification des documents PDF signés ou certifiés.

2. Systèmes d'exploitation, logiciels requis et préalable

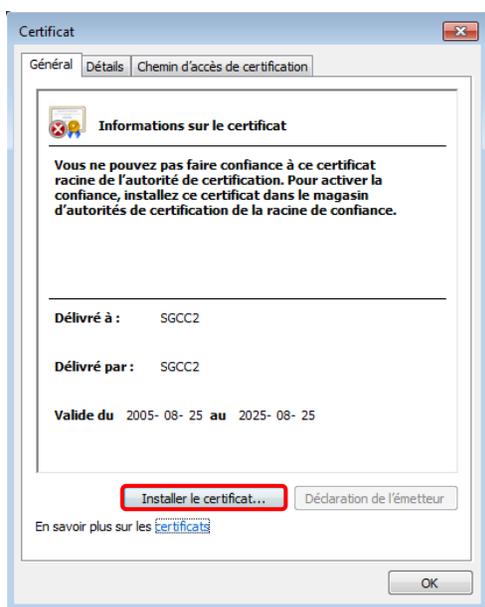
- ▶ Systèmes d'exploitation :
 - Microsoft Windows 7 – Toutes les versions 32 bits et 64 bits ayant la rustine Windows « 10.0.40 » et plus
 - Microsoft Windows 8.1 Pro et 8.1 Enterprise
 - Microsoft Windows 10 Pro et 10 Enterprise
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows Server 2016
- ▶ Logiciels requis : *Adobe Acrobat DC* ou *Adobe Reader DC*.
- ▶ Préalable : Communiquer avec le Service de certification du MJQ pour obtenir les trois certificats de l'autorité de certification (certificats racines ou *root*) et le fichier de registre (*.reg).

3. Installation des certificats racines (*root*)

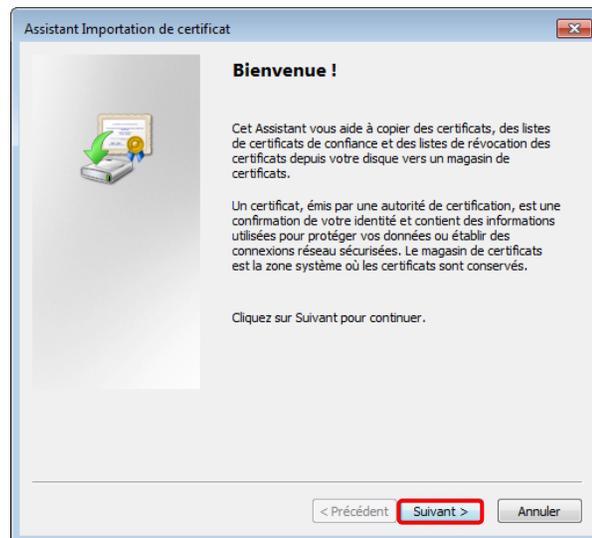
Les certificats racines sont utilisés lors de la signature ou de la validation d'une signature pour s'assurer de l'autorité de la certification.

Après avoir obtenu les certificats racines du Service de certification du MJQ (fichiers avec extension « .der ») et les avoir déposés dans un répertoire, installer les certificats dans la liste des certificats d'autorité sur le poste :

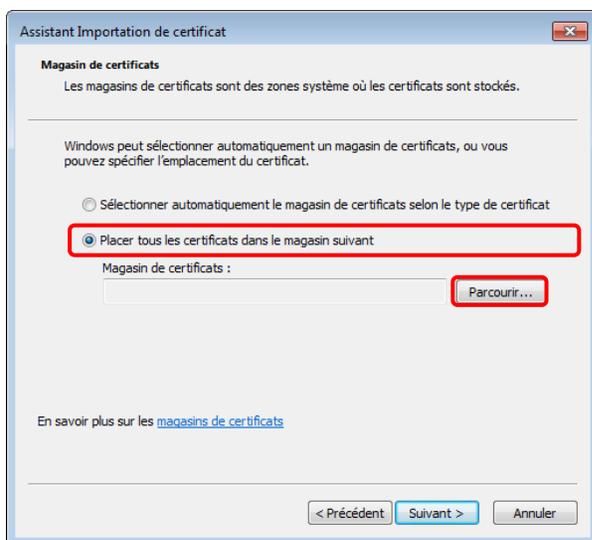
1. Double-cliquer sur le premier des trois certificats racines sauvegardés sur le poste. Une fenêtre apparaîtra. Cliquer sur le bouton « Installer le certificat... ».



