

Signature électronique avancée avec Microsoft Office 2010

Version 1.0

Publication : mai 2010

Auteurs : Philippe Beraud (Microsoft France), Rémi Pifaut (KEYNECTIS)

*Copyright*

*© 2010* [*Microsoft Corporation*](http://www.microsoft.com)*. Tous droits réservés.*

Résumé

Nous communiquons tous de plus en plus, de plus ne plus vite. Par ailleurs, nous dématérialisons de plus en plus de documents et nous partageons et faisons partager de plus en plus d’informations et de créations, professionnelles, confidentielles, contractuelles, officielles et personnelles. Pour autant, *comment signer nos divers documents dans l’espace numérique, et ce comme nous le faisons depuis toujours dans la vie et le monde réel ? Comment donner au numérique toute la portée et toute la valeur légale que nous savons donner sur le papier avec une signature manuscrite ?*

Ce guide présente, en partenariat avec la société KEYNECTIS, la signature électronique avancée de documents et sa prise en charge dans Microsoft Office 2010 qui représente l’une des évolutions significatives de cette version de la suite Microsoft Office.

Il démontre son usage aisé au sein des applications Office, de concert avec des produits et services proposés par la société KEYNECTIS dans ce contexte, pour signer des documents et présente, dans ce cadre, les différents paramètres afférents pour la génération d’une signature électronique avancée et/ou sa vérification ultérieure au sein de la suite Office.



© 2010 Microsoft Corporation. Tous droits réservés.

Les informations contenues dans ce document représentent le point de vue actuel de Microsoft Corporation sur les sujets traités à la date de publication. Etant donné que Microsoft doit s’adapter aux conditions changeantes du marché, ces informations ne doivent pas être interprétées comme un engagement de la part de Microsoft, et Microsoft n’est pas en mesure de garantir l’exactitude de toute information présentée après la date de publication.

MICROSOFT NE DONNE AUCUNE GARANTIE EXPRESSE OU IMPLICITE DANS CE DOCUMENT.

Les autres noms de produits ou de sociétés cités dans ce document peuvent être des marques de leurs propriétaires respectifs.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • Etats-Unis

**Sommaire**

1 Introduction 1

1.1 Généralisation de la dématérialisation 1

1.2 Objectifs de ce guide 3

1.3 Organisation du guide 4

1.4 Audience de ce guide 4

1.5 À propos de ce guide 4

1.6 Principaux logiciels et services illustrés dans ce guide 5

2 Signature électronique avancée, de quoi s’agit-il ? 8

2.1 Signature électronique et certificat 8

2.2 Signature électronique avancée 10

2.3 Signature électronique qualifiée 12

3 Générer une signature électronique (avancée) dans les documents Office 13

3.1 Considérations relatives aux versions d’Office et formats de document 13

3.2 Notions de lignes de signature et de signature électronique invisible 15

3.3 Procédures 15

4 Contrôler et visualiser la signature avancée d’un document 20

4.1 Procédures 20

5 Configurer la prise en charge de la signature avancée 25

5.1 Configurer une installation locale 25

5.2 Configurer Office 2010 à l’échelle de l’entreprise 31

6 Remarques en guise de conclusion 37

7 Pour aller plus loin 38

8 Compiler et installer l’add-in de configuration pour Microsoft Word 2010 39

8.1 Configuration pour compiler l’add-in 39

8.2 Compiler l’add-in depuis Microsoft Visual Studio 2010 40

8.3 Installer l’add-in 40

9 Script de configuration des paramètres relatifs aux signatures électroniques (avancées) 42

10 Extrait du modèle de stratégie office14.adm relatif aux signatures électroniques (avancées) 47

# Introduction

## Généralisation de la dématérialisation

La dématérialisation a pour objet de gérer de façon totalement électronique des données ou des documents métier (correspondances, contrats, factures, brochures, contenus techniques, plans, supports administratifs, etc.) qui transitent au sein des entreprises et/ou dans le cadre d’échanges avec des partenaires (administrations, clients, fournisseurs…).

La dématérialisation, c’est le remplacement des documents papier par des fichiers informatiques, entraînant la mise en œuvre du fameux « bureau sans papier ».

Les échanges papier font donc et vont faire de plus en plus place aux échanges de documents numériques par différents réseaux d’acheminement (Internet, intranet, etc.).

Ce nouveau mode de communication se heurte cependant aux obstacles de la sécurité et de l’authentification des échanges. En effet, la [loi n°2000-230 du 13 mars 2000 portant sur l’adaptation du droit de la preuve aux technologies de l’information et relative à la signature électronique](http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200&dateTexte=20100510)[[1]](#footnote-1) (JO du 31 mars 2001) pose le principe de l’indépendance entre le document écrit et son support technique. Dès lors, un document électronique peut avoir la même valeur de preuve qu’un document papier.

Toutefois, ce document numérique doit remplir deux conditions :

* permettre l’identification de son auteur,
* être conservé dans des conditions de nature à garantir son intégrité.

Cette même loi a reconnu la validité juridique de la signature électronique au même titre que la signature manuscrite. Le [décret n°2001-272 du 30 mars 2001](http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=20100511)[[2]](#footnote-2) pris en application de la loi précitée détermine les conditions pour que des procédés de signature électronique puissent être considérés comme fiables, notamment le recours à des prestataires de services de certification qui délivreront des certificats de signature électronique après avoir vérifié l’identité des demandeurs.

En d’autres termes, les documents électroniques non munis d’une signature correspondant à ces critères n’auront aucune valeur de preuve juridique. C’est la raison pour laquelle on ne peut envisager de généraliser les applications de la dématérialisation et de tous les bénéfices qu’elles occasionnent pour une entreprise, sans certificat électronique.

La dématérialisation est un sujet concret, l’entreprise a compris qu’elle avait tout à y gagner : gain de temps, réduction de papier imprimé, meilleure communication intra et extra entreprise, amélioration de la productivité, retour spontané des services commerciaux, achats, techniques…

Chaque fonction dans l’entreprise, à son niveau, peut tirer profit de la dématérialisation : les tâches administratives sont réduites, et les gains de productivité, et de rendement sont optimisés.

Remplacer le courrier postal par du courrier électronique, en lui conférant une valeur légale, est l’un des atouts que peut exploiter toute entité. Ce sont, en outre, des réductions d’envois postaux et de coursiers qui sont visibles dans les frais internes de fonctionnement de la société.

Sur le plan juridique, une signature électronique égale une signature manuscrite. Conformément à la directive européenne, la loi n°2000-230 du 13 mars 2000 porte sur le droit de la preuve et de la signature électronique. D’une part, elle reconnaît juridiquement l’écrit sur support électronique comme équivalent à l’écrit sur support papier ; d’autre part, elle consacre la force probante de l’écrit électronique par l’usage d’un procédé fiable d’identification garantissant son lien avec l’acte auquel celui-ci se rattache.

Décret n°2001-272 du 30 mars 2001 :

* mise en œuvre d'une signature électronique sécurisée,
* la signature électronique sécurisée doit être établie grâce à un dispositif sécurisé de création de signature électronique,
* utilisation d'un certificat électronique qualifié pour vérifier la signature électronique.

Bulletin Officiel des Impôts, selon le n°136 du 7 août 2003,

« *Constitue une facture électronique sécurisée […],Toute facture ou flux de factures créé, transmis et archivé sous forme électronique dans un format qui permet de garantir l’intégrité et la pérennité de son contenu depuis son émission jusqu’à l’expiration de la période de stockage.* »

### Organiser la dématérialisation

Administrations, grandes entreprises, PME-PMI, toutes les entreprises, quelles que soient leurs tailles, sont concernées par la dématérialisation des échanges. Des nouveaux modes de fonctionnement se développent, avec à la clé plus de performance, de réactivité et de productivité.

Des fichiers confidentiels, aux chiffres clés de la société, en passant par les contrats signés, etc., les informations qui transitent par les réseaux peuvent être décisives, et engagent l’entreprise. Assurer la confidentialité des échanges est donc tout à fait essentiel. Il est donc nécessaire d’organiser la dématérialisation des informations dans l’entreprise car les risques liés au vol des données et à l’usurpation d’identité sont importants.

Pour cela, le certificat électronique qui permet de s’identifier sur Internet, de protéger et de garantir les données transmises constitue un moyen incontournable de sécurisation des transactions et des échanges dématérialisés.

### Certificat électronique

Un certificat électronique (Cf. section § 2.1.2 Certificat de signature et autorité de certification) est une carte d'identité numérique dont l'objet est d'identifier une entité physique ou non-physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique. Ce certificat électronique peut être instancié de différentes façons, sur son disque dur ou matérialisé sous forme de carte à puce ou de clé USB. Le certificat électronique permet de s’identifier sur Internet. Sa légitimité est liée à l’Autorité de certification qui le génère et à l’Autorité d’enregistrement qui le délivre.

Outre l’authentification de l’émetteur, le certificat permet d’assurer l’intégrité des documents échangés, avec l’assurance que le document reçu est identique au document initial. Avec un logiciel de signature, ou une application intégrée à un portail, le certificat permet également de signer des documents d’un simple clic de souris. Enfin, c’est une garantie juridique ; en effet, les documents signés par un certificat de classe 3+ (remis en face à face par une autorité légitime et sur un support cryptographique clé USB ou carte à puce) sont opposables aux tiers, en vertu des lois et décrets sur la signature électronique.

Pour protéger, authentifier, formaliser les échanges de toute entreprise qui utilise les outils Internet (Extranet, intranet, messagerie, etc.), le certificat électronique facilite la gestion des services dans l’entreprise. Ainsi, pour le service commercial, il permet la mise en place de catalogues en ligne, de bons de commandes, de factures ou de dossiers de candidature aux appels d’offres (à noter : toutes les administrations sont aujourd’hui dans l’obligation de pouvoir recevoir les dossiers des soumissionnaires en ligne). Pour le service des ressources humaines, il permet un traitement sécurisé des demandes de congés ou des notes de frais. Pour le service juridique, il permet l’échange et la remise de contrats ou d’envoyer les convocations aux assemblées générales.

En signant électroniquement les documents (lettres, contrats, bons de commande, factures, propositions commerciales, etc.), ils ne sont pas modifiables et vous pouvez leur conférer une valeur probante en fonction du contexte d’utilisation : ils sont ainsi opposables aux tiers.

Pour des raisons de sécurité d’identification, un certificat électronique est aussi généralement nécessaire pour l’ensemble des télé-procédures administratives proposées par l’Etat ou les collectivités locales.

### Solutions techniques associées

Pour sécuriser juridiquement ses échanges et les rendre confidentiels, il existe aujourd’hui des solutions techniques qui reposent sur l’utilisation des certificats électroniques. Des plates-formes hébergées par des Tiers de Confiance sont nécessaires, en complément des certificats, pour signer, dater, archiver, gérer des preuves électroniquement ou s’assurer de l’identité d’un destinataire.

On peut ainsi disposer :

* **de la signature électronique** : avec l’aide d’un système de signature, tous les documents électroniques peuvent devenir opposables aux tiers au même titre qu’un document manuscrit. En plus de certifier l’identité des signataires, la signature électronique assure que le document n’a pas été modifié depuis qu’il a été signé.
* **Du dépôt de documents avec horodatage chez un Tiers-Horodateur** : pour avoir les date et heure certifiées d’un document et la garantie de son intégrité.
* **D’un archivage légal chez un Tiers-Archiveur** : garantit une conservation de vos fichiers pendant au moins 10 ans et une restitution de ces derniers sous leur forme d’origine quelles que soient les évolutions technologiques.
* **D’un échange confidentiel** : pour être certain qu’un document envoyé électroniquement ne soit pas intercepté par quelqu’un d’autre, le destinataire présente son certificat électronique avant de pouvoir lire le message.

## Objectifs de ce guide

Ce guide vise à présenter, en partenariat avec la société [KEYNECTIS](http://www.keynectis.fr)[[3]](#footnote-3), la signature électronique avancée de documents et sa prise en charge dans Microsoft Office 2010 qui représente l’une des évolutions significatives de cette version de la suite Microsoft Office. Une telle signature est proposée dans Microsoft Excel 2010, PowerPoint 2010 et Word 2010.

Vous trouverez sur le [site officiel du produit Microsoft Office 2010](http://officebeta.microsoft.com)[[4]](#footnote-4) une [mise en route de Word 2010](http://officebeta.microsoft.com/fr-fr/products/word/mise-en-route-de-word-2010-HA010370239.aspx)[[5]](#footnote-5) avec notamment une présentation complète des nouveautés de cette version.

Pour plus d’informations, vous pouvez consulter l’aide de Word 2010 en ligne sur [Microsoft Office Online](http://officebeta.microsoft.com/fr-fr/word-help/)[[6]](#footnote-6) ainsi que les billets du [blog du groupe produit Microsoft Word 2010](http://blogs.msdn.com/microsoft_office_word/)[[7]](#footnote-7).

Ce document se veut une mise à jour et un complément du livre blanc [2007 Office System Document: Digital Signing of Microsoft 2007 Office System Documents](http://www.microsoft.com/downloads/details.aspx?FamilyId=79d06e72-4b45-4669-9eac-0eca5821e8ff&displaylang=en)[[8]](#footnote-8) (en anglais) sur la signature électronique dans Office System 2007.

La prise en charge native de la signature avancée vous permet de bénéficier de toute la protection prévue par le droit français et européen comme décrit dans l’[Article 1316-1 du Code civil](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=BD34C835AAE5B20B48E029125AC91D25.tpdjo02v_2?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006437813&dateTexte=20100510&categorieLien=id#LEGIARTI000006437813)[[9]](#footnote-9) :

« *L’écrit sous forme électronique est admis en preuve au même titre que l’écrit sur support papier sous réserve que puisse être dûment identifiée la personne dont il émane et qu’il soit établi et conservé dans des conditions de nature à en garantir l’intégrité.* »

[Loi n°2000-230 du 13 mars 2000 portant sur l’adaptation du droit de la preuve aux technologies de l’information et relative à la signature électronique](http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200&dateTexte=20100510)[[10]](#footnote-10) - [Directive européenne 1999/93/EC du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML)[[11]](#footnote-11)

## Organisation du guide

De façon à couvrir l’ensemble des considérations relatives à la signature électronique avancée d’un document Office, le présent document s’intéresse, dans un premier temps, à décrire ce qu’est, dans la pratique, une signature électronique avancée d’un document en abordant des considérations relatives aux cadres législatifs, à la recevabilité d’une telle signature, au(x) standard(s) qui la soutendent.

Le document présente ensuite la génération d’une signature avancée pour un document Office ainsi que sa vérification ultérieure, et aborde diverses considérations associées en termes de mise en œuvre.

Par ailleurs, ces principes de génération et de vérification de signatures électroniques avancées sont complétés dans un second temps par les éléments de configuration associés de ce support dans Microsoft Office 2010, que ce soit au niveau local pour une installation donnée ou à l’échelle d’une entreprise lors du déploiement de la suite Microsoft Office 2010 ou ultérieurement.

Enfin, des références fournies en annexe permettent de retrouver sur le Web des informations complémentaires.

## Audience de ce guide

Ce guide est principalement destiné aux trois audiences suivantes :

1. Les personnes qui souhaitent signer des documents Office avec une signature avancée ;
2. Les personnes qui souhaitent vérifier la signature de documents Office existants ;
3. Les personnes qui souhaitent mettre en œuvre une solution de signature de documents bureautiques.

## À propos de ce guide

 Ce guide a été développé en collaboration avec la société [KEYNECTIS](http://www.keynectis.fr)[[12]](#footnote-12). Leader européen des technologies et services de confiance, KEYNECTIS dispose d’une offre globale assurant la gestion des identités et la sécurisation des échanges électroniques pour le compte des gouvernements, des industriels et des institutions financières à travers le monde.

L’offre KEYNECTIS, logiciel ou service, bénéficie de l’expérience de plus de 25 millions de certificats électroniques émis et 10 millions de documents signés par ses technologies.

## Principaux logiciels et services illustrés dans ce guide

### Microsoft Office 2010

Comme le titre l’indique, ce guide prend en considération la version 2010 de Microsoft Office pour la signature électronique (avancée) de documents bureautiques Office.

note_dd Remarque : Dans Microsoft Office Starter 2010, vous pouvez ouvrir des documents signés numériquement, mais vous ne pouvez pas ajouter ni supprimer des signatures électroniques.

D’une façon générale, une telle signature est prise en charge pour les documents Word, Excel et PowerPoint au format par défaut, à savoir des fichiers au format Office Open XML. En effet, Microsoft Office 2010, tout comme Microsoft Office System 2007, s’appuie sur le format XML-DSig pour les signatures électroniques ; ce qui suppose à la base un format de document fondé sur la technologie XML (Extensible Markup Language).

Microsoft Office 2010 génère par défaut des fichiers conformes à la norme ISO 29500:2008 Office Open XML pour la classe de conformité « transitional ».

Pour mémoire, la version 2007 de Microsoft Office générait par défaut des fichiers conformes au standard international ECMA-376 Office Open XML 1ère Edition (décembre 2006) de l’Ecma International qui est le format précurseur de la norme ISO 29500:2008.

Depuis le 2 avril 2008, ce format ECMA-376 Office Open XML 1ère Edition a donné lieu à la norme ISO 29500:2008 ; le standard international ECMA-376 Office Open XML 2ième Edition (décembre 2008) correspond à cette norme.

Dans les faits, les spécifications Office Open XML décrivent un format de fichier amélioré et ouvert fondé sur la technologie XML.

Ce format de fichier standardisé puis normalisé procure de nombreux avantages ; il :

* permet de réduire de façon sensible la taille des documents ;
* contribue à réduire les risques d'altération des documents et améliore le potentiel de récupération ;
* aide à rendre vos documents plus sûrs.

Par ailleurs, ce format de fichier prend en charge de nombreuses autres fonctionnalités[[13]](#footnote-13), telles que des équations mathématiques, des outils graphiques SmartArt, des thèmes, etc.