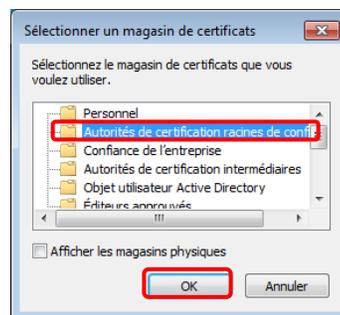
2. L'assistant d'importation de certificat apparaîtra. Cliquer sur le bouton « Suivant > » pour poursuivre avec l'assistant d'importation.



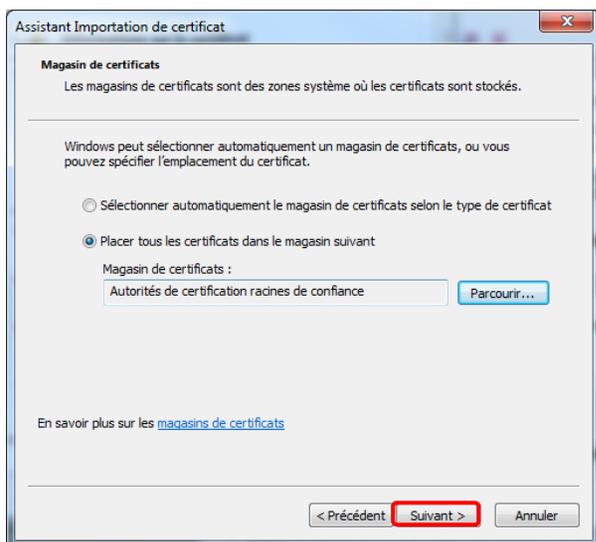
3. La fenêtre suivante demandera où sauvegarder le certificat. Cocher la section « Placer tous les certificats dans le magasin suivant » et cliquer sur le bouton « Parcourir... ».



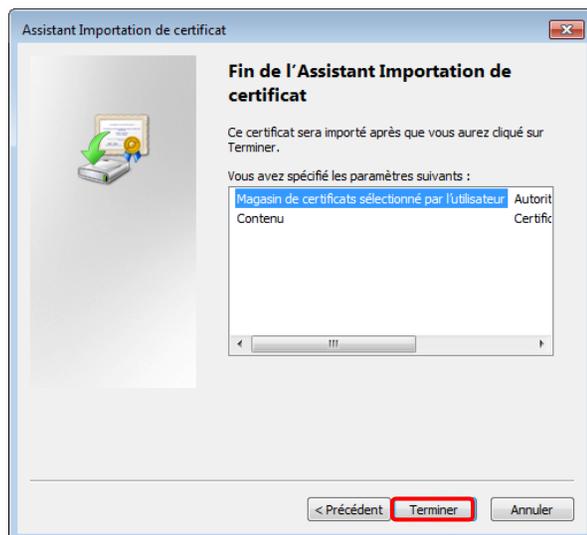
4. Dans la fenêtre suivante, sélectionner le magasin de certificats « Autorités de certification racines de confiance » et cliquer sur le bouton « OK ».



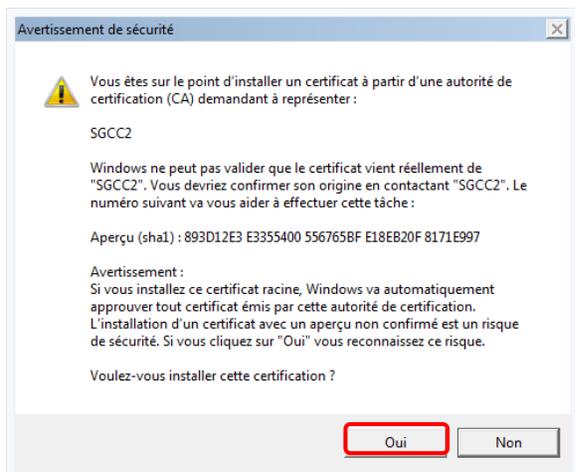
5. Cliquer sur le bouton « Suivant > ».



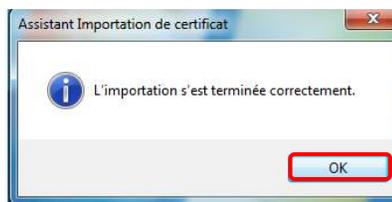
6. Pour mettre fin à l'assistant, cliquer sur le bouton « Terminer ».



7. Une fenêtre d'avertissement de sécurité apparaîtra pour demander de confirmer l'installation du certificat racine de l'autorité de certification. Cliquer sur le bouton « Oui ».



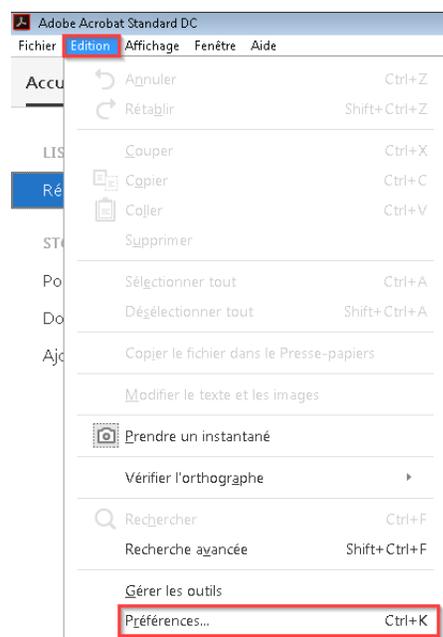
8. L'importation du certificat est terminée. Cliquer sur le bouton « OK ».



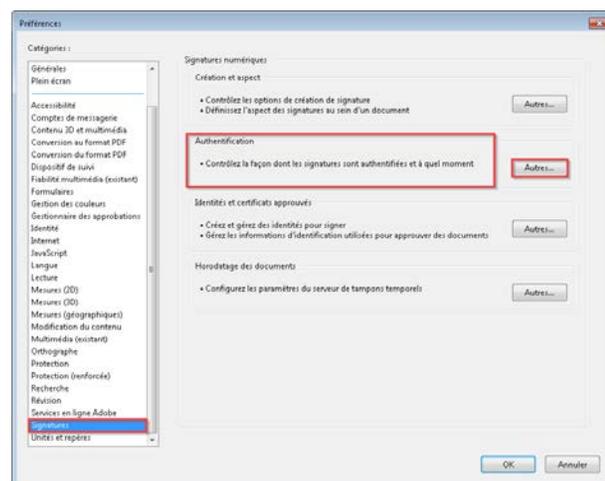
9. Répéter les étapes 1 à 8 pour les deux autres certificats racines.

4. Configuration d'Adobe Reader DC ou d'Adobe Acrobat DC

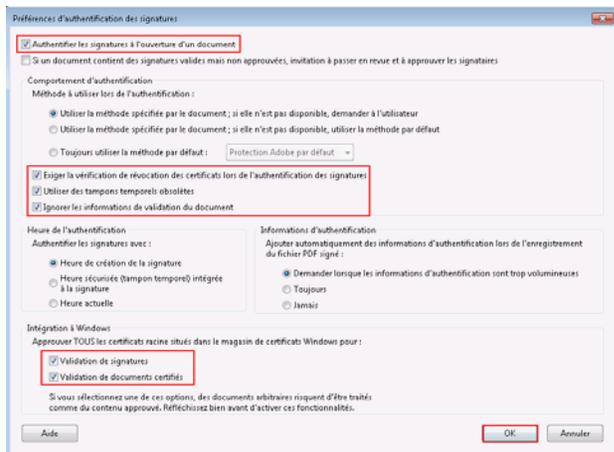
1. Ouvrir *Adobe Acrobat*. À partir du menu « Édition », sélectionner « Préférences... ».