Les procédures indiquées dans ce guide prennent en considération les caractéristiques du format Office Open XML tel que supporté par Microsoft Office 2010*.*

Comme décrit dans le billet [Open XML: One Year In](http://blogs.technet.com/office2010/archive/2009/11/19/open-xml-one-year-in.aspx)[[14]](#footnote-14), le passage du format ECMA-376 Office Open XML 1ère Edition au format ISO 29500:2008/ECMA-376 Office Open XML 2ième Edition induit quelques différences dans la syntaxe résultant à la fois de corrections de bogues ou de changements introduits dans la norme. Pour autant, il convient que les utilisateurs des précédentes versions d'Office puissent continuer de travailler avec des fichiers s’appuyant sur cette « nouvelle » syntaxe.

Pour de plus amples informations, les [spécifications d’Office Open XML](http://www.ecma-international.org/publications/standards/Ecma-376.htm)[[15]](#footnote-15) peuvent être téléchargées sur le site de l’Ecma International. Par ailleurs, les [notes d'implémentation Microsoft Office 2007 SP2 Office Open XML (ECMA-376 1ère Edition)](http://www.documentinteropinitiative.org/OASISODF1.1/reference.aspx)[[16]](#footnote-16) (et [informations additionnelles](http://www.documentinteropinitiative.org/additionalinfo/2007TOC.aspx)[[17]](#footnote-17)) ainsi que [celles relatives à l’implémentation de la norme ISO 29500:2008](http://www.documentinteropinitiative.org/ISO-IEC29500-2008/reference.aspx)[[18]](#footnote-18) (et [informations additionnelles](http://www.documentinteropinitiative.org/additionalinfo/2010TOC.aspx)[[19]](#footnote-19)) disponibles sur le [site Document Interop Initiative](http://www.documentinteropinitiative.org)[[20]](#footnote-20) donnent des informations détaillées sur la prise en charge par la suite Office des spécifications Office Open XML, qu’il s’agissent d’ECMA-376 1ère Edition et/ou d’ISO 29500 :2008/ ECMA-376 2ième Edition. Ces notes expliquent, entre autres choses, la prise en charge par la suite Office des fonctionnalités optionnelles, les plages de restrictions pour les valeurs d'attribut ainsi que les détails sur le mappage de fonctionnalités Office avec telle ou telle structure propre aux spécifications Office Open XML.

L’ensemble des évolutions induites par ISO 29500 :2008/ ECMA-376 2ième Edition a été intégré dans Office 2007 Service Pack 2 (SP2) pour garantir une compatibilité continue. Dans le même temps, le [pack de compatibilité pour Microsoft Office 2000, Office XP ou Office 2003](http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=941b3470-3ae9-4aee-8f43-c6bb74cd1466)[[21]](#footnote-21) qui permet aux versions précédentes d’Office d’ouvrir, de modifier et d’enregistrer des fichiers Office Open XML a également été mis à jour.

En d'autres termes, si vous disposez de Microsoft Office 2007 Service Pack 2 (SP2) ou de la dernière version du pack de compatibilité avec une précédente version d’Office, l’utilisation de fichiers Word 2010 sera transparente, à certaines considérations près vis-à-vis de la signature électronique (avancée) que nous précisons dans la suite de ce document.

Les illustrations données respectent la version finale de Microsoft Office 2010 en version française. De façon à tirer le meilleur profit de ce guide, il est nécessaire de disposer en parallèle de Microsoft Office 2010. L’ensemble des illustrations s’appuie sur Microsoft Word 2010 mais le propos et les procédures sont identiques avec Microsoft Excel 2010 et PowerPoint 2010.

Microsoft Office 2010 fonctionne sous Microsoft Windows XP Service Pack 3 (SP3), Windows Server 2003 R2, Windows Vista Service Pack (SP1), Windows Server 2008, Windows 7 ou ultérieur. Par défaut, Microsoft Office 2010 installe la version 32 bits d’Office 2010 même si votre ordinateur exécute des éditions 64 bits de Windows. La version 32 bits d’Office 2010 est l’option recommandée pour la plupart des utilisateurs, car elle permet d’éviter d’éventuels problèmes de compatibilité avec les autres applications.

Pour de plus amples informations sur la configuration requise, nous vous invitons à vous reporter à la [configuration système requise](http://technet.microsoft.com/fr-fr/library/ee624351(office.14).aspx)[[22]](#footnote-22) sur le [Centre de ressources Microsoft TechNet pour Microsoft Office 2010](http://technet.microsoft.com/fr-fr/office/ee263913.aspx)[[23]](#footnote-23).

### Produits et services de sécurité KEYNECTIS

Les éléments de configuration proposés pour la prise en charge de la signature électronique avancée dans Microsoft Office 2010 reposent sur les produits et services de sécurité suivants proposés par la société KEYNECTIS.

#### K.Stamp®

[K.Stamp](http://www.keynectis.fr/fr/produits-et-services/pki/kstamp-horodatage-electronique.html)[[24]](#footnote-24) est un module d’horodatage électronique. Disponible en mode service transactionnel ou en mode solution, K.Stamp vous permet d’apposer un jeton d’horodatage sur vos documents électroniques leur conférant ainsi intégrité et datation certaine. K.Stamp permet de gérer plusieurs sources de temps et s’appuie sur le standard [RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)](http://tools.ietf.org/html/rfc3161)[[25]](#footnote-25).

#### K.Valid®

[K.Valid](http://www.keynectis.fr/fr/produits-et-services/pki/kvalid-validation-certificat-ocsp.html)[[26]](#footnote-26) est un module de validation de certificat. Disponible en mode service transactionnel ou en mode solution, K.Valid permet aux applications acceptant des certificats électroniques provenant d’émetteurs divers, de s’adresser à un point de confiance unique, appelé Autorité de Validation, pour obtenir en temps réel l’état de validité du certificat grâce au protocole OCSP (Online Certificate Status Protocol) tel que décrit dans le standard [RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP](http://tools.ietf.org/html/rfc2560)[[27]](#footnote-27).

# Signature électronique avancée, de quoi s’agit-il ?

Comme mentionné en introduction, de plus en plus d’entreprises et de particuliers utilisent des documents numériques à la place de documents papier pour leurs opérations quotidiennes. En limitant nos besoins en matière de documents papier, nous protégeons l’environnement et nous préservons les ressources de la planète. Les signatures électroniques accompagnent ce changement en fournissant des garanties quant à la validité et l’authenticité d’un document numérique.

## Signature électronique et certificat

### Qu’est-ce qu’une signature électronique ?

Une signature électronique est un tampon d’authentification électronique chiffré sur des informations numériques comme des documents bureautiques dans le contexte de ce guide. La signature confirme que les informations proviennent du signataire et n’ont pas été modifiées.

L’image ci-après illustre une ligne de signature dans Office 2010.

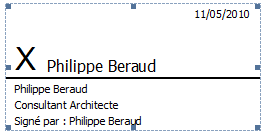


Figure 1. Ligne de signature dans Office 2010

### Certificat de signature et autorité de certification

Pour créer une signature électronique, vous avez besoin d’un certificat de signature qui prouve votre identité et de l’accès à la clé privée qui lui est associée. Lorsque vous envoyez un document signé numériquement, vous envoyez votre certificat et une clé publique.

Pour de plus amples informations les notions de clés privée et publique, vous pouvez consulter l’article MSDN [Asymmetric Keys](http://msdn.microsoft.com/en-us/library/aa387460(VS.85).aspx)[[28]](#footnote-28).

Les certificats sont émis par une autorité de certification et peuvent être révoqués, comme une carte d’identité. En règle générale, un certificat est valide entre un et trois ans. Au terme de cette période, le signataire doit renouveler le certificat de signature ou en obtenir un nouveau pour établir son identité.

Une autorité de certification (AC) est une entité similaire à un office notarial. Elle émet les certificats numériques, les signe pour empêcher toute modification (donc vérifier leur authenticité) et effectue le suivi des certificats ayant été révoqués ou étant arrivés à expiration.

Deux cas peuvent généralement se présenter en termes de certificats de signature :

1. **Certificats créés en utilisant l’infrastructure de gestion de clé publique de l’entreprise** - Les entreprises ont la possibilité de créer leur propre l’infrastructure de gestion de clé publique (IGC). Dans ce scénario, l’entreprise définit une ou plusieurs autorités de certification (AC) qui peuvent émettre des certificats électroniques pour les ordinateurs et utilisateurs de l'entreprise.

Lorsqu'une telle infrastructure est fondée sur les services de certificats Active Directory Certificate Services (AD CS) de Windows Server et combinée avec le service d'annuaire Active Directory, une entreprise peut reposer sur une solution complète intégrée qui permet i) à l’ensemble des ordinateurs gérés de disposer de la chaîne de confiance approuvée de l’entreprise avec les certificats des autorités de certification intermédiaires et racine associés et ii) à l’ensemble des utilisateurs et des ordinateurs de se voir attribuer (et renouveler dans le temps) automatiquement des certificats numériques pour le chiffrement et la signature des documents.

Cela autorise tous les collaborateurs d'une société à faire confiance automatiquement aux certificats numériques (et, par conséquent, de valider les signatures électroniques) des autres collaborateurs de cette même entreprise.

Pour de plus amples information sur les services AD CS, vous pouvez consulter le site dédié [Active Directory Certificate Services](http://go.microsoft.com/fwlink/?LinkId=119113)[[29]](#footnote-29).

Les entreprises peuvent aussi reposer sur la suite logicielle Sequoia de KEYNECTIS pour déployer leur propre infrastructure de gestion de clés. Quelle que soit la solution retenue pour la mise en place d’une infrastructure de gestion de clé publique au sein de votre entreprise, KEYNECTIS vous propose une reconnaissance universelle de vos certificats par tous vos interlocuteurs grâce à l’offre [Trust.Wider](http://go.microsoft.com/fwlink/?LinkId=119114)[[30]](#footnote-30). Cette offre permet une large utilisation des certificats à l’extérieur de l’entreprise, notamment pour faire reconnaitre les signatures de messages électroniques de type e-mail à l’ensemble de vos interlocuteurs comme vos clients, partenaires et fournisseurs.

1. **Certificats émis par une autorité commerciale** - Les certificats commerciaux sont achetés auprès d’une société dont l'activité en ligne consiste à vendre des certificats numériques.

L’un des principaux avantages de l'utilisation de certificats commerciaux est que le certificat racine de l’IGC relatif à ce service est automatiquement installé sur les systèmes d'exploitation Windows, qui permet à ces ordinateurs d’approuver automatiquement ces autorités de certification ; le certificat racine doit pour cela faire partie du programme Microsoft des certificats racine dont les modalités sont décrites dans l’article Microsoft TechNet [Microsoft Root Certificate Program](http://technet.microsoft.com/en-us/library/cc751157.aspx)[[31]](#footnote-31) et les membres courants dans l’article [Windows root certificate program members](http://support.microsoft.com/kb/931125/en-US)[[32]](#footnote-32).

Contrairement à la situation précédente, les certificats commerciaux vous permettent directement de partager vos documents signés avec des utilisateurs qui n'appartiennent pas à votre entreprise, sans qu’il ne soit besoin de déclarer un émetteur approuvé. Pour ajouter un éditeur approuvé, vous pouvez consulter l’article de l’aide en ligne [Ajouter, supprimer ou afficher un éditeur approuvé](http://office2010.microsoft.com/fr-fr/word-help/ajouter-supprimer-ou-afficher-un-editeur-approuve-HA010354309.aspx?CTT=5&origin=HA010354321)[[33]](#footnote-33)

Microsoft Office dispose de plusieurs solutions pour obtenir des certificats via [Office Marketplace](http://go.microsoft.com/fwlink/?LinkId=119114)[[34]](#footnote-34).

KEYNECTIS dispose de la capacité d’émettre des certificats pour le compte de ses clients, que ce soit par l’intermédiaire d’autorités de certification déjà en place et clientes de KEYNECTIS ou par l’intermédiaire de sociétés qui souhaitent mettre en place un système ou un service de gestion de certificats pour leur compte et le cas échéant celui de leurs clients, partenaires ou fournisseurs. Dans les deux cas de figure, KEYNECTIS vous apporte l’accompagnement nécessaire pour répondre à ce besoin de gestion de certificats.

### Garanties des signatures électroniques

Les termes et définitions ci-après montrent les garanties fournies par les signatures électroniques.

* **Authenticité** : le signataire est confirmé en tant que tel ;
* **Intégrité** : le contenu d’un document n’a pas été modifié ou falsifié depuis sa signature électronique ;
* **Non-répudiation** : prouve à toutes les parties l’origine du contenu signé. Le terme répudiation fait référence à l’acte d’un signataire rejetant tout lien avec le contenu signé ;
* **Notarisation** : dans certains cas, les signatures confirmées par un serveur d’horodatage sécurisé dans les fichiers Microsoft Excel 2010, PowerPoint 2010, ou Word 2010 ont la validité d’une notarisation. On parle alors de signature électronique avancée, Cf. section suivante éponyme.

Pour offrir ces garanties, le créateur du contenu doit le signer numériquement à l'aide d'une signature répondant aux critères suivants :

* La signature électronique est valide.
* Le certificat associé à la signature électronique est effectif (non expiré).
* La personne ou l’entreprise signataire, également appelée « éditeur », est approuvée.

important_ddImportant : les documents signés, dont l’horodatage est valide, sont considérés comme ayant des signatures valides, quelle que soit l’ancienneté du certificat de signature.

* Le certificat associé à la signature électronique est délivré à l’éditeur signataire par une autorité de certification reconnue.

L’image ci-après illustre les informations de certificat qui peuvent être consultées.

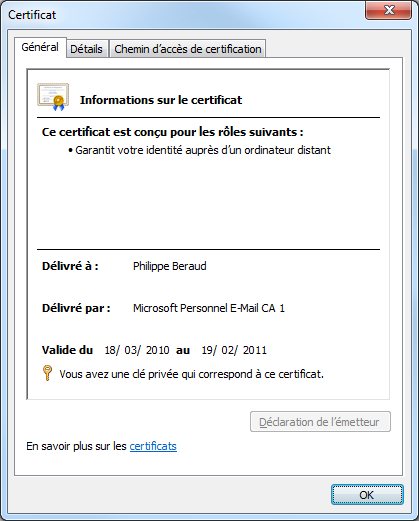


Figure 2. Informations sur le certificat électronique

## Signature électronique avancée

Une signature électronique avancée est susceptible de rester valide pendant de grandes périodes, conformément à la [Directive 1999/93/EC du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML)[[35]](#footnote-35) :

« *Une signature électronique avancée au sens de la directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques est une signature électronique qui satisfait aux exigences suivantes :*

1. *être liée uniquement au signataire ;*
2. *permettre d'identifier le signataire ;*
3. *être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;*
4. *être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.* »

Dans le contexte de documents fondés sur XML comme les documents au format Office Open XML de Microsoft Office 2010, le standard [RFC3275 (Extensible Markup Language) XML-Signature Syntax and Processing](http://tools.ietf.org/html/rfc3275)[[36]](#footnote-36) définit un format adapté pour les signatures électroniques.

Ce format XML-DSig a pour objectif principal de garantir l'intégrité du contenu d'un message ou d’un document et de confirmer l'identité de son émetteur. S'appuyant sur XML pour décrire et structurer les documents, cette spécification présente comme principal avantage d’autoriser plusieurs intervenants à signer différentes parties d'un même message, et ceci sans invalider les autres.

Le standard [XAdES (XML Advanced Electronic Signatures)](http://www.w3.org/TR/XAdES/)[[37]](#footnote-37) constitue un ensemble d'extensions hiérarchisées fondées sur XML-DSig et différant dans le niveau de protection offert.

Ces extensions concernent notamment le domaine de la non-répudiation en définissant des formats XML pour les signatures électroniques avancées dans l’acceptation précédente au sens de la Directive 1999/93/EC.

Le standard XAdES définit ainsi six niveaux ou profils (formes), chaque niveau inclut et prolonge le précédent pour fournir des signatures électroniques plus fiables. Par exemple, XAdES-X contient l’ensemble des capacités de XAdES-BES/EPES, XAdES-T et XAdES-C avec, en plus, les capacités propres à XAdES-X.

Microsoft Office 2010, tout comme Microsoft Office System 2007, utilise le format XML-DSig pour les signatures électroniques. XML-DSig. A cette prise en charge rendue possible par l’adoption du format de fichier XML standardisé et normalisé Office Open XML, Office 2010 ajoute la prise en charge du standard XAdES.

Le tableau suivant liste les niveaux disponibles dans Microsoft Office 2010 :

Tableau 1. Niveaux de signature (XAdES) disponibles

| Niveau de signature | Description |
| --- | --- |
| XAdES-BES/EPES | Forme de base répondant juste à des exigences légales directives pour la signature avancée |
| XAdES-T (horodateur) | Ajoute le champ d'horodateur pour se protéger contre la répudiation |
| XAdES-C (complet) | Ajoute des références aux données de vérification (certificats et listes de révocation) aux documents signés pour permettre la vérification en mode déconnecté et la vérification à l'avenir (mais ne stocke pas les données réelles) |
| XAdES-X (prolongé) | Ajoute des horodateurs sur les références présentées par XAdES-C pour se protéger contre le compromis possible à l’avenir des certificats dans la chaîne |
| XAdES-X-L (terme prolongé) | Ajoute les certificats et les listes réels de révocation au document signé pour permettre la vérification à l'avenir même si leur source originale n'est pas disponible |

Par défaut, Microsoft Office 2010 crée des signatures électroniques XAdES-EPES, si un certificat auto-signé ou un certificat signé par une autorité de certification est utilisé lors de la création de la signature électronique.

La configuration du niveau souhaité est décrite dans le chapitre § 5 Configurer la prise en charge de la signature avancée.

La possibilité avec Office 2010 d’ajouter un horodatage à une signature électronique permet de contribuer à prolonger la durée de vie d'une signature électronique. Par exemple, si un certificat révoqué précédemment a été utilisé pour la création de la signature électronique, qui contient un horodatage depuis un serveur d’horodatage de confiance, la signature électronique pourrait encore être considérée comme valide si l'horodatage est survenu avant la révocation du certificat. Pour utiliser la fonctionnalité d’horodatage avec les signatures électroniques, il convient de préciser, au niveau de la configuration d’Office 2010, l’URL d’un serveur d’horodatage conforme à la recommandation [RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)](http://tools.ietf.org/html/rfc3161)[[38]](#footnote-38), comme K.Stamp de la société KEYNECTIS dans le contexte de ce guide.

Des paramètres additionnels pour l’horodatage peuvent être précisés : il s’agit en l’occurrence de l’algorithme de hachage d’horodatage utilisé et du délai d’expiration du serveur d’horodatage. Ces éléments sont également décrits dans le chapitre mentionné ci-avant.

Si ces paramètres ne sont pas configurés, la valeur par défaut pour l’algorithme de hachage d’horodatage utilisée est SHA-1 et la durée par défaut qu’Office 2010 doit attendre pour le serveur d’horodatage pour la réponse à une demande est de 5 secondes.

## Signature électronique qualifiée

Pour être qualifiée, la signature électronique avancée doit se baser sur un certificat qualifié et être créée par un dispositif sécurisé. Elle doit aussi répondre aux exigences légales de la même manière qu’une signature manuscrite et sont recevables comme preuve en justice.

Le certificat qualifié doit, lui, comporter plusieurs indications :

* qu’il a été délivré à titre de certificat qualifié ;
* l’identification du prestataire de service de certification ;
* le nom du signataire ou son pseudonyme ;
* une qualité spécifique du signataire en fonction de l’usage auquel le certificat est destiné (par ex. avocat), si désiré ;
* la signature électronique avancée du prestataire de service de certification qui délivre le certificat ;
* la période de validité du certificat ;
* le cas échéant, les limites à la valeur de transactions.

Pour délivrer de tels certificats, le prestataire de service doit lui-aussi remplir certaines exigences. À titre d’exemple, citons qu’il doit prouver sa fiabilité et celle de son système et veiller à déterminer avec précision la date et l’heure d’émission et de révocation d’un certificat ; il assurera les services d’annuaire et de révocation surs et rapides ; son personnel sera qualifié et compétent ; il ne peut ni stocker ni copier les clés privées qu’il délivre ; il a le devoir d’information envers le public ; etc.

La société KEYNECTIS a obtenu, dans le cadre de son activité d’opérateur de service de confiance, la certification [ETSI TS 101 456](http://docbox.etsi.org/EC_Files/EC_Files/ts_101456v010101p.pdf)[[39]](#footnote-39) et a été le premier prestataire à émettre des certificats qualifiés en France.

# Générer une signature électronique (avancée) dans les documents Office

Vous pouvez signer numériquement des documents à l'aide de Microsoft Excel 2010, Microsoft PowerPoint 2010 et Microsoft Word 2010. Vous pouvez également ajouter une ligne de signature ou un horodatage de signature à l'aide de ces mêmes applications.

Ce chapitre aborde les modalités et procédures associées, après préciser dans les deux sections suivantes éponymes :

* les considérations relatives aux versions d’Office et formats de document ;
* les notions de lignes de signature et de signature électronique invisible propres à Microsoft Office 2010.

## Considérations relatives aux versions d’Office et formats de document

Lorsqu’un document Word est ouvert dans Word 2010, il s’ouvrira dans l'un des trois modes suivants :

1. « Word 2010 » correspondant à un document au format ISO 29500:2008/ECMA-376 Office Open XML 2ième édition pour la classe de conformité « transitional » ;
2. « Mode de compatibilité Word 2007 » correspondant à un document au format ECMA-376 Office Open XML 1ère édition ;
3. « Mode de compatibilité Word 97-2003 » correspondant à un document au format binaire dont la [spécification du format binaire (\*.doc)](http://www.microsoft.com/interop/docs/OfficeBinaryFormats.mspx)[[40]](#footnote-40) peut être téléchargée sur le site de Microsoft.

La signature avancée, objet de ce guide, est supportée pour les deux premiers modes.

Pour déterminer dans quel mode se trouve le document, il convient de vérifier la barre de titre du document. Si (mode de compatibilité) apparaît après le nom du fichier, le document est en mode de compatibilité de Word 2007 ou en mode de compatibilité avec Word 97-2003. Vous pouvez continuer à travailler en mode de compatibilité, ou vous pouvez convertir votre document au format de fichier Word 2010.

Pour convertir un document dans le format de fichier Word 2010, procédez de la façon suivante :

1. Cliquez sur l’onglet **Fichier** dans le coin supérieur gauche, le **mode Microsoft Office Backstage** s’active.
2. Réalisez l’une des opérations suivantes :

* Pour convertir le document sans enregistrer une copie, cliquez sur **Informations** et ensuite sur **Convertir**.
* Pour créer une nouvelle copie du document en mode Word 2010, cliquez sur **Enregistrer sous**, entrez un nouveau nom pour le document dans le champ **Nom de fichier** et puis cliquez sur **Document Word (\*.docx)** dans la liste déroulante **Type**.

Si, au contraire, un document est converti dans les précédents formats de Microsoft Word, le **Vérificateur de compatibilité Microsoft Word** répertorie les éléments dans le document qui ne sont pas pris en charge ou qui se comportent différemment dans Word 2007 ou au format Word 97-2003.

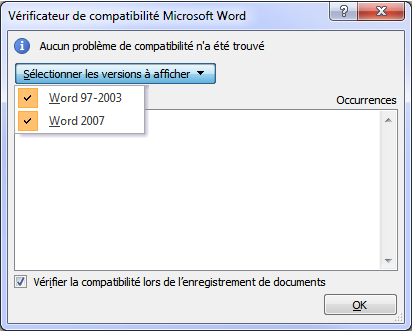


Figure 3. Sélection des versions à afficher pour la vérification de la compatibilité

Certaines de ces fonctionnalités seront définitivement modifiées et ne seront pas converties en éléments Word 2010, même si le document est ultérieurement converti au format Word 2010.

Au-delà de ces éléments, et dans le contexte précis de ce guide, **il est important d'être conscient que les signatures électroniques (avancées) générées dans Microsoft Office 2010 sont incompatibles avec les versions antérieures de Microsoft Office à Office System 2007.**

Par exemple, si un document est signé à l'aide d'une application Office 2010 (ou avec Office system 2007) et ouvert au sein d'une application Office 2003, qui dispose du [pack de compatibilité pour Microsoft Office 2000, Office XP ou Office 2003](http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=941b3470-3ae9-4aee-8f43-c6bb74cd1466)[[41]](#footnote-41) installé, l'utilisateur sera informé que le document a été signé par une version plus récente de Microsoft Office et que la signature électronique (avancée) sera perdue.

Par ailleurs, si le standard XAdES est utilisé dans Office 2010 pour la signature électronique, cette signature électronique ne sera pas compatible avec Office System 2007 à moins que la configuration d’Office 2010 fasse que l’objet de référence XAdES ne soit pas inclus dans le manifeste. Ceci suppose, par exemple, de désactiver le paramètre de stratégie de groupe **Ne pas inclure d’objet de référence XAdES** **dans le manifeste** (Do not include XAdES reference object in the manifest).

Si vous avez besoin de générer des signatures électroniques dans Office 2010 pour être compatible avec Office 2003 et versions antérieures, vous pouvez configurer le paramètre de stratégie de groupe **Signatures au format hérité (Legacy format signatures) et le définir comme activé**. Ce paramètre de stratégie de groupe se trouve sous :

User Configuration\Administrative Templates\(ADM\ADMX)\Microsoft Office 2010\Signing

Les applications Office 2010 utiliseront alors le format binaire Office 2003 pour appliquer des signatures électroniques aux documents au format binaire Office 97-2003 créés dans Office 2010.

Tous ces éléments sont décrits au chapitre § 5 Configurer la prise en charge de la signature avancée.

## Notions de lignes de signature et de signature électronique invisible

### Lignes de signature

Une ligne de signature dans Excel 2010 ou Word 2010 ressemble à un espace réservé à une signature pouvant se trouver sur un document imprimé. Elle fonctionne toutefois différemment. Lorsqu’une ligne de signature est insérée dans un fichier Office, l’auteur peut spécifier des informations et des instructions à l’attention du signataire. Lorsqu’une copie électronique du fichier est envoyée au signataire visé, celui-ci voit la ligne de signature et une notification lui signifiant que sa signature est requise.

Le signataire peut effectuer les opérations suivantes :

* taper une signature ;
* sélectionner une image numérique de signature ;

-ou-

* tracer une signature à l’aide de la fonctionnalité d’entrée manuscrite du Tablet PC.

Lorsque le signataire ajoute une représentation visible d’une signature au document, une signature électronique est ajoutée en même temps pour authentifier son identité.

important_ddImportant : un document signé numériquement passe en lecture seule pour empêcher toute modification ultérieure.

L’image ci-après illustre la barre des messages vous avertissant qu’un document signé est en mode de lecture seule.

Illustration du message "Marqué comme final"

Figure 4. Barre des messages pour un document signé

L’utilisation de lignes de signature dans les fichiers Office 2010 permet aux entreprises de limiter les risques lors de l’utilisation de transactions électroniques et de simplifier les procédures papier pour les contrats ou autres documents contractuels. Les signatures électroniques (avancées) fournissent un enregistrement de ce qui a été exactement signé et sont vérifiables ultérieurement.

Lorsque le signataire ajoute une signature visible au document, une signature électronique (avancée) est ajoutée en même temps pour authentifier l’identité. Une fois le document signé numériquement, il passe en lecture seule pour empêcher toute modification comme indiqué ci-avant.

### Signature électronique (avancée) invisible

Une signature électronique (avancée) invisible, telle qu’une ligne de signature invisible, garantit l’authenticité, l’intégrité et l’origine du document. Vous pouvez ajouter des signatures électroniques invisibles aux feuilles de calcul Excel, aux présentations PowerPoint et aux documents Word.

Le bouton **Signatures** apparaîtra en bas des documents signés. En outre, pour les documents signés, les informations de signature apparaissent dans la section **Informations** en **mode Microsoft Office Backstage**.

## Procédures

Les deux méthodes, les signatures électroniques (avancées) visibles et invisibles, utilisent un certificat numérique pour signer le classeur, la présentation ou le document. La différence est la représentation graphique dans le document lorsqu'une ligne de signature électronique visible est utilisée.

Nous détaillons ci-après les deux axes et procédures associées.

### Créer une ligne de signature

Pour créer une ligne de signature dans Excel 2010 ou Word 2010, procédez de la façon suivante :

1. Dans le document ou la feuille de calcul, positionnez le pointeur à l’emplacement où vous voulez ajouter une ligne de signature.
2. Sous l’onglet **Insertion**, dans le groupe **Texte**, cliquez sur la liste **Ligne de signature**, puis cliquez sur **Ligne de signature Microsoft Office**.
3. Dans la boîte de dialogue **Configuration de signature**, tapez les informations qui s’afficheront sous la ligne de signature :

* **Signataire suggéré** : nom complet du signataire ;
* **Fonction du signataire suggéré** : fonction du signataire, le cas échéant ;
* **Adresse de messagerie du signataire suggéré** : adresse de messagerie du signataire, le cas échéant ;
* **Instructions destinées au signataire** : ajoutez des instructions destinées au signataire ;
* **Permettre au signataire d’ajouter des commentaires dans la boîte de dialogue Signer** : permettre au signataire de taper un objet de signature ;
* **Afficher la date dans la ligne de signature** : la date de signature s’affichera avec la signature.

1. Cliquez sur **OK**.

L’image ci-après illustre la boîte de dialogue **Configuration de signature**.

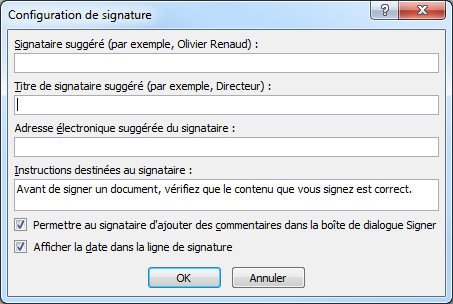


Figure 5. Configuration de la ligne de signature

Pour ajouter des lignes de signature supplémentaires, répétez les étapes précédentes.

Description: note_dd Remarque : Si le document reste non signé, la barre des messages Signatures apparaît. Cliquez sur le bouton Afficher les signatures pour terminer le processus de signature, ou, dans la barre, cliquez sur le lien pour accéder au mode Microsoft Backstage pour en savoir plus sur les autorisations, la distribution et les versions de ce document.

L’image ci-après illustre le bouton Afficher les signatures de la barre des messages.

Illustration du message "Signatures - ce document doit être signé"

Figure 6. Barre des messages pour un document à signer

### Signer la ligne de signature

Lorsque vous signez une ligne de signature dans Excel 2010 ou Word 2010, vous ajoutez une représentation visible de votre signature et une signature électronique.

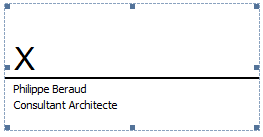


Figure 7. Ligne de signature à signer

Pour signer une ligne de signature, procédez de la façon suivante :

1. Dans le fichier, cliquez avec le bouton droit sur la ligne de signature.

Description: note_dd Remarque : Si le fichier s’ouvre en mode protégé, cliquez sur Modifier quand même si le fichier provient d’une source fiable.

1. Sélectionnez **Signer** dans le menu.

* Pour ajouter une version imprimée de votre signature, tapez votre nom dans la zone située en regard de X.

Ligne de signature

* Pour sélectionner une image de votre signature manuscrite, cliquez sur **Sélectionner une image**. Dans la boîte de dialogue **Sélectionner l'image de la signature**, localisez votre fichier d'image de signature, puis cliquez sur **Sélectionner**.

Description: note_dd Remarque : vous pouvez signer une ligne de signature en double-cliquant sur celle-ci. Tapez votre nom en regard de la croix (X). Vous pouvez également cliquer sur la flèche en regard de la signature dans la section Signatures requises du volet Signature. Dans le menu, sélectionnez Signer.

* Pour ajouter une signature manuscrite (utilisateurs de Tablet PC uniquement), signez votre nom dans la zone située en regard de la croix (**X**) à l'aide de la fonction de saisie manuscrite.
* Cliquez sur **Signer**.

Le bouton rouge **Signatures** apparaît en bas du document ou de la feuille de calcul.

L’image ci-après illustre le bouton **Signatures**.

Barre de statut ave le bouton Signatures

Figure 8. Bouton Signatures

### Supprimer des signatures électroniques (avancées)

Pour supprimer des signatures électroniques (avancées), procédez de la façon suivante :

1. Ouvrez le document ou la feuille de calcul contenant la signature visible à supprimer.
2. Cliquez avec le bouton droit sur la ligne de signature.
3. Sélectionnez **Supprimer la signature** dans le menu.
4. Cliquez sur **Oui**.

Description: note_dd Remarque : Vous pouvez en outre supprimer une signature en cliquant sur la flèche située en regard de celle-ci dans le volet Signature. Dans le menu, sélectionnez Supprimer la signature.

### Ajouter des signatures électroniques (avancées) invisibles

Pour protéger l’authenticité du contenu d’un document, vous pouvez ajouter une signature électronique (avancée) invisible. Le bouton **Signatures** apparaîtra en bas des documents signés. En outre, pour les documents signés, les informations de signature apparaissent dans la section **Informations** du **mode Microsoft Office Backstage**.

Pour ajouter des signatures électroniques (avancées) invisibles, procédez de la façon suivante :

1. Cliquez sur l’onglet **Fichier**. Le **mode Microsoft Office Backstage** apparaît.
2. Cliquez sur **Informations**.
3. Dans la section **Autorisations**, cliquez sur **Protéger le classeur**, **Protéger la présentation** ou **Protéger le document**.
4. Sélectionnez **Ajouter une signature numérique** dans le menu.
5. Lisez le message Microsoft Excel, PowerPoint ou Word, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Signer**, dans la zone **Objectif de la signature de ce document**, indiquez la raison.
7. Cliquez sur **Signer**.

Une fois le fichier signé numériquement, le bouton **Signatures** apparaît et le fichier devient en lecture seule pour empêcher toute modification.

L’image ci-après illustre les options **Protéger le document**.

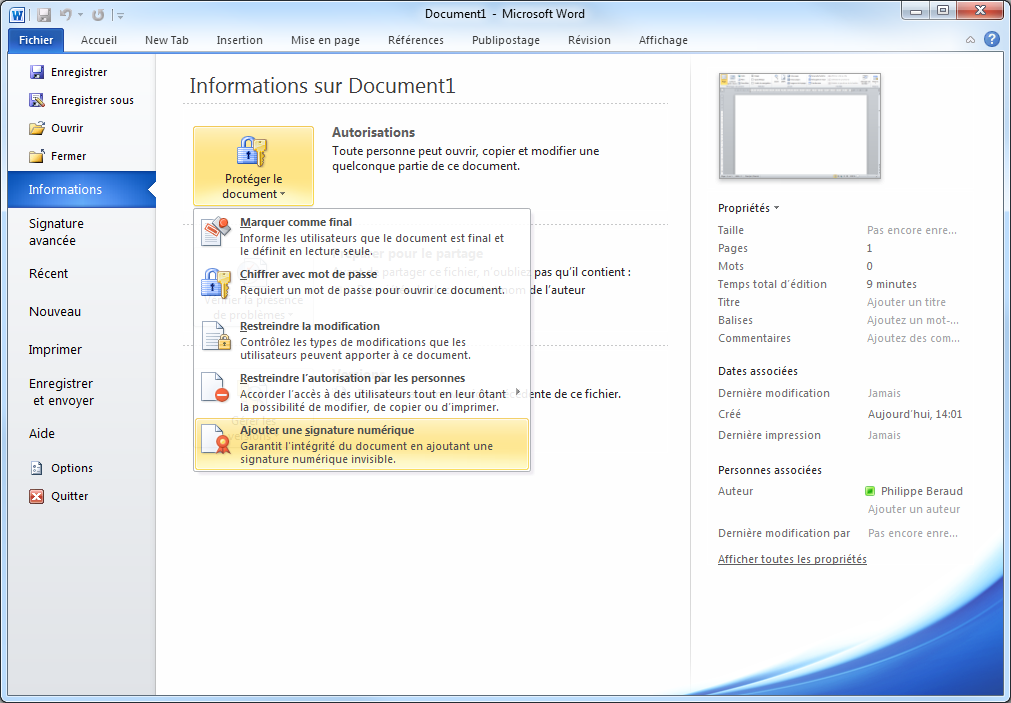


Figure 9. Option Ajouter une signature numérique

### Supprimer des signatures électroniques (avancées) invisibles

Pour supprimer des signatures électroniques (avancées) invisibles, procédez de la façon suivante :

1. Ouvrez la feuille de calcul, la présentation ou le document contenant la signature électronique (avancée) invisible à supprimer.
2. Cliquez sur l’onglet **Fichier**. Le **mode Microsoft Office Backstage** apparaît.
3. Cliquez sur **Informations**.
4. Cliquez sur **Afficher les signatures**.
5. L’affichage des documents, feuilles de calcul ou présentations réapparaît, ainsi que le volet **Signatures**.
6. Cliquez sur la flèche située en regard du nom de la signature.
7. Sélectionnez **Supprimer la signature** dans le menu.
8. Cliquez sur **Oui**.