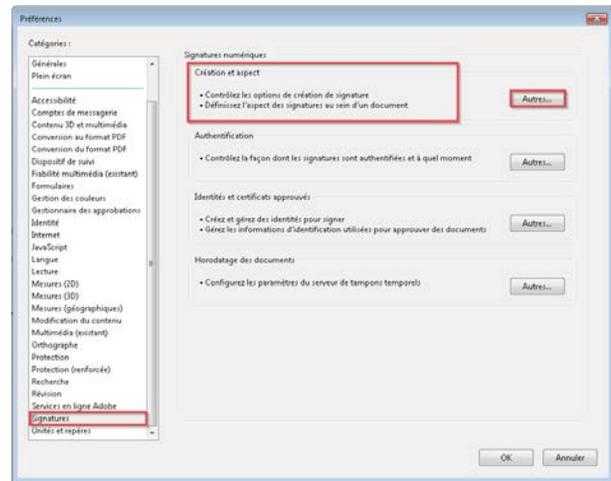
2. Dans la partie gauche de la fenêtre, s'assurer que l'option « Signatures » est sélectionnée. À partir de la section « Authentification », cliquer sur le bouton « Autres... ».



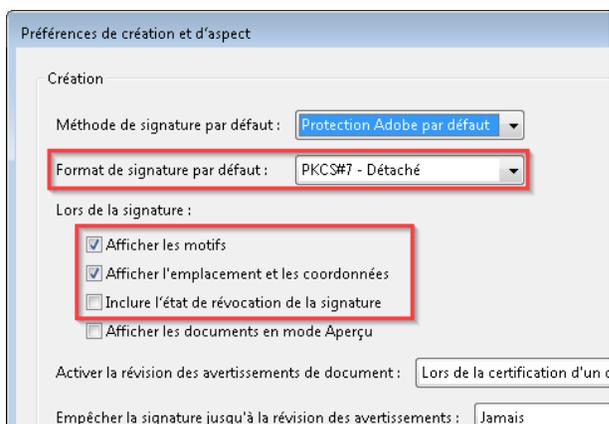
3. S'assurer que
 - a. dans la partie supérieure, l'option « Authentifier les signatures à l'ouverture d'un document » est cochée;
 - b. sous la section « Comportement d'authentification », la case « Exiger la vérification de révocation des certificats lors de l'authentification des signatures » ainsi que « Ignorer les informations de validation du document » sont cochées;
 - c. sous la section « Intégration à Windows », les cases « Validation de signatures » et « Validation de documents certifiés » sont cochées.
4. Cliquer sur « OK » pour fermer la fenêtre des « Préférences d'authentification des signatures ».



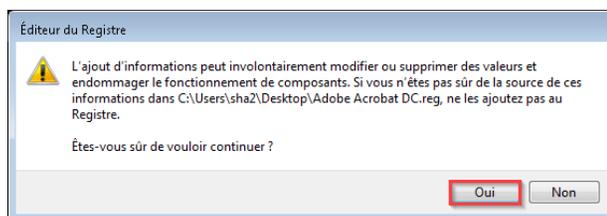
5. Dans la partie gauche de la fenêtre, s'assurer que l'option « Signatures » est sélectionnée. À partir de la section « Création et aspect », cliquer sur le bouton « Autres... ».



6. Dans la fenêtre « Préférences de création et d'aspect », s'assurer que :
 - a. le format de signature par défaut est « PKCS#7 - Détaché »;
 - b. la case « Afficher les motifs » est cochée;
 - c. la case « Afficher l'emplacement et les coordonnées » est cochée;
 - d. la case « Inclure l'état de révocation de la signature » n'est pas cochée.
7. Cliquer sur « OK » pour fermer la fenêtre des préférences de création et d'aspect.
8. Cliquer sur « OK » pour fermer la fenêtre des préférences.



9. Fermer le logiciel.
10. Double-cliquer sur le fichier de registre (*.reg) précédemment téléchargé.
11. Dans la fenêtre « Éditeur du Registre », cliquer sur le bouton « Oui ».



12. Cliquer sur le bouton « OK » au message de l'éditeur du registre.