# Contrôler et visualiser la signature avancée d’un document

Ce chapitre s’intéresse au contrôle et à la visualisation de la signature avancée à l’aide de la suite Microsoft Office 2010 sur toute la durée de vie du document, dans toutes les langues et ce sans aucun investissement additionnel pour le destinataire.

Vous pouvez afficher les informations relatives à une signature électronique (avancée) ou le certificat utilisé pour créer la signature électronique (avancée) dans Microsoft Excel 2010, PowerPoint 2010 et Word 2010.

Description: note_dd Remarque : comme précédemment indiqué, les signatures électroniques (avancées) ne peuvent pas être créées ou supprimées dans Microsoft Excel Starter 2010 ou Microsoft Word Starter 2010.

## Procédures

### Afficher les détails d’une signature électronique (avancée)

Pour afficher les détails des signatures électroniques (avancées), procédez de la façon suivante :

1. Ouvrez le fichier qui contient la signature électronique que vous souhaitez afficher.
2. Cliquez sur l’onglet **Fichier**. Le **mode Microsoft Office Backstage** apparaît.
3. Cliquez sur l’onglet **Informations**, puis sur **Afficher les signatures**. Le volet **Signatures** s’affiche.
4. Dans la liste, sur un nom de signature, cliquez sur la **flèche vers le bas**. Sélectionnez **Détails de la signature**.
5. La boîte de dialogue **Détails de la signature** s’affiche.

L’image suivante est un exemple de la boîte de dialogue **Détails de la signature**.

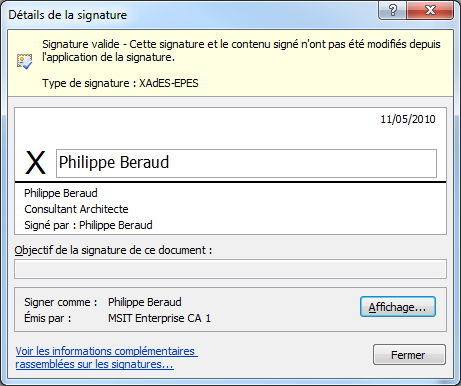


Figure 10. Détails de la signature

#### Messages de validité de la boîte de dialogue Détails de la signature

Des informations importantes relatives à la validité d’une signature électronique s’affichent dans la boîte de dialogue **Détails de la signature**. À partir de ces messages, vous pouvez déterminer si la signature correspond à l’un des états suivants :

* **Valide** : la signature est en cours de validité. Le certificat est approuvé ; il n’est pas arrivé à expiration ou n’a pas été révoqué.
* **Non valide** : Les raisons pour lesquelles une signature électronique est/peut devenir non valide sont les suivantes :
* La signature électronique est endommagée, car son contenu a été modifié ou falsifié ;
* Le certificat n’a pas été émis par une autorité de certification approuvée ; par exemple, il peut s’agir d’un certificat auto-signé. Si tel est le cas, vous devez choisir d’approuver un émetteur non approuvé pour rendre à nouveau la signature valide

Pour ajouter un éditeur approuvé, vous pouvez consulter l’article de l’aide en ligne [Ajouter, supprimer ou afficher un éditeur approuvé](http://office2010.microsoft.com/fr-fr/word-help/ajouter-supprimer-ou-afficher-un-editeur-approuve-HA010354309.aspx?CTT=5&origin=HA010354321)[[42]](#footnote-42) ;

* Le certificat utilisé pour créer la signature a été révoqué, et aucun horodatage n’est disponible.
* **Erreur récupérable** : Dans Office 2010, il existe une nouvelle catégorie de classification pour les signatures électroniques (avancées). Au lieu d’être valide ou non valide, une signature dans Office 2010 peut être qualifiée de signature contenant une erreur récupérable, ce qui signifie qu’il y a un problème avec la signature. Toutefois, l’erreur peut être résolue afin de rendre à nouveau la signature valide. Il existe trois scénarios pour les erreurs récupérables :

1. Le vérificateur est hors connexion (déconnecté d’Internet), ce qui empêche de vérifier les données de révocation de certificat, ou de vérifier si les horodatages sont présents ;
2. Le certificat utilisé pour créer la signature a expiré, et aucun horodatage n’est disponible ;
3. L’autorité de certification racine ayant émis le certificat n’est pas approuvée.

* **Signature partielle** : une partie d’un fichier est signée. Dans Office 2010, une signature électronique (avancée) valide signe certaines parties d’un fichier. Toutefois, vous pouvez créer une signature qui signe moins d’éléments que les parties requises. Cette signature partielle est valide du point de vue du chiffrement.

Office peut lire ces signatures. Toutefois, elles n’ont probablement pas été créées par un programme Office.

#### Niveaux et standards de signature électronique (avancée)

Outre le message de validité de la boîte de dialogue Détails de la signature, vous pouvez trouver des informations sur les niveaux de signature électronique respectant le standard XML-DSig pour la signature électronique (XML) et le standard XAdES pour les signatures électroniques avancées (XML) comme décrit à la section § 2.2 Signature électronique avancée.

important_ddImportant : Par défaut, Microsoft Excel 2010, PowerPoint 2010, et Word 2010 créent des signatures XAdES-BES/EPES. Le chapitre suivant § 5 Configurer la prise en charge de la signature avancée décrit les paramètres de configuration nécessaires pour créer des signatures électroniques avancées de niveau supérieur.

### Afficher les détails d’un certificat

La boîte de dialogue **Détails de la signature** affiche des informations sur le certificat, par exemple le nom du signataire dans la zone **Signer comme**, ainsi que l’identité de l’émetteur du certificat.

Pour afficher plus de détails sur le certificat, procédez de la façon suivante :

1. Ouvrez le fichier qui contient le certificat que vous souhaitez afficher.
2. Cliquez sur l’onglet **Fichier**. Le **mode Microsoft Office Backstage** apparaît.
3. Cliquez sur l’onglet **Informations**, puis sur **Afficher les signatures**. Le volet **Signatures** s’affiche.

L’image suivante est un exemple du volet **Signatures**.



Figure 11. Volet Signatures

1. Dans la liste, sur un nom de signature, cliquez sur la **flèche vers le bas**. Sélectionnez **Détails de la signature**.
2. La boîte de dialogue **Détails de la signature** s’affiche. Cliquez sur **Afficher**.
3. La boîte de dialogue **Certificat** s’affiche.

L’image suivante est un exemple de la boîte de dialogue **Certificat**.

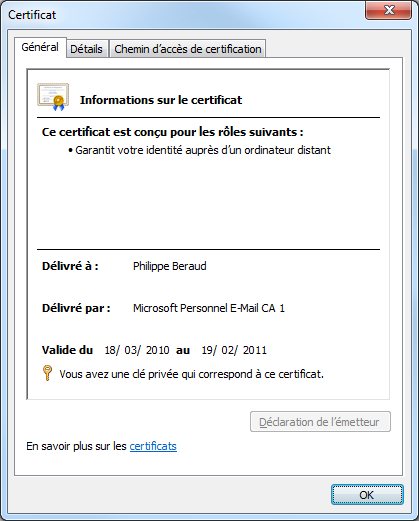


Figure 12. Boîte de dialogue Certificat

Dans la boîte de dialogue **Certificat**, des informations s’affichent à propos du certificat, par exemple, dans l’onglet **Général** :

* Délivré à ;
* Délivré par ;
* Période de validité du certificat ;
* État, tel que valide, expiré ou révoqué.

#### Informations complémentaires d’une signature électronique (avancée)

Lorsque vous signez numériquement un fichier Microsoft Excel 2010, PowerPoint 2010 ou Word 2010, la signature électronique (avancée) s’applique au contenu du fichier.

Cela inclut des informations qui risquent de ne pas être visibles dans l’affichage actuel du fichier. Ces programmes Office 2010 stockent également des informations supplémentaires dans la signature électronique (avancée) elle-même.

Pour afficher les informations complémentaires d’une signature électronique (avancée) depuis la boîte de dialogue **Détails de la signature**, procédez comme suit :

1. Cliquez sur **Voir les informations complémentaires rassemblées** sur les signatures.

La boîte de dialogue **Informations complémentaires** s’affiche.

L’image suivante est un exemple de la boîte de dialogue **Informations complémentaires**.

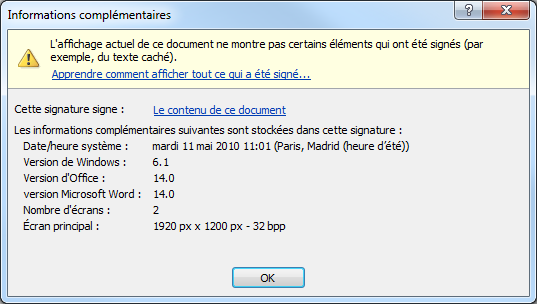


Figure 13. Informations complémentaires sur la signature

Les informations suivantes relatives à la signature s’affichent :

* Ce que signe la signature ;
* Date et heure locales de l’application de la signature ;
* Version du système d’exploitation Microsoft Windows installé ;
* Version du programme Microsoft Office installé ;
* Version du programme Microsoft Office utilisé ;
* Nombre de moniteurs installés ;
* Résolution du moniteur.

Vous pouvez voir éventuellement le message indiquant que le fichier n’affiche pas le contenu masqué.

#### Contenu masqué

Il existe parfois des informations non visibles dans le fichier, notamment du texte masqué.

Tableau 2. Informations non visibles

| Type de contenu | Action |
| --- | --- |
| Pour afficher les en-têtes et les pieds de page | Sous l’onglet **Affichage**, dans le groupe **Affichages de <types de fichiers>**, cliquez sur **Page** ou **Mise en page**. |
| Texte masqué dans des documents Word | Cliquez sur l’onglet **Fichier**. Le **mode Microsoft Office Backstage** apparaît. Sous **Aide**, cliquez sur **Options**. La boîte de dialogue **Options** s’affiche. Cliquez sur **Affichage**, puis sélectionnez **Texte masqué**. |

# Configurer la prise en charge de la signature avancée

Comme indiqué par avant et notamment à la section § 2.2 Signature électronique avancée, Microsoft Excel 2010, PowerPoint 2010, et Word 2010 créent par défaut des signatures XAdES-BES/EPES. Ce chapitre décrit les paramètres de configuration nécessaires pour créer des signatures électroniques avancées de niveau supérieur.

## Configurer une installation locale

Cette section s’intéresse à la configuration au niveau local des paramètres qui régissent les signatures électroniques (avancées) au niveau de Microsoft Office 2010.

### Configurer une installation locale en modifiant les valeurs de Registre

Dans la pratique, un certain nombre de valeurs de Registre permettent de configurer comment les signatures électroniques (avancées) sont configurée au niveau de l’installation locale.

Ces valeurs de Registre sont situées sous la clé :

HKEY\_CURRENT\_USER\Software\Microsoft\Office\14.0\Common\Signatures

Ces valeurs peuvent être modifiées via :

* l’exécution d’un fichier de Registre .reg adapté ;
* l’éditeur de Base de Registre (regedit.exe ou regedt32.exe) ;

important_ddImportant : toute modification incorrecte du Registre à l'aide de l'Éditeur du Registre ou d'une autre méthode peut entraîner des problèmes sérieux. Ces problèmes peuvent vous obliger à réinstaller le système d'exploitation. Microsoft ne peut pas garantir que ces problèmes puissent être résolus. Vous assumez l'ensemble des risques liés à la modification du Registre.

* l’exécution du script .vbs (Visual Basic Script) proposé également en complément dans le cadre de ce guide pour Windows Scripting Host (Cf. section § 5.1.3 Configurer une installation locale par script) ;
* l’add-in Configuration des signatures avancées (XAdES) pour Microsoft Office 2010 proposé en complément dans le cadre de ce guide (Cf. section § 5.1.2 Configurer une installation locale depuis Office 2010) ;
* une stratégie de groupe comme développé à la section § 5.2.1 Appliquer une stratégie de groupe.

Les valeurs de la Base de Registre concernées ainsi que les types et descriptions associés sont listés dans le tableau suivant.

Tableau 3. Valeurs de Registre régissant les signatures électroniques dans Microsoft Office 2010

| Valeur de Registre | Type | Description |
| --- | --- | --- |
| RequireOCSP | DWORD | Cette valeur vous permet de spécifier si Office 2010 requiert des données de révocation OCSP (Online Certificate Status Protocol) pour tous les certificats numériques dans une chaîne lors de la génération des signatures électroniques.  Si vous configurez cette valeur à 1, Office 2010 requiert des données de révocation OCSP pour tous les certificats dans une chaîne lors de la génération des signatures électroniques. Ces données sur le statut de révocation d’un certificat peuvent être fournies, par exemple, par le module de validation de certificat K.Valid de KEYNECTIS.  Si vous configurez cette valeur à 0 ou ne créez pas cette valeur, Office 2010 ne définit pas de restrictions sur le type de données de révocation devant être utilisé. |
| MinXAdESLevel | DWORD | Cette valeur vous permet de spécifier un niveau XAdES minimal que les applications Office 2010 doivent atteindre pour créer une signature électronique XAdES. Si elles ne parviennent pas à atteindre ce niveau minimal, les applications Office ne peuvent pas créer la signature.  Si vous configurez cette valeur, vous pouvez définir les niveaux XAdES minimaux suivants que les applications Office doivent atteindre avant de créer la signature électronique:   * 0 (défaut) : aucun niveau minimal * 1 : doit atteindre au moins le niveau XAdES-BES/EPES ou échec * 2 : doit atteindre au moins le niveau XAdES-T (horodateur) ou échec. * 3 : doit atteindre au moins le niveau XAdES-C (complet) ou échec * 4 : doit atteindre au moins le niveau XAdES-X (prolongé) ou échec * 5 : doit atteindre au moins le niveau XAdES-X-L (terme prolongé) ou échec   Si vous ne configurez pas cette valeur, Office 2010 ne requiert pas de niveau XAdES minimal et crée la signature XAdES la plus avancée possible, jusqu’au niveau spécifié par la valeur XAdESLevel. |
| XAdESValidationLevel | DWORD | Cette valeur vous permet de spécifier si Office 2010 doit vérifier ou non les parties XAdES d’une signature électronique, le cas échéant, lors de la validation d’une signature électronique d’un document.  Si vous configurez cette valeur à 1, Office 2010 vérifie les parties XAdES d’une signature électronique lors de sa validation.  Si vous configurez cette valeur à 0 ou ne créez pas cette valeur, Office 2010 valide uniquement les parties XML-DSig et XAdES-BES/EPES d’une signature électronique. |
| IgnoreExpiredCert | DWORD | Cette valeur vous permet de déterminer si les applications Office 2010 doivent accepter les certificats numériques arrivés à expiration lors de la vérification des signatures électroniques.  Si vous configurez cette valeur à 0, un certificat arrivé à expiration ne peut pas être utilisé pour vérifier une signature électronique.  Si vous configurez cette valeur à 1 ou ne créez pas ce paramètre de stratégie, les certificats numériques arrivés à expiration sont traités comme des certificats numériques valides. |
| O12CompatibleXAdES | DWORD | Cette valeur vous permet de déterminer si un objet de référence XAdES doit apparaître dans le manifeste.  Si vous configurez cette valeur à 0, la référence XAdES n’apparaît pas dans le manifeste.  Si vous configurez cette valeur à 1 ou ne créez pas cette valeur, la référence XAdES apparaît dans le manifeste. |
| SignatureHashAlg | REG\_SZ | Cette valeur vous permet de configurer l’algorithme de hachage utilisé par les applications Office 2010 pour valider les signatures électroniques.  Si vous configurez cette valeur, vous pouvez spécifier l’une des fonctions SHA standard suivantes :   * « sha1 » (défaut) * « sha256 » * « sha384 » * « sha512 »   Si vous ne créez pas cette valeur, « sha1 » est utilisé par défaut. |
| TSALocation | REG\_SZ | Cette valeur vous permet de définir l’URL HTTP pour le serveur d’horodatage utilisé par les applications Office 2010 dans le processus de validation des messages ou documents.  Si vous activez ce paramètre de stratégie, vous devez fournir une adresse URL HTTP valide du serveur d’horodatage utilisant par exemple le module d’horodatage électronique K.Stamp de KEYNECTIS.  Si vous ne créez pas cette valeur, un serveur d’horodatage n’est pas utilisé. |
| TSATimeout | DWORD | Cette valeur vous permet de configurer le nombre de secondes durant lesquelles les applications Office 2010 attendent une réponse du serveur d’horodatage avant l’expiration du délai. Si le délai arrive à expiration, l’application Office 2010 n'ouvre pas le message ou le document.  Si vous configurez cette valeur, le nombre de secondes spécifié correspond à la durée pendant laquelle Office 2010 attend le retour d’un résultat du serveur d’horodatage.  Si vous ne créez pas cette valeur, la valeur par défaut de 5 secondes est utilisée. |
| TimestampHashAlg | REG\_SZ | Cette valeur vous permet de configurer l’algorithme de hachage d’horodatage utilisé par les applications Office 2010 pour valider un message ou un document.  Si vous configurez cette valeur, vous pouvez spécifier une des fonctions d’algorithme de hachage standard suivantes :   * « sha1 » (défaut) * « sha256 » * « sha384 » * « sha512 »   Si vous ne créez pas cette valeur, « sha1 » est utilisé par défaut. |
| VerifyVersion | DWORD | Cette valeur vous permet de définir le niveau de vérification utilisé par les applications Office 2010 lors de la validation d’une signature électronique.  Si vous configurez cette valeur, vous pouvez définir le niveau de vérification sur l’une des options suivantes :   * 0 : aucune règle - les règles de signature électronique Office 2010 sont désactivées. * 1 (défaut) : règles Office 2007 - Office 2010 utilise les règles de signature électronique Office 2007. * 2 : règles Office 2010 - Office 2010 utilise les règles de signature électronique Office 2010.   Si vous ne créez pas cette valeur, Office 2010 utilise les règles de signature électronique Office 2007. |
| XAdESLevel | REG\_SZ | Cette valeur vous permet de spécifier un niveau XAdES demandé ou désiré lors de la création d’une signature électronique.  Si vous configurez cette valeur, vous pouvez spécifier le niveau XAdES lors de la création d’une signature électronique. Si le niveau XAdES désiré n’est pas atteint, le dernier niveau XAdES le plus élevé atteint est utilisé s’il est plus élevé que le niveau XAdES minimal (XAdES-BES/EPES).   * 0 : aucun niveau XAdES : XML-DSig - Aucun niveau XAdES * 1 (défaut) : niveau XAdES minimal * 2 : retour au niveau XAdES-BES/EPES si le niveau XAdES minimal < XAdES-T * 3 : retour au niveau XAdES-T si le niveau XAdES minimal < XAdES-C * 4 : retour au niveau XAdES-C si le niveau XAdES minimal < XAdES-X * 5 : retour au niveau XAdES-X si le niveau XAdES minimal < XAdES-X-L   Si vous ne créez pas cette valeur, le niveau XAdES-BES/EPES est utilisé (valeur 1). |

Le billet [Digital Signatures in Office 2010](http://blogs.technet.com/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx)[[43]](#footnote-43) peut être consulté à titre de complément.

### Configurer une installation locale depuis Office 2010

De façon à faciliter la configuration des différentes valeurs de Registre qui régissent les signatures électroniques (avancées) au niveau de Microsoft Office 2010, le présent guide propose, en termes de ressources complémentaires, un code source exemple, qui, une fois compilé avec Microsoft Visual Studio 2010 ou Visual C# 2010 Express, permet de disposer depuis Microsoft Word 2010 d’un add-in de configuration de la signature avancée (XAdES).

Ce code source est disponible dans le fichier archive Ressources Signature électronique avancée avec Microsoft Office 2010.zip qui accompagne le présent guide.

Le code source de cet add-in est publié sous le [contrat de licence de logiciel libre CeCILL-B](http://www.cecill.info/licences/Licence_CeCILL-B_V1-fr.txt)[[44]](#footnote-44). Le chapitre § 8 Compiler et installer l’add-in de configuration pour Microsoft Word 2010 décrit comme son nom l’indique les modalités de compilation et d’installation au niveau local.

Une fois l’add-in installé, pour configurer les différentes valeurs de Registre précédentes, procédez de la façon suivante :

1. Cliquez sur l’onglet **Fichier**. Le **mode Microsoft Office Backstage** apparaît.
2. Cliquez sur **Signature avancée**.
3. Dans la section **Génération des signatures**, sélectionnez la configuration adaptée à vos besoins.
4. Dans la section **Vérification des signatures**, sélectionnez la configuration adaptée à vos besoins.

La sélection du paramétrage souhaité entraîne automatiquement l’écriture dans le Registre de la valeur de Registre correspondante précisée à la section précédente. **Ce paramétrage sera pris en compte lors de la prochaine exécution de Microsoft Word 2010.**

Pour revenir à la configuration par défaut, cliquez sur l’un des boutons **Restaurer les valeurs par défaut**. L’ensemble des valeurs de registre listées à la section précédente est alors supprimée sous la clé : HKEY\_CURRENT\_USER\Software\Microsoft\Office\14.0\Common\Signatures

L’image ci-après illustre les paramètres de configuration exposés par l’add-in **Configuration de la signature avancée (XAdES)**.

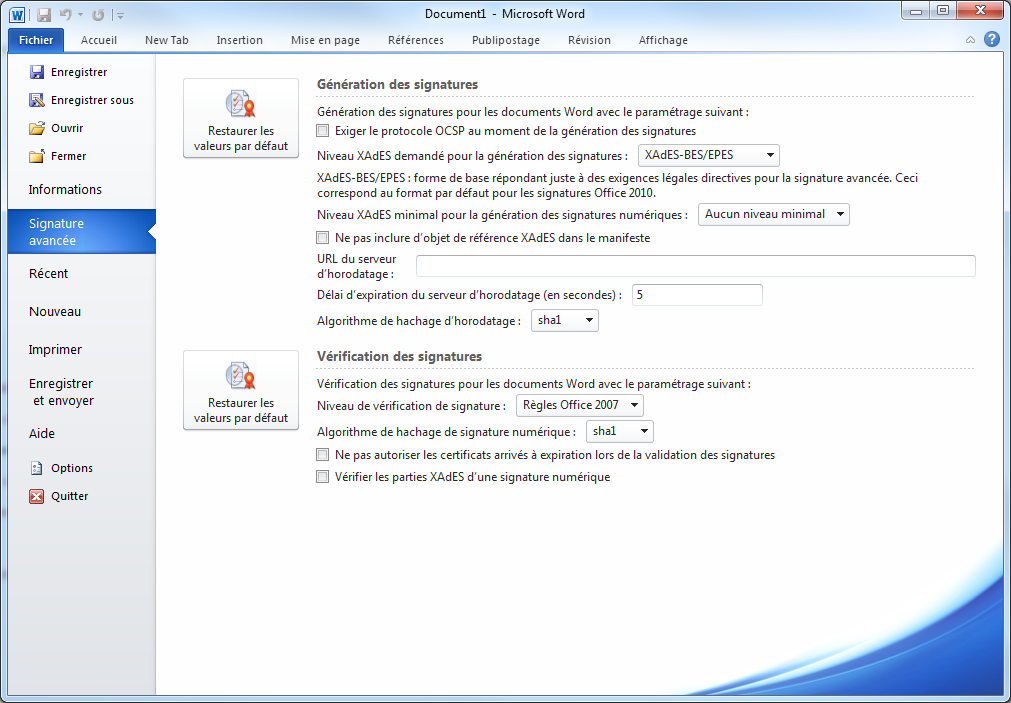


Figure 14. Add-in de configuration de la signature avancée (XAdES)

### Configurer une installation locale par script

Le présent guide propose également, en termes de ressources complémentaires, un script .vbs (Visual Basic Script) destiné à l’environnement d’exécution WSH (Windows Scripting Host) disponible sur les plateformes Windows. Ce script est disponible dans le fichier archive Ressources Signature électronique avancée avec Microsoft Office 2010.zip qui accompagne le présent guide.

Pour de plus amples informations sur WSH et les scripts .vbs, vous pouvez consulter les ressources proposées par le [ScriptCenter Microsoft TechNet](http://technet.microsoft.com/fr-fr/scriptcenter/default.aspx)[[45]](#footnote-45).

Le code de ce script est précisé au chapitre § 9 Script de configuration des paramètres relatifs aux signatures électroniques (avancées).

Pour afficher l’aide du script, procédez de la façon suivante :

1. Cliquez sur **Démarrer** puis sur **Exécuter…**
2. Saisissez *cmd* et cliquez sur **OK** pour ouvrir un invite de commande.
3. Tapez la commande suivante : *cscript XAdES.vbs /?*
4. Appuyez sur la touche ENTREE.

Cette commande produit la sortie suivante au niveau de l’invite de commande :

Microsoft (R) Windows Script Host Version 5.8

Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

XAdES.vbs - Advanced Signature (XAdES) Configuration for Microsoft Office 2010

Usage: /XAdESLevel:<0|1|2|3|4|5>

/MinXAdESLevel:<0|1|2|3|4|5>

/VerifyVersion:<0|1|2>

/TSATimeout:<0-500>

/RequireOCSP:<0|1>

/O12CompatibleXAdES:<0|1>

/IgnoreExpiredCert:<0|1>

/XAdESValidationLevel:<0|1>

/TSALocation:<http://>

/SignatureHashAlg:<sha1|sha256|sha384|sha512>

/TimestampHashAlg:<sha1|sha256|sha384|sha512>

/Show

/XAdESLevel: requested XAdES level for signature generation

0 (No XAdES)

1 (XAdES-BES/EPES)

2 (XAdES-T)

3 (XAdES-C)

4 (XAdES-X)

5 (XAdES-X-L)

/MinXAdESLevel: minimum XAdES level for digital signature generation (same values as XAdESLevel)

/VerifyVersion: signature verification level

0 (No rules)

1 (Office 2007 rules)

2 (Office 2010 rules)

/TSALocationocation: URL to the timestamp server

/TSATimeout: Timeout between 0 and 500 (included)

/RequireOCSP: require OCSP at signature generation time

/O12CompatibleXAdES: do not include XAdES reference object in the manifest

/IgnoreExpiredCert: do not allow expired certificates when validating signatures

/XAdESValidationLevel: check the XAdES portions of a digital signature

/SignatureHashAlg: digital signature hashing algorithm

sha1

sha256

sha384

sha512

/TimestampHashAlg: timestamp server timeout (same values as SignatureHashAlg)

/Show: Show values

Pour modifier depuis l’invite de commande, par exemple, le niveau XAdES demandé ou désiré lors de la création d’une signature électronique, procédez de la façon suivante :

1. Tapez la commande suivante : *cscript XAdES.vbs /XAdESLevel:2*
2. Appuyez sur la touche ENTREE.

## Configurer Office 2010 à l’échelle de l’entreprise

De façon à permettre une configuration de Microsoft Office 2010 à l’échelle de l’entreprise, Microsoft a publié à destination de Microsoft Office 2010des fichiers de modèle d'administration de stratégie de groupe (ADM, ADMX, ADML) et l'outil de personnalisation d'Office (OPO). Vous pouvez télécharger ces fichiers afférents depuis le Centre de téléchargement Microsoft : [Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool](http://go.microsoft.com/fwlink/?LinkId=189316)[[46]](#footnote-46).

Ce téléchargement comprend également :

* un classeur Excel intitulé Office2010GroupPolicyAndOCTSettings.xls qui fournit des informations sur les paramètres de stratégie de groupe d'Office 2010 et sur les paramètres OPA relatifs à l'outil de personnalisation d'Office ;
* les notes de version Office2010AdministrativeTemplateFilesDownload\_ReleaseNotes.doc qui fournissent des informations sur les paramètres qui diffèrent dans les paramètres de stratégie énumérés dans la référence Excel Office2010GroupPolicyAndOCTSettings.xls précédente.

Pour plus d'informations sur ce téléchargement, vous pouvez consulter l’article [Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool](http://go.microsoft.com/fwlink/?LinkId=190598)[[47]](#footnote-47).

Les sections suivantes s’appuient sur ces éléments pour la définition des éléments de configuration relatifs à la signature électronique avancée.

### Appliquer une stratégie de groupe

L’application d’une stratégie de groupe repose sur les fichiers de modèles d'administration intitulés office14 et proposés dans le cadre du téléchargement précédent.

Vous pouvez utiliser le fichier office14.adm pour tous les systèmes d'exploitation Windows ou la combinaison de fichiers office14.admx et office14.adml spécifiques à la langue sur des ordinateurs exécutant au moins Windows Vista ou Windows Server 2008.

Pour plus d'informations sur les fichiers .admx et .adml, vous pouvez consulter sur l’article Microsoft TechNet [Managing Group Policy ADMX Files Step-by-Step Guide](http://technet.microsoft.com/en-us/library/cc709647(WS.10).aspx)[[48]](#footnote-48).

Les fichiers office14 précédents contiennent un certain nombre de paramètres de stratégie de groupe qui permettent de configurer comment les signatures électroniques sont configurée et contrôlées au sein d’une entreprise.

Comme précédemment indiqué, les différentes valeurs de Registre mentionnées sont toutes situées sous la clé :

HKEY\_CURRENT\_USER\Software\Polices\Microsoft\Office\14.0\Common\Signatures

Les valeurs de Registre concernées (Cf. section précédente § 5.1 Configurer une installation locale) ainsi que les noms et descriptions relatifs des paramètres de stratégie de groupe sont listés dans le tableau suivant.

Tableau 4. Paramètres de stratégie de groupe régissant la signature électronique dans Microsoft Office 2010

| Valeur de Registre | Paramètre de stratégie de groupe | Description |
| --- | --- | --- |
| RequireOCSP | **Exiger le protocole OCSP au moment de la génération des signatures** (Require OCSP at signature generation time) | Ce paramètre de stratégie vous permet de déterminer si Office 2010 requiert des données de révocation OCSP (Online Certificate Status Protocol) pour tous les certificats numériques dans une chaîne lors de la génération des signatures électroniques.  Si vous activez ce paramètre de stratégie, Office 2010 requiert des données de révocation OCSP pour tous les certificats dans une chaîne lors de la génération des signatures électroniques. Ces données sur le statut de révocation d’un certificat peuvent être fournies, par exemple, par le module de validation de certificat K.Valid de KEYNECTIS.  Si vous désactivez ou ne configurez pas ce paramètre de stratégie, Office 2010 ne définit pas de restrictions sur le type de données de révocation devant être utilisé. |
| MinXAdESLevel | **Spécifier le niveau XAdES minimal pour la génération des signatures numériques** (Specify minimum XAdES level for digital signature generation) | Ce paramètre de stratégie vous permet de spécifier un niveau XAdES minimal que les applications Office 2010 doivent atteindre pour créer une signature électronique XAdES. Si elles ne parviennent pas à atteindre ce niveau minimal, les applications Office ne peuvent pas créer la signature.  Si vous activez ce paramètre de stratégie, vous pouvez définir les niveaux XAdES minimaux suivants que les applications Office doivent atteindre avant de créer la signature électronique :   * Aucun niveau minimal * XAdES-BES/EPES : doit atteindre au moins le niveau XAdES-BES/EPES ou échec * XAdES-T : doit atteindre au moins le niveau XAdES-T (horodatage) ou échec. * XAdES-C : doit atteindre au moins le niveau XAdES-C (références de certificat et de révocation) ou échec * XAdES-X : doit atteindre au moins le niveau XAdES-X (horodatage -C) ou échec * XAdES-X-L : doit atteindre au moins le niveau XAdES-X-L (stockage du certificat et valeurs de révocation) ou échec   Si vous désactivez ce paramètre de stratégie, Office 2010 ne requiert pas de niveau XAdES minimal et crée la signature XAdES la plus avancée possible, jusqu’au niveau spécifié par le paramètre de stratégie. |
| XAdESValidationLevel | **Vérifier les parties XAdES d’une signature numérique** (Check the XAdES portions of a digital signature) | Ce paramètre de stratégie vous permet de spécifier si Office 2010 doit vérifier ou non les parties XAdES d’une signature électronique, le cas échéant, lors de la validation d’une signature électronique d’un document.  Si vous activez ce paramètre de stratégie, Office 2010 vérifie les parties XAdES d’une signature électronique lors de sa validation.  Si vous désactivez ou ne configurez pas ce paramètre de stratégie, Office 2010 valide uniquement les parties XML-DSig et XAdES-BES/EPES d’une signature électronique. |
| IgnoreExpiredCert | **Ne pas autoriser les certificats arrivés à expiration lors de la validation des signatures** (Do not allow expired certificates when validating signatures) | Ce paramètre de stratégie vous permet de déterminer si les applications Office 2010 doivent accepter les certificats numériques arrivés à expiration lors de la vérification des signatures électroniques.  Si vous activez ce paramètre de stratégie, un certificat arrivé à expiration ne peut pas être utilisé pour vérifier une signature électronique.  Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les certificats numériques arrivés à expiration sont traités comme des certificats numériques valides. |
| O12CompatibleXAdES | **Ne pas inclure d’objet de référence XAdES dans le manifeste** (Do not include XAdES reference object in the manifest) | Ce paramètre de stratégie vous permet de déterminer si un objet de référence XAdES doit apparaître dans le manifeste.  Si vous activez ce paramètre de stratégie, la référence XAdES n’apparaît pas dans le manifeste.  Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la référence XAdES apparaît dans le manifeste. |
| SignatureHashAlg | **Sélectionner l’algorithme de hachage de signature numérique** (Select digital signature hashing algorithm) | Ce paramètre de stratégie vous permet de configurer l’algorithme de hachage utilisé par les applications Office 2010 pour valider les signatures électroniques.  Si vous activez ce paramètre de stratégie, vous pouvez spécifier l’une des fonctions SHA standard suivantes :   * SHA1 * SHA256 * SHA384 * SHA512   Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la valeur par défaut SHA1 est utilisée. |
| TSALocation | **Spécifier le nom du serveur d’horodatage** (Specify timestamp server name) | Ce paramètre de stratégie vous permet de définir l’URL HTTP pour le serveur d’horodatage utilisé par les applications Office 2010 dans le processus de validation des messages ou documents.  Si vous activez ce paramètre de stratégie, vous devez fournir une adresse URL HTTP valide du serveur d’horodatage utilisant par exemple le module d’horodatage électronique K.Stamp de KEYNECTIS.  Si vous désactivez ou ne configurez pas ce paramètre de stratégie, un serveur d’horodatage n’est pas utilisé. |
| TSATimeout | **Définir le délai d’expiration du serveur d’horodatage** (Set timestamp server timeout) | Ce paramètre de stratégie vous permet de configurer le nombre de secondes durant lesquelles les applications Office 2010 attendent une réponse du serveur d’horodatage avant l’expiration du délai. Si le délai arrive à expiration, l’application Office 2010 n'ouvre pas le message ou le document.  Si vous activez ce paramètre de stratégie, le nombre de secondes spécifié correspond à la durée pendant laquelle Office 2010 attend le retour d’un résultat du serveur d’horodatage.  Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la valeur par défaut de 5 secondes est utilisée. |
| TimestampHashAlg | **Configurer l’algorithme de hachage d’horodatage** (Configure time stamping hashing algorithm) | Ce paramètre de stratégie vous permet de configurer l’algorithme de hachage d’horodatage utilisé par les applications Office 2010 pour valider un message ou un document.  Si vous activez ce paramètre de stratégie, vous pouvez spécifier une des fonctions d’algorithme de hachage standard suivantes :   * SHA1 * SHA256 * SHA384 * SHA512   Si vous désactivez ou ne configurez pas ce paramètre de stratégie, SHA1 est utilisé. |
| VerifyVersion | **Définir le niveau de vérification de signature** (Set signature verification level) | Ce paramètre de stratégie vous permet de définir le niveau de vérification utilisé par les applications Office 2010 lors de la validation d’une signature électronique.  Si vous activez ce paramètre de stratégie, vous pouvez définir le niveau de vérification sur l’une des options suivantes :   * Aucune règle : les règles de signature électronique Office 2010 sont désactivées. * Règles Office 2007 : Office 2010 utilise les règles de signature électronique Office 2007. * Règles Office 2010 : Office 2010 utilise les règles de signature électronique Office 2010.   Si vous désactivez ou ne configurez pas ce paramètre de stratégie, Office 2010 utilise les règles de signature électronique Office 2007. |
| XAdESLevel | **Niveau XAdES demandé pour la génération des signatures** (Requested XAdES level for signature generation) | Ce paramètre de stratégie vous permet de spécifier un niveau XAdES demandé ou désiré lors de la création d’une signature électronique.  Si vous activez ce paramètre de stratégie, vous pouvez spécifier le niveau XAdES lors de la création d’une signature électronique. Si le niveau XAdES désiré n’est pas atteint, le dernier niveau XAdES le plus élevé atteint est utilisé s’il est plus élevé que le niveau XAdES minimal (XAdES-BES/EPES).   * Aucun niveau XAdES : XML-DSig - Aucun niveau XAdES * XAdES-BES/EPES : niveau XAdES minimal (valeur par défaut) * XAdES-T : retour au niveau XAdES-BES/EPES si le niveau XAdES minimal < XAdES-T * XAdES-C : retour au niveau XAdES-T si le niveau XAdES minimal < XAdES-C * XAdES-X : retour au niveau XAdES-C si le niveau XAdES minimal < XAdES-X * XAdES-X-L : retour au niveau XAdES-X si le niveau XAdES minimal < XAdES-X-L   Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le niveau XAdES-BES/EPES est utilisé. |

Des paramètres additionnels de stratégie de groupe viennent compléter, le cas échéant, les paramètres précédents. Il s’agit des paramètres suivants :

* **Filtrage d’utilisation de la clé (Key Usage Filtering)** ;
* **Définir le répertoire d’images par défaut (Set default image directory) ;**
* **Filtrage EKU (EKU filtering)**;
* **Signatures au format hérité (Legacy format signatures)**;
* **Supprimer les fournisseurs de signature Office (Suppress Office Signing Providers)**;
* **Supprimer l’élément de menu des services de signature externes (Suppress external signature services menu item).**

Pour de plus amples informations sur chaque paramètre de stratégie de groupe, vous pouvez consulter les fichiers d’aide qui accompagnent les fichiers de modèle d’administration pour Office 2010.

Le [Kit de ressources Microsoft Office 2010](http://technet.microsoft.com/fr-fr/library/cc303401(office.14).aspx)[[49]](#footnote-49) fournit des informations sur les nouvelles fonctionnalités et sur les changements dans les stratégies de déploiement d'Office 2010.

Cette documentation s'adresse aux professionnels de l'informatique qui planifient, implémentent et gèrent des installations Office au sein de leur organisation. Cette dernière s’intéresse notamment au support de la signature avancée dans Microsoft Office 2010.

La définition et l’application de stratégies de groupe dépassent le cadre et l’objet de ce document. Pour l’utilisation de cet outil. En termes de procédures, au-delà des éléments développés ici dans le cadre de ce guide, vous pouvez consulter en particulier les articles Microsoft TechNet suivants : [Plan digital signature settings for Office 2010](http://technet.microsoft.com/fr-fr/library/cc545900(office.14).aspx)[[50]](#footnote-50), [Group Policy overview for Office 2010](http://technet.microsoft.com/fr-fr/library/cc179176(office.14).aspx)[[51]](#footnote-51), [Enforce settings by using Group Policy in Office 2010](http://technet.microsoft.com/fr-fr/library/cc179081(office.14).aspx)[[52]](#footnote-52).

### Personnaliser l’installation de Microsoft Office

Le téléchargement [Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool](http://go.microsoft.com/fwlink/?LinkId=189316)[[53]](#footnote-53) disponible sur le Centre de téléchargement Microsoft contient un dossier \Admin avec l’outil de personnalisation d'Office mis à jour.

L'outil de personnalisation Office (OPO) fait partie du programme d'installation de Microsoft Office 2010 et permet la personnalisation des installations. Le téléchargement ci-avant permet de disposer dans ce cadre avec les fichiers office14.opax/.opal d’un paramétrage similaire à celui exposé pour les stratégies de groupe à la section précédente.

La mise en œuvre de cet outil dépasse le cadre et l’objet de ce document. Pour l’utilisation de cet outil avec les fichiers office14.opax/.opal, vous pouvez consulter les articles Microsoft TechNet suivants : [Outil de personnalisation Office dans Office System 2010](http://technet.microsoft.com/fr-fr/library/cc179097(office.14).aspx)[[54]](#footnote-54) et [Configurer des paramètres utilisateur pour Office 2010](http://technet.microsoft.com/fr-fr/library/cc178990(office.14).aspx)[[55]](#footnote-55).

# Remarques en guise de conclusion

Ce document introduit les quelques notions clés vis-à-vis de la signature avancée et présente les axes de mise en œuvre à observer pour permettre à toute personne qui le souhaite de signer ou de vérifier la signature d’un document produit avec Microsoft Office 2010.

Ce guide nous a permis de démontrer pour cela les nouvelles fonctionnalités proposées par la version 2010 de la suite Microsoft Office. Ces fonctionnalités ont été illustrées avec Microsoft Word 2010.

Les principes ainsi que les éléments et modalités de configuration mis en exergue sont similaires voir identiques avec les autres Microsoft Excel 2010 et PowerPoint 2010.

# Pour aller plus loin

Pour des informations générales sur la société KEYNECTIS et ses produits et services de sécurité, nous vous invitons à consulter le [site de KEYNECTIS](http://www.keynectis.com/)[[56]](#footnote-56).

Pour des informations générales sur Microsoft et la sécurité, nous vous invitons à consulter le [site dédié](http://www.microsoft.com/france/securite)[[57]](#footnote-57).

Pour des informations générales sur Microsoft Office 2010, nous vous invitons à consulter le [site Microsoft France Office](http://www.microsoft.com/france/office)[[58]](#footnote-58) et, pour des informations plus techniques, le [Centre de ressources Microsoft TechNet pour Microsoft Office 2010](http://technet.microsoft.com/fr-fr/office/ee263913.aspx)[[59]](#footnote-59).

# Compiler et installer l’add-in de configuration pour Microsoft Word 2010

## Configuration pour compiler l’add-in

### Prérequis

Le code source de l’add-in de configuration proposé pour Word 2010 comme ressource complémentaire et publié sous le [contrat de licence de logiciel libre CeCILL-B](http://www.cecill.info/licences/Licence_CeCILL-B_V1-fr.txt)[[60]](#footnote-60) est disponible dans le fichier archive Ressources Signature électronique avancée avec Microsoft Office 2010.zip qui accompagne le présent guide.

Il nécessite les éléments suivants pour sa compilation :

* Microsoft .NET Framework 3.5 Service Pack 1 (SP 1)
* Mise à jour KB959209 du Microsoft .NET Framework 3.5 Service Pack 1 (SP 1)
* Microsoft Visual Studio 2010 (ou Microsoft Visual C# 2010 Express Edition)

Le Microsoft .NET Framework 3.5 Service Pack 1 (SP1) est le modèle de programmation de code managé pour la plateforme Windows. Il combine la puissance du .NET Framework 2.0 avec de nouvelles techniques pour le développement d’applications qui communiquent très facilement au-delà des frontières technologiques, et qui sont capables de prendre en charge un large éventail de processus métiers.

Pour des informations complémentaires sur le Microsoft .NET Framework, veuillez consulter le [Centre de développement MSDN éponyme dédié](http://msdn.microsoft.com/fr-fr/netframework/default.aspx)[[61]](#footnote-61).

Le [package redistribuable Microsoft .NET Framework 3.5 SP1](http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7)[[62]](#footnote-62) est disponible par téléchargement gratuit sur le Centre de téléchargement Microsoft. Microsoft .NET Framework 3.5 SP1 est une mise à jour cumulative qui contient de nombreuses nouvelles fonctionnalités qui sont construites par incréments à partir de .NET Framework 2.0 et 3.0, et inclut les mises à jour cumulatives de .NET Framework 2.0 Service Pack 2 et de .NET Framework 3.0 Service Pack 2.

La [mise à jour KB959209 pour .NET Framework 3.5 SP1](http://go.microsoft.com/fwlink/?LinkId=136730)[[63]](#footnote-63) est disponible par le biais d’un téléchargement gratuit sur le Centre de téléchargement Microsoft. :.

Les outils de développement pour .NET Framework 3.5 SP1 permettent aux développeurs de prendre en charge la création d’applications .NET Framework 3.5 SP1 à l’aide de Visual Studio 2010 ou Visual C# 2010 Express Edition.

Vous pouvez télécharger Microsoft Visual C# 2010 Express Edition gratuitement depuis le [site Microsoft Visual Studio Express Editions](http://msdn.microsoft.com/fr-fr/express/default.aspx)[[64]](#footnote-64).

### Installation des composants nécessaire

Vous trouverez ci-dessous la procédure d’installation pour la mise en place d’un environnement de développement pour Microsoft .NET Framework 3.5 SP1 :

1. Installez Microsoft .NET Framework 3.5 SP1 ainsi que la mise à jour KB959209. Cette installation n’est pas nécessaire pour Windows 7 et Windows 2008 R2 puisque ces systèmes d'exploitation incluent déjà le .NET Framework 3.5 SP1. Cependant, assurez-vous d’utiliser la version finale de Windows 7 ou de Windows Server 2008 R2 afin de disposer de la configuration adéquate du .NET Framework 3.5 SP1.
2. Installez Microsoft Visual Studio 2010 (ou à défaut Microsoft Visual C# 2010 Express Edition).

## Compiler l’add-in depuis Microsoft Visual Studio 2010

Pour compiler l’add-in depuis Microsoft Visual Studio 2010 (ou à défaut Microsoft Visual C# 2010 Express Edition), procédez de la façon suivante :

1. Décompressez le fichier archive Ressources Signature électronique avancée avec Microsoft Office 2010.zip dans un dossier.
2. Ouvrez Windows Explorer et placez-vous dans le sous-répertoire Add-in\Source du répertoire d’extraction.
3. Double-cliquez sur l’icône du fichier XAdESAddIn.sln situé dans le sous-répertoire *Source* pour ouvrir le fichier dans l’environnement Visual Studio.
4. Dans le menu **Compilation**, choisissez **Recompiler la solution**. L’add-in est alors compilé dans le sous-répertoire Add-In\Source\bin\[Debug|Release]. Le sous-répertoire Debug ou Release dépend de votre choix lors de la compilation (mode Débogage ou non).

-ou-

Pour créer directement un package d’installation de l’add-in, depuis le menu **Compilation**, choisissez **Publier XAdESAddIn**. L’assistant de publication s’ouvre et vous propose de publier la package d’installation dans le sous-dossier Add-in\Publish du répertoire d’extraction. Cliquer sur **Terminer** pour créer le sous-dossier Add-in\Publish et le package dans celui-ci.

Les fichiers présents sous le sous-dossier correspondent au programme d’installation.

## Installer l’add-in

Pour installer l’add-in depuis le sous-dossier Add-in\Publishdu dossier d’extraction, procédez de la façon suivante :

1. Ouvrez Windows Explorer et placez-vous dans le sous-répertoire Add-in\Publish du répertoire d’extraction créé à la section précédente.
2. Double-cliquez sur le fichier Setup.exe pour lancer le programme d’installation. La fenêtre **Programme d’installation de la personnalisation Microsoft Office** s’ouvre.

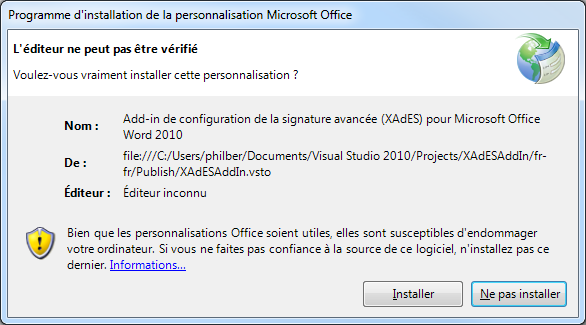


Figure 15. Fenêtre du programme d'installation de la personnalisation Microsoft Office

1. Cliquez sur le bouton **Installer**.

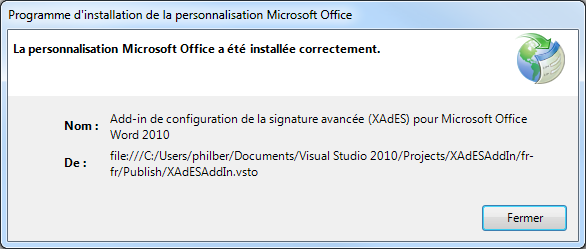


Figure 16. Fenêtre de confirmation de l'installation

1. Cliquez sur le bouton **Fermer**. L’add-in est installé.

# Script de configuration des paramètres relatifs aux signatures électroniques (avancées)

Le script suivant propose un exemple pour la configuration depuis l’environnement Windows Scripting Host des différents paramètres qui régissent les signatures électroniques (avancées) dans Microsoft Office 2010.

Ce script est disponible dans le fichier archive Ressources Signature électronique avancée avec Microsoft Office 2010.zip proposé en complément du présent guide. Il est situé dans le sous-dossier Script de cette archive.

' XAdES.vbs - Advanced Signature (XAdES) Configuration Script for Microsoft Office 2010

'

' Usage and help provided by typing "XAdES.vbs /?"

'

Option Explicit

Const ValueNoSet = "Not set (default value applies)"

Const HKEY\_CURRENT\_USER = &H80000001

Const HKEY\_LOCAL\_MACHINE = &H80000002

Const regkey = "Software\Microsoft\Office\14.0\Common\Signatures\"

Dim oReg 'As Object

Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv")

Dim RequiredOCSP, prevRequiredOCSP 'As Integer

Dim XAdESLevel, prevXAdESLevel 'As Integer

Dim XAdESMinLevel, prevXAdESMinLevel 'As Integer

Dim O12CompatibleXAdES, prevO12CompatibleXAdES 'As Integer

Dim TSATimeout, prevTSATimeout 'As Integer

Dim VerIfyVersion, prevVerIfyVersion 'As Integer

Dim XAdESValidationLevel, prevIgnoreExpiredCert 'As Integer

Dim IgnoreExpiredCert, prevXAdESValidationLevel 'As Integer

Dim TSALocation, prevTSALocation 'As String

Dim TimestampHashAlg, prevTimestampHashAlg 'As String

Dim SignatureHashAlg, prevSignatureHashAlg 'As String

Call Main()

Sub Main ()

WScript.Echo "XAdES.vbs - Advanced Signature (XAdES) Configuration for Microsoft Office 2010"

WScript.Echo ""

Call RetrieveValues()

If WScript.Arguments.count = 0 Or \_

WScript.Arguments.Named.Exists("?") Or \_

WScript.Arguments.Named.Exists("help") Then

PrintUsage

WScript.Quit

End If

Call SetValues()

If WScript.Arguments.Named.Exists("Show") Then

Call PrintCurrentValues()

Else

Call PrintPreviousValues()

Call PrintCurrentValues()

End If

End Sub

Function GetLevelNameById(id)

Select Case id

Case 0

GetLevelNameById = "No XAdES"

Case 1

GetLevelNameById = "XAdES-BES/EPES"

Case 2

GetLevelNameById = "XAdES-T"

Case 3

GetLevelNameById = "XAdES-C"

Case 4

GetLevelNameById = "XAdES-X"

Case 5

GetLevelNameById = "XAdES-X-L"

Case Else

GetLevelNameById = ValueNoSet & " or Invalid Value"

End Select

End Function

Sub PrintUsage()

WScript.Echo "Usage: /XAdESLevel:<0|1|2|3|4|5>"

WScript.Echo " /MinXAdESLevel:<0|1|2|3|4|5>"

WScript.Echo " /VerIfyVersion:<0|1|2>"

WScript.Echo " /TSATimeout:<0-500>"

WScript.Echo " /RequireOCSP:<0|1>"

WScript.Echo " /O12CompatibleXAdES:<0|1>"

WScript.Echo " /IgnoreExpiredCert:<0|1>"

WScript.Echo " /XAdESValidationLevel:<0|1>"

WScript.Echo ""

WScript.Echo " /TSALocation:<http://>"

WScript.Echo " /SignatureHashAlg:<sha1|sha256|sha384|sha512>"

WScript.Echo " /TimestampHashAlg:<sha1|sha256|sha384|sha512>"

WScript.Echo " /Show"

WScript.Echo ""

WScript.Echo "/XAdESLevel: requested XAdES level for signature generation"

WScript.Echo " 0 (No XAdES)"

WScript.Echo " 1 (XAdES-BES/EPES)"

WScript.Echo " 2 (XAdES-T)"

WScript.Echo " 3 (XAdES-C)"

WScript.Echo " 4 (XAdES-X)"

WScript.Echo " 5 (XAdES-X-L)"

WScript.Echo ""

WScript.Echo "/MinXAdESLevel: minimum XAdES level for digital signature generation (same values as XAdESLevel)"

WScript.Echo ""

WScript.Echo "/VerIfyVersion: signature verification level"

WScript.Echo " 0 (No rules)"

WScript.Echo " 1 (Office 2007 rules)"

WScript.Echo " 2 (Office 2010 rules)"

WScript.Echo ""

WScript.Echo "/TSALocationocation: URL to the timestamp server"

WScript.Echo ""

WScript.Echo "/TSATimeout: Timeout between 0 and 500 (included)"

WScript.Echo ""

WScript.Echo "/RequireOCSP: require OCSP at signature generation time"

WScript.Echo ""

WScript.Echo "/O12CompatibleXAdES: do not include XAdES reference object in the manIfest"

WScript.Echo ""

WScript.Echo "/IgnoreExpiredCert: do not allow expired certificates when validating signatures"

WScript.Echo ""

WScript.Echo "/XAdESValidationLevel: check the XAdES portions of a digital signature"

WScript.Echo ""

WScript.Echo "/SignatureHashAlg: digital signature hashing algorithm"

WScript.Echo " sha1"

WScript.Echo " sha256"

WScript.Echo " sha384"

WScript.Echo " sha512"

WScript.Echo ""

WScript.Echo "/TimestampHashAlg: timestamp server timeout (same values as SignatureHashAlg)"

WScript.Echo ""

WScript.Echo "/show: Show values"

End Sub

Sub RetrieveValues()

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "RequireOCSP", prevRequiredOCSP

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "XAdESLevel", prevXAdESLevel

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "MinXAdESLevel", prevXAdESMinLevel

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "O12CompatibleXAdES", prevO12CompatibleXAdES

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "TSATimeout", prevTSATimeout

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "VerIfyVersion", prevVerIfyVersion

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "IgnoreExpiredCert", prevIgnoreExpiredCert

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "XAdESValidationLevel", prevXAdESValidationLevel

oReg.GetStringValue HKEY\_CURRENT\_USER, regKey, "TSALocation", prevTSALocation

oReg.GetStringValue HKEY\_CURRENT\_USER, regKey, "TimestampHashAlg", prevTimestampHashAlg

oReg.GetStringValue HKEY\_CURRENT\_USER, regKey, "SignatureHashAlg", prevSignatureHashAlg

End Sub

Sub SetValues()

Dim dwValue 'As Integer

Dim strValue 'As String

'DWORD values

If WScript.Arguments.Named.Exists("XAdESLevel") Then

dwValue = WScript.Arguments.Named("XAdESLevel")

If dwValue < 0 or dwValue > 5 Then

WScript.Echo "[XAdESLevel] an incorrect value is specified: the value must be in the following range: [0-5]"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"XAdESLevel",dwValue

End If

If WScript.Arguments.Named.Exists("MinXAdESLevel") Then

dwValue = WScript.Arguments.Named("MinXAdESLevel")

If dwValue < 0 or dwValue > 5 Then

WScript.Echo "[MinXAdESLevel] an incorrect value is specified: the value must be in the following range: [0-5]"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"MinXAdESLevel",dwValue

End If

If WScript.Arguments.Named.Exists("TSATimeout") Then

dwValue = WScript.Arguments.Named("TSATimeout")

If dwValue < 0 or dwValue > 500 Then

WScript.Echo "[TSATimeout] an incorrect value is specified: the value must be in the following range: [0-500]"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"TSATimeout",dwValue

End If

If WScript.Arguments.Named.Exists("RequireOCSP") Then

dwValue = WScript.Arguments.Named("RequireOCSP")

If dwValue < 0 or dwValue > 1 Then

WScript.Echo "[RequireOCSP] an incorrect value is specified: the value must be 0 or 1"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"RequireOCSP",dwValue

End If

If WScript.Arguments.Named.Exists("O12CompatibleXAdES") Then

dwValue = WScript.Arguments.Named("O12CompatibleXAdES")

If dwValue < 0 or dwValue > 1 Then

WScript.Echo "[O12CompatibleXAdES] an incorrect value is specified: the value must be 0 or 1"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"O12CompatibleXAdES",dwValue

End If

If WScript.Arguments.Named.Exists("VerIfyVersion") Then

dwValue = WScript.Arguments.Named("VerIfyVersion")

If dwValue < 0 or dwValue > 2 Then

WScript.Echo "[VerIfyVersion] an incorrect value is specified: the value must be in the following range: [0-500]"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"VerifyVersion",dwValue

End If

If WScript.Arguments.Named.Exists("IgnoreExpiredCert") Then

dwValue = WScript.Arguments.Named("IgnoreExpiredCert")

If dwValue < 0 or dwValue > 1 Then

WScript.Echo "[IgnoreExpiredCert] an incorrect value is specified: the value must be 0 or 1"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"IgnoreExpiredCert",dwValue

End If

If WScript.Arguments.Named.Exists("XAdESValidationLevel") Then

dwValue = WScript.Arguments.Named("XAdESValidationLevel")

If dwValue < 0 or dwValue > 1 Then

WScript.Echo "[XAdESValidationLevel] an incorrect value is specified: the value must be 0 or 1"

WScript.Quit

End If

oReg.SetDWORDValue HKEY\_CURRENT\_USER,regKey,"XAdESValidationLevel",dwValue

End If

'Strings values

If WScript.Arguments.Named.Exists("TSALocation") Then

strValue = WScript.Arguments.Named("TSALocation")

oReg.SetStringValue HKEY\_CURRENT\_USER,regKey,"TSALocation",strValue

End If

If WScript.Arguments.Named.Exists("SignatureHashAlg") Then

strValue = WScript.Arguments.Named("SignatureHashAlg")

oReg.SetStringValue HKEY\_CURRENT\_USER,regKey,"SignatureHashAlg",strValue

End If

If WScript.Arguments.Named.Exists("TimestampHashAlg") Then

strValue = WScript.Arguments.Named("TimestampHashAlg")

oReg.SetStringValue HKEY\_CURRENT\_USER,regKey,"TimestampHashAlg",strValue

End If

End Sub

Sub PrintCurrentValues()

WScript.Echo "Current settings:"

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "RequireOCSP", RequiredOCSP

If IsNull(RequiredOCSP) Then RequiredOCSP = ValueNoSet

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "XAdESLevel", XAdESLevel

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "MinXAdESLevel", XAdESMinLevel

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "O12CompatibleXAdES", O12CompatibleXAdES

If IsNull(O12CompatibleXAdES) Then O12CompatibleXAdES = ValueNoSet

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "TSATimeout", TSATimeout

If IsNull(TSATimeout) Then TSATimeout = ValueNoSet

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "VerIfyVersion", VerIfyVersion

If IsNull(VerIfyVersion) Then VerIfyVersion = ValueNoSet

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "IgnoreExpiredCert", IgnoreExpiredCert

If IsNull(IgnoreExpiredCert) Then IgnoreExpiredCert = ValueNoSet

oReg.GetDWORDValue HKEY\_CURRENT\_USER, regKey, "XAdESValidationLevel", XAdESValidationLevel

If IsNull(XAdESValidationLevel) Then XAdESValidationLevel = ValueNoSet

oReg.GetStringValue HKEY\_CURRENT\_USER, regKey, "TSALocation", TSALocation

If IsNull(TSALocation) Then TSALocation = ValueNoSet

oReg.GetStringValue HKEY\_CURRENT\_USER, regKey, "SignatureHashAlg", SignatureHashAlg

If IsNull(SignatureHashAlg) Then SignatureHashAlg = ValueNoSet

oReg.GetStringValue HKEY\_CURRENT\_USER, regKey, "TimestampHashAlg", TimestampHashAlg

If IsNull(TimestampHashAlg) Then TimestampHashAlg = ValueNoSet

WScript.Echo "RequireOCSP : " & RequiredOCSP

WScript.Echo "XAdESLevel : " & GetLevelNameById(XAdESLevel)

WScript.Echo "MinXAdESLevel : " & GetLevelNameById(XAdESMinLevel)

WScript.Echo "O12CompatibleXAdES : " & O12CompatibleXAdES

WScript.Echo "TSALocation : " & TSALocation

WScript.Echo "TSATimeout : " & TSATimeout

WScript.Echo "TimestampHashAlg : " & TimestampHashAlg

WScript.Echo "VerIfyVersion : " & VerIfyVersion

WScript.Echo "XAdESValidationLevel: " & XAdESValidationLevel

WScript.Echo "IgnoreExpiredCert : " & IgnoreExpiredCert

WScript.Echo "SignatureHashAlg : " & SignatureHashAlg

WScript.Echo ""

End Sub

Sub PrintPreviousValues()

WScript.Echo "Previous settings:"

If IsNull(prevRequiredOCSP) Then prevRequiredOCSP = ValueNoSet

If IsNull(prevO12CompatibleXAdES) Then prevO12CompatibleXAdES = ValueNoSet

If IsNull(prevTSATimeout) Then prevTSATimeout = ValueNoSet

If IsNull(prevVerIfyVersion) Then prevVerIfyVersion = ValueNoSet

If IsNull(prevIgnoreExpiredCert) Then prevIgnoreExpiredCert = ValueNoSet

If IsNull(prevXAdESValidationLevel) Then prevXAdESValidationLevel = ValueNoSet

If IsNull(prevTSALocation) Then prevTSALocation = ValueNoSet

If IsNull(prevSignatureHashAlg) Then prevSignatureHashAlg = ValueNoSet

If IsNull(prevTimestampHashAlg) Then prevTimestampHashAlg = ValueNoSet

WScript.Echo "RequireOCSP : " & prevRequiredOCSP

WScript.Echo "XAdESLevel : " & GetLevelNameById(prevXAdESLevel)

WScript.Echo "MinXAdESLevel : " & GetLevelNameById(prevXAdESMinLevel)

WScript.Echo "O12CompatibleXAdES : " & prevO12CompatibleXAdES

WScript.Echo "TSALocation : " & prevTSALocation

WScript.Echo "TSATimeout : " & prevTSATimeout

WScript.Echo "TimestampHashAlg : " & prevTimestampHashAlg

WScript.Echo "VerIfyVersion : " & prevVerIfyVersion

WScript.Echo "XAdESValidationLevel: " & prevXAdESValidationLevel

WScript.Echo "IgnoreExpiredCert : " & prevIgnoreExpiredCert

WScript.Echo "SignatureHashAlg : " & prevSignatureHashAlg

WScript.Echo ""

End Sub

# Extrait du modèle de stratégie office14.adm relatif aux signatures électroniques (avancées)

Le fichier XAdES.adm suivant représente un extrait du fichier de modèle de stratégie de groupe office14.adm. Ce script est disponible dans le fichier archive Ressources Signature électronique avancée avec Microsoft Office 2010.zip proposé en complément du présent guide. Il est situé dans le sous-dossier Admin de cette archive.

Il précise de façon succincte les paramètres de stratégies de groupes relatifs aux signatures électroniques (avancées).

CLASS USER

CATEGORY !!L\_MicrosoftOfficeSystemAdvancedSignature

POLICY !!L\_RequireOCSPAtSignatureGenerationTime

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_RequireOCSPAtSignatureGenerationTimeExplain

VALUENAME "RequireOCSP"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END POLICY

POLICY !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGeneration

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationExplain

PART!!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationDropID DROPDOWNLIST

VALUENAME "MinXAdESLevel"

ITEMLIST

NAME !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr1 VALUE NUMERIC 0 DEFAULT

NAME !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr2 VALUE NUMERIC 1

NAME !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr3 VALUE NUMERIC 2

NAME !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr4 VALUE NUMERIC 3

NAME !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr5 VALUE NUMERIC 4

NAME !!L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr6 VALUE NUMERIC 5

END ITEMLIST

NOSORT

END PART

END POLICY

POLICY !!L\_CheckTheXAdESPortionsOfADigitalSignature

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_CheckTheXAdESPortionsOfADigitalSignatureExplain

VALUENAME "XAdESValidationLevel"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END POLICY

POLICY !!L\_DoNotAllowExpiredCertificatesWhenValidatingSignatures

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_DoNotAllowExpiredCertificatesWhenValidatingSignaturesExplain

VALUENAME "IgnoreExpiredCert"

VALUEON NUMERIC 0

VALUEOFF NUMERIC 1

END POLICY

POLICY !!L\_DoNotIncludeXAdESReferenceObjectInTheManifest

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_DoNotIncludeXAdESReferenceObjectInTheManifestExplain

VALUENAME "O12CompatibleXAdES"

VALUEON NUMERIC 0

VALUEOFF NUMERIC 1

END POLICY

POLICY !!L\_SelectDigitalSignatureHashingAlgorithm

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_SelectDigitalSignatureHashingAlgorithmExplain

PART !!L\_SelectDigitalSignatureHashingAlgorithmDropID DROPDOWNLIST

VALUENAME "SignatureHashAlg"

ITEMLIST

NAME !!L\_SelectDigitalSignatureHashingAlgorithmStr1 VALUE "sha1" DEFAULT

NAME !!L\_SelectDigitalSignatureHashingAlgorithmStr2 VALUE "sha256"

NAME !!L\_SelectDigitalSignatureHashingAlgorithmStr3 VALUE "sha384"

NAME !!L\_SelectDigitalSignatureHashingAlgorithmStr4 VALUE "sha512"

END ITEMLIST

NOSORT

END PART

END POLICY

POLICY !!L\_ConfigureTimeStampingHashingAlgorithm

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_ConfigureTimeStampingHashingAlgorithmExplain

PART !!L\_ConfigureTimeStampingHashingAlgorithmDropID DROPDOWNLIST

VALUENAME "TimestampHashAlg"

ITEMLIST

NAME !!L\_ConfigureTimeStampingHashingAlgorithmStr1 VALUE "sha1" DEFAULT

NAME !!L\_ConfigureTimeStampingHashingAlgorithmStr2 VALUE "sha256"

NAME !!L\_ConfigureTimeStampingHashingAlgorithmStr3 VALUE "sha384"

NAME !!L\_ConfigureTimeStampingHashingAlgorithmStr4 VALUE "sha512"

END ITEMLIST

NOSORT

END PART

END POLICY

POLICY !!L\_SpecifyTimestampServerName

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_SpecifyTimestampServerNameExplain

PART !!L\_SpecifyTimestampServerNameID EDITTEXT REQUIRED

VALUENAME "TSALocation"

END PART

END POLICY

POLICY !!L\_SetTimestampServerTimeout

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_SetTimestampServerTimeoutExplain

PART !!L\_SetTimestampServerTimeoutSpinID NUMERIC

VALUENAME "TSATimeout"

DEFAULT 5

MAX 500

MIN 0

SPIN 1

END PART

END POLICY

POLICY !!L\_SetSignatureVerificationLevel

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_SetSignatureVerificationLevelExplain

PART !!L\_SetSignatureVerificationLevelDropID DROPDOWNLIST

VALUENAME "VerifyVersion"

ITEMLIST

NAME !!L\_SetSignatureVerificationLevelStr1 VALUE NUMERIC 0

NAME !!L\_SetSignatureVerificationLevelStr2 VALUE NUMERIC 1 DEFAULT

NAME !!L\_SetSignatureVerificationLevelStr3 VALUE NUMERIC 2

END ITEMLIST

NOSORT

END PART

END POLICY

POLICY !!L\_RequestedXAdESLevelForSignatureGeneration

KEYNAME "software\policies\microsoft\office\14.0\common\signatures"

EXPLAIN !!L\_RequestedXAdESLevelForSignatureGenerationExplain

PART !!L\_RequestedXAdESLevelForSignatureGenerationDropID DROPDOWNLIST

VALUENAME "XAdESLevel"

ITEMLIST

NAME !!L\_RequestedXAdESLevelForSignatureGenerationStr1 VALUE NUMERIC 0

NAME !!L\_RequestedXAdESLevelForSignatureGenerationStr2 VALUE NUMERIC 1 DEFAULT

NAME !!L\_RequestedXAdESLevelForSignatureGenerationStr3 VALUE NUMERIC 2

NAME !!L\_RequestedXAdESLevelForSignatureGenerationStr4 VALUE NUMERIC 3

NAME !!L\_RequestedXAdESLevelForSignatureGenerationStr5 VALUE NUMERIC 4

NAME !!L\_RequestedXAdESLevelForSignatureGenerationStr6 VALUE NUMERIC 5

END ITEMLIST

NOSORT

END PART

END POLICY

END CATEGORY

[Strings]

L\_MicrosoftOfficeSystemAdvancedSignature="Signature avancée dans Microsoft Office 2010"

L\_RequireOCSPAtSignatureGenerationTime="Exiger le protocole OCSP au moment de la génération des signatures"

L\_RequireOCSPAtSignatureGenerationTimeExplain="Ce paramètre de stratégie vous permet de déterminer si Office 2010 requiert des données de révocation OCSP (Online Certificate Status Protocol) pour tous les certificats numériques dans une chaîne lors de la génération des signatures numériques.\n \n Si vous activez ce paramètre de stratégie, Office 2010 requiert des données de révocation OCSP pour tous les certificats dans une chaîne lors de la génération des signatures numériques.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, Office 2010 ne définit pas de restrictions sur le type de données de révocation devant être utilisé."

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGeneration="Spécifier le niveau XAdES minimal pour la génération des signatures numériques"

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationExplain="Ce paramètre de stratégie vous permet de spécifier un niveau XAdES minimal que les applications Office 2010 doivent atteindre pour créer une signature numérique XAdES. Si elles ne parviennent pas à atteindre ce niveau minimal, les applications Office ne peuvent pas créer la signature. \n \n Si vous activez ce paramètre de stratégie, vous pouvez définir les niveaux XAdES minimaux suivants que les applications Office doivent atteindre avant de créer la signature numérique : \n \n - Aucun niveau minimal\n - XAdES-BES : doit atteindre au moins le niveau XAdES-BES ou échec\n - XAdES-T : doit atteindre au moins le niveau XAdES-T (horodatage) ou échec. \n - XAdES-C : doit atteindre au moins le niveau XAdES-C (références de certificat et de révocation) ou échec \n - XAdES-X : doit atteindre au moins le niveau XAdES-X (horodatage -C) ou échec \n - XAdES-X-L : doit atteindre au moins le niveau XAdES-X-L (stockage du certificat et valeurs de révocation) ou échec \n \n Si vous désactivez ce paramètre de stratégie, Office 2010 ne requiert pas de niveau XAdES minimal et crée la signature XAdES la plus avancée possible, jusqu’au niveau spécifié par le paramètre de stratégie."

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationDropID=" "

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr1="Aucun niveau minimal"

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr2="XAdES-BES"

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr3="XAdES-T"

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr4="XAdES-C"

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr5="XAdES-X"

L\_SpecifyMinimumXAdESLevelForDigitalSignatureGenerationStr6="XAdES-X-L"

L\_CheckTheXAdESPortionsOfADigitalSignature="Vérifier les parties XAdES d’une signature numérique"

L\_CheckTheXAdESPortionsOfADigitalSignatureExplain="Ce paramètre de stratégie vous permet de spécifier si Office 2010 doit vérifier ou non les parties XAdES d’une signature numérique, le cas échéant, lors de la validation d’une signature numérique d’un document. \n \n Si vous activez ce paramètre de stratégie, Office 2010 vérifie les parties XAdES d’une signature numérique lors de sa validation.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, Office 2010 valide uniquement les parties XML-DSig et XAdES-BES d’une signature numérique."

L\_DoNotAllowExpiredCertificatesWhenValidatingSignatures="Ne pas autoriser les certificats arrivés à expiration lors de la validation des signatures"

L\_DoNotAllowExpiredCertificatesWhenValidatingSignaturesExplain="Ce paramètre de stratégie vous permet de déterminer si les applications Office 2010 doivent accepter les certificats numériques arrivés à expiration lors de la vérification des signatures numériques.\n \n Si vous activez ce paramètre de stratégie, un certificat arrivé à expiration ne peut pas être utilisé pour vérifier une signature numérique.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les certificats numériques arrivés à expiration sont traités comme des certificats numériques valides."

L\_DoNotIncludeXAdESReferenceObjectInTheManifest="Ne pas inclure d’objet de référence XAdES dans le manifeste"

L\_DoNotIncludeXAdESReferenceObjectInTheManifestExplain="Ce paramètre de stratégie vous permet de déterminer si un objet de référence XAdES doit apparaître dans le manifeste.\n \n Si vous activez ce paramètre de stratégie, la référence XAdES n’apparaît pas dans le manifeste.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la référence XAdES n’apparaît pas dans le manifeste."

L\_SelectDigitalSignatureHashingAlgorithm="Sélectionner l’algorithme de hachage de signature numérique"

L\_SelectDigitalSignatureHashingAlgorithmExplain="Ce paramètre de stratégie vous permet de configurer l’algorithme de hachage utilisé par les applications Office 2010 pour valider les signatures numériques.\n \n Si vous activez ce paramètre de stratégie, vous pouvez spécifier l’une des fonctions SHA standard suivantes :\n - SHA1\n - SHA256\n - SHA384\n - SHA512\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la valeur par défaut SHA1 est utilisée."

L\_SelectDigitalSignatureHashingAlgorithmDropID=" "

L\_SelectDigitalSignatureHashingAlgorithmStr1="SHA1"

L\_SelectDigitalSignatureHashingAlgorithmStr2="SHA256"

L\_SelectDigitalSignatureHashingAlgorithmStr3="SHA384"

L\_SelectDigitalSignatureHashingAlgorithmStr4="SHA512"

L\_SpecifyTimestampServerName="Spécifier le nom du serveur d’horodatage"

L\_SpecifyTimestampServerNameExplain="Ce paramètre de stratégie vous permet de définir l’URL HTTP pour le serveur d’horodatage utilisé par les applications Office 2010 dans le processus de validation des messages ou documents.\n \n Si vous activez ce paramètre de stratégie, vous devez fournir une adresse URL HTTP valide pour le serveur d’horodatage.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, un serveur d’horodatage n’est pas utilisé."

L\_SpecifyTimestampServerNameID="http://"

L\_SetTimestampServerTimeout=Définir le délai d’expiration du serveur d’horodatage"

L\_SetTimestampServerTimeoutExplain="Ce paramètre de stratégie vous permet de configurer le nombre de secondes durant lesquelles les applications Office 2010 attendent une réponse du serveur d’horodatage avant l’expiration du délai. Si le délai arrive à expiration, l’application Office 2010 n'ouvre pas le message ou le document.\n \n Si vous activez ce paramètre de stratégie, le nombre de secondes spécifié correspond à la durée pendant laquelle Office 2010 attend le retour d’un résultat du serveur d’horodatage.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la valeur par défaut de 5 secondes est utilisée."

L\_SetTimestampServerTimeoutSpinID="En secondes"

L\_ConfigureTimeStampingHashingAlgorithm="Configurer l’algorithme de hachage d’horodatage"

L\_ConfigureTimeStampingHashingAlgorithmExplain="Ce paramètre de stratégie vous permet de configurer l’algorithme de hachage d’horodatage utilisé par les applications Office 2010 pour valider un message ou un document.\n \n Si vous activez ce paramètre de stratégie, vous pouvez spécifier une des fonctions d’algorithme de hachage standard suivantes :\n - SHA1\n - SHA256\n - SHA384\n - SHA512\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, SHA1 est utilisé."

L\_SetTimestampServerTimeoutSpinID=" "

L\_L\_ConfigureTimeStampingHashingAlgorithmStr1="SHA1"

L\_L\_ConfigureTimeStampingHashingAlgorithmStr2="SHA256"

L\_L\_ConfigureTimeStampingHashingAlgorithmStr3="SHA384"

L\_L\_ConfigureTimeStampingHashingAlgorithmStr4="SHA512"

L\_SetSignatureVerificationLevel="Définir le niveau de vérification de signature"

L\_SetSignatureVerificationLevelExplain="Ce paramètre de stratégie vous permet de définir le niveau de vérification utilisé par les applications Office 2010 lors de la validation d’une signature numérique.\n \n Si vous activez ce paramètre de stratégie, vous pouvez définir le niveau de vérification sur l’une des options suivantes :\n \n - Aucune règle : les règles de signature numérique Office 2010 sont désactivées.\n - Règles Office 2007 : Office 2010 utilise les règles de signature numérique Office 2007.\n - Règles Office 2010 : Office 2010 utilise les règles de signature numérique Office 2010.\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, Office 2010 utilise les règles de signature numérique Office 2007."

L\_SetSignatureVerificationLevelDropID=" "

L\_SetSignatureVerificationLevelStr1="Aucune règle"

L\_SetSignatureVerificationLevelStr2="Règles Office 2007"

L\_SetSignatureVerificationLevelStr3="Règles Office 2010"

L\_RequestedXAdESLevelForSignatureGeneration="Niveau XAdES demandé pour la génération des signatures"

L\_RequestedXAdESLevelForSignatureGenerationExplain="Ce paramètre de stratégie vous permet de spécifier un niveau XAdES demandé ou désiré lors de la création d’une signature numérique. \n \n Si vous activez ce paramètre de stratégie, vous pouvez spécifier le niveau XAdES lors de la création d’une signature numérique. Si le niveau XAdES désiré n’est pas atteint, le dernier niveau XAdES le plus élevé atteint est utilisé s’il est plus élevé que le niveau XAdES minimal (XAdeES-BES).\n \n - Aucun niveau XAdES : XML-DSig - Aucun niveau XAdES\n - XAdES-BES : niveau XAdES minimal (valeur par défaut)\n - XAdES-T : retour au niveau XAdES-BES si le niveau XAdES minimal < XAdes-T\n - XAdES-C : retour au niveau XAdES-T si le niveau XAdES minimal < XAdes-C\n - XAdES-X : retour au niveau XAdES-C si le niveau XAdES minimal < XAdes-X\n - XAdES-X-L : retour au niveau XAdES-X si le niveau XAdES minimal < XAdes-X-L\n \n Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le niveau XAdES-BES est utilisé."

L\_RequestedXAdESLevelForSignatureGenerationDropID=" "

L\_RequestedXAdESLevelForSignatureGenerationStr1="Aucun niveau XAdES"

L\_RequestedXAdESLevelForSignatureGenerationStr2="XAdES-BES"

L\_RequestedXAdESLevelForSignatureGenerationStr3="XAdES-T"

L\_RequestedXAdESLevelForSignatureGenerationStr4="XAdES-C"

L\_RequestedXAdESLevelForSignatureGenerationStr5="XAdES-X"

L\_RequestedXAdESLevelForSignatureGenerationStr6="XAdES-X-L"

1. Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200&dateTexte=20100510 [↑](#footnote-ref-1)
2. Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=20100511 [↑](#footnote-ref-2)
3. Site KEYNECTIS : www.keynectis.com [↑](#footnote-ref-3)
4. Site officiel du produit Microsoft Office 2010 : http://officebeta.microsoft.com [↑](#footnote-ref-4)
5. Mise en route de Word 2010 : http://officebeta.microsoft.com/fr-fr/products/word/mise-en-route-de-word-2010-HA010370239.aspx [↑](#footnote-ref-5)
6. Aide et procédures Word 2010 : http://officebeta.microsoft.com/fr-fr/word-help/ [↑](#footnote-ref-6)
7. Blog du groupe produit Microsoft Word 2010 : http://blogs.msdn.com/microsoft\_office\_word/ [↑](#footnote-ref-7)
8. Livre blanc 2007 Office System Document: Digital Signing of Microsoft 2007 Office System Documents : http://www.microsoft.com/downloads/details.aspx?FamilyId=79d06e72-4b45-4669-9eac-0eca5821e8ff&displaylang=en [↑](#footnote-ref-8)
9. Article 1316-1 du Code civil : http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=BD34C835AAE5B20B48E029125AC91D25.tpdjo02v\_2?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006437813&dateTexte=20100510&categorieLien=id#LEGIARTI000006437813 [↑](#footnote-ref-9)
10. Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200&dateTexte=20100510 [↑](#footnote-ref-10)
11. European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML [↑](#footnote-ref-11)
12. Site KEYNECTIS : www.keynectis.com [↑](#footnote-ref-12)
13. Une présentation de ce nouveau format est disponible sur le site Microsoft France à l’adresse Internet http://www.microsoft.com/france/office/2007/LivreBlanc.mspx. [↑](#footnote-ref-13)
14. Billet Open XML: One Year In : http://blogs.technet.com/office2010/archive/2009/11/19/open-xml-one-year-in.aspx [↑](#footnote-ref-14)
15. Standard ECMA-376 : http://www.ecma-international.org/publications/standards/Ecma-376.htm [↑](#footnote-ref-15)
16. Notes d’implémenteur ECMA-376 1ère Edition : http://www.documentinteropinitiative.org/ECMA-376/reference.aspx [↑](#footnote-ref-16)
17. Informations additionnelles Office 2007 : http://www.documentinteropinitiative.org/additionalinfo/2007TOC.aspx [↑](#footnote-ref-17)
18. Notes d’implémenteur ISO 29500:2008 : http://www.documentinteropinitiative.org/ISO-IEC29500-2008/reference.aspx [↑](#footnote-ref-18)
19. Informations additionnelles Office 2010 : http://www.documentinteropinitiative.org/additionalinfo/2010TOC.aspx [↑](#footnote-ref-19)
20. Site Document Interop Initiative : http://www.documentinteropinitiative.org [↑](#footnote-ref-20)
21. Téléchargement Pack de compatibilité pour Microsoft Office 2000, Office XP ou Office 2003 : http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=941b3470-3ae9-4aee-8f43-c6bb74cd1466 [↑](#footnote-ref-21)
22. Configuration système requise : http://technet.microsoft.com/fr-fr/library/ee624351(office.14).aspx [↑](#footnote-ref-22)
23. Centre de ressources Microsoft TechNet pour Microsoft Office 2010 : http://technet.microsoft.com/fr-fr/office/ee263913.aspx [↑](#footnote-ref-23)
24. K.Stamp : http://www.keynectis.com/fr/produits-et-services/pki/kstamp-horodatage-electronique.html [↑](#footnote-ref-24)
25. RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) : http://tools.ietf.org/html/rfc3161 [↑](#footnote-ref-25)
26. K.Valid : http://www.keynectis.com/fr/produits-et-services/pki/kvalid-validation-certificat-ocsp.html [↑](#footnote-ref-26)
27. RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP : http://tools.ietf.org/html/rfc2560 [↑](#footnote-ref-27)
28. Article MSDN Asymmetric Keys : http://msdn.microsoft.com/en-us/library/aa387460(VS.85).aspx [↑](#footnote-ref-28)
29. Site Active Directory Certificate Services : http://go.microsoft.com/fwlink/?LinkId=119113 [↑](#footnote-ref-29)
30. Trust.Wider : http://www.keynectis.com/fr/produits-et-services/pki/trustwider-autorite-de-certification-racine.html [↑](#footnote-ref-30)
31. Article MICROSOFT ROOT CERTIFICATE PROGRAM : http://technet.microsoft.com/fr-fr/library/cc751157(en-us).aspx [↑](#footnote-ref-31)
32. Article WINDOWS ROOT CERTIFICATE PROGRAM MEMBERS : http://support.microsoft.com/kb/931125/en-US [↑](#footnote-ref-32)
33. Article  Ajouter, supprimer ou afficher un éditeur approuvé : http://office2010.microsoft.com/fr-fr/word-help/ajouter-supprimer-ou-afficher-un-editeur-approuve-HA010354309.aspx?CTT=5&origin=HA010354321 [↑](#footnote-ref-33)
34. Office Marketplace : http://go.microsoft.com/fwlink/?LinkId=119114 [↑](#footnote-ref-34)
35. European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML [↑](#footnote-ref-35)
36. RFC3275 (Extensible Markup Language) XML-Signature Syntax and Processing : http://tools.ietf.org/html/rfc3275 [↑](#footnote-ref-36)
37. XML Advanced Electronic Signatures (XAdES) W3C Note 20 February 2003 : http://www.w3.org/TR/XAdES/ [↑](#footnote-ref-37)
38. RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) : http://tools.ietf.org/html/rfc3161 [↑](#footnote-ref-38)
39. ETSI TS 101 456 V1.1.1 (2000-12) Policy requirements for certification authorities issuing qualified certificates : http://docbox.etsi.org/EC\_Files/EC\_Files/ts\_101456v010101p.pdf [↑](#footnote-ref-39)
40. Spécifications Formats binaires de Microsoft Office 97-2003 : http://www.microsoft.com/interop/docs/OfficeBinaryFormats.mspx [↑](#footnote-ref-40)
41. Téléchargement Pack de compatibilité pour Microsoft Office 2000, Office XP ou Office 2003 : http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=941b3470-3ae9-4aee-8f43-c6bb74cd1466 [↑](#footnote-ref-41)
42. Article  Ajouter, supprimer ou afficher un éditeur approuvé : http://office2010.microsoft.com/fr-fr/word-help/ajouter-supprimer-ou-afficher-un-editeur-approuve-HA010354309.aspx?CTT=5&origin=HA010354321 [↑](#footnote-ref-42)
43. Billet DIGITAL SIGNATURES IN OFFICE 2010 : http://blogs.technet.com/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx [↑](#footnote-ref-43)
44. Contrat de licence de logiciel libre CeCILL-B : http://www.cecill.info/licences/Licence\_CeCILL-B\_V1-fr.txt [↑](#footnote-ref-44)
45. ScriptCenter Microsoft TechNet : http://technet.microsoft.com/fr-fr/scriptcenter/default.aspx [↑](#footnote-ref-45)
46. Téléchargement OFFICE 2010 ADMINISTRATIVE TEMPLATE FILES (ADM, ADMX, ADML) AND OFFICE CUSTOMIZATION TOOL : http://go.microsoft.com/fwlink/?LinkId=189316 [↑](#footnote-ref-46)
47. Article OFFICE 2010 ADMINISTRATIVE TEMPLATE FILES (ADM, ADMX, ADML) AND OFFICE CUSTOMIZATION TOOL : http://go.microsoft.com/fwlink/?LinkId=190598 [↑](#footnote-ref-47)
48. Article MANAGING GROUP POLICY ADMX FILES STEP-BY-STEP GUIDE : http://technet.microsoft.com/en-us/library/cc709647(WS.10).aspx [↑](#footnote-ref-48)
49. Kit de ressources Microsoft Office 2010 : http://technet.microsoft.com/fr-fr/library/cc303401(office.14).aspx [↑](#footnote-ref-49)
50. Article Plan digital signature settings for Office 2010 : http://technet.microsoft.com/fr-fr/library/cc545900(office.14).aspx [↑](#footnote-ref-50)
51. Article GROUP POLICY OVERVIEW FOR OFFICE 2010 : http://technet.microsoft.com/fr-fr/library/cc179176(office.14).aspx [↑](#footnote-ref-51)
52. Article Enforce settings by using Group Policy in Office 2010 : http://technet.microsoft.com/fr-fr/library/cc179081(office.14).aspx [↑](#footnote-ref-52)
53. Téléchargement OFFICE 2010 ADMINISTRATIVE TEMPLATE FILES (ADM, ADMX, ADML) AND OFFICE CUSTOMIZATION TOOL : http://go.microsoft.com/fwlink/?LinkId=189316 [↑](#footnote-ref-53)
54. Article OUTIL DE PERSONNALISATION OFFICE DANS OFFICE SYSTEM 2010 : http://technet.microsoft.com/fr-fr/library/cc179097(office.14).aspx [↑](#footnote-ref-54)
55. Article CONFIGURER DES PARAMETRES UTILISATEUR POUR OFFICE 2010 : http://technet.microsoft.com/fr-fr/library/cc178990(office.14).aspx [↑](#footnote-ref-55)
56. Site KEYNECTIS : http://www.keynectis.com [↑](#footnote-ref-56)
57. Site Microsoft France Sécurité : http://www.microsoft.com/france/securité [↑](#footnote-ref-57)
58. Site Microsoft France Office : http://www.microsoft.com/france/office [↑](#footnote-ref-58)
59. Centre de ressources Microsoft TechNet pour Microsoft Office 2010 : http://technet.microsoft.com/fr-fr/office/ee263913.aspx [↑](#footnote-ref-59)
60. Contrat de licence de logiciel libre CeCILL-B : http://www.cecill.info/licences/Licence\_CeCILL-B\_V1-fr.txt [↑](#footnote-ref-60)
61. Centre de développement MSDN éponyme dédié : http://msdn.microsoft.com/fr-fr/netframework/default.aspx [↑](#footnote-ref-61)
62. Package redistribuable Microsoft .NET Framework 3.5 SP1 : http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 [↑](#footnote-ref-62)
63. Mise à jour KB959209 pour .NET Framework 3.5 SP1: http://go.microsoft.com/fwlink/?LinkId=136730 [↑](#footnote-ref-63)
64. Site Microsoft Visual Studio Express Editions : http://msdn.microsoft.com/fr-fr/express/default.aspx [↑](#footnote-ref-64)