Guide du Kit de démarrage Signature avancée XAdES (XML Advanced Electronic Signatures)

# Détails du document

Version : 1.0

Publication : octobre 2010

Auteurs : Philippe Beraud (Microsoft France), Eddy Rubbens (Microsoft Belgique)

Sommaire

[Détails du document 1](#_Toc275091089)

[Avertissement 4](#_Toc275091090)

[Licence 5](#_Toc275091091)

[Objectifs du guide 6](#_Toc275091092)

[Organisation du guide 6](#_Toc275091093)

[Audience du guide 7](#_Toc275091094)

[Prérequis 7](#_Toc275091095)

[Remerciements 7](#_Toc275091096)

[Généralisation de la dématérialisation 8](#_Toc275091097)

[Organiser la dématérialisation 9](#_Toc275091098)

[Certificat électronique 9](#_Toc275091099)

[Solutions techniques associées 10](#_Toc275091100)

[Signature électronique avancée XAdES, de quoi s’agit-il ? 11](#_Toc275091101)

[Signature électronique et certificat 11](#_Toc275091102)

[Qu’est-ce qu’une signature électronique ? 11](#_Toc275091103)

[Certificat de signature et autorité de certification 11](#_Toc275091104)

[Garanties des signatures électroniques 12](#_Toc275091105)

[Signature électronique avancée 13](#_Toc275091106)

[Signature électronique qualifiée 15](#_Toc275091107)

[Signatures avancées XAdES avec le Framework .NET 17](#_Toc275091108)

[Principes de mise en œuvre avec le Kit de démarrage XAdES 17](#_Toc275091109)

[Organisation du Kit de démarrage XAdES 19](#_Toc275091110)

[Compilation des composants du Kit de démarrage XAdES 20](#_Toc275091111)

[Compilation des composants à la ligne de commande 20](#_Toc275091112)

[Compilation des composants en utilisant Visual Studio 2010 20](#_Toc275091113)

[Exécution des composants du Kit de démarrage XAdES 21](#_Toc275091114)

[Débogage des composants 22](#_Toc275091115)

[Génération de la documentation du Kit de démarrage XAdES 22](#_Toc275091116)

[Scénarios de mise en œuvre du Kit de démarrage XAdES 25](#_Toc275091117)

[Scénario 1 – Création d’une signature avancée XAdES simple 25](#_Toc275091118)

[Objectif du scénario 25](#_Toc275091119)

[Déroulé du scénario 25](#_Toc275091120)

[Scénario 2 – Horodatage et vérification d’une signature avancée XAdES 30](#_Toc275091121)

[Objectif du scénario 30](#_Toc275091122)

[Déroulé du scénario 31](#_Toc275091123)

[Scénario 3 – Préparation d’une signature avancée XAdES pour le stockage 33](#_Toc275091124)

[Objectif du scénario 33](#_Toc275091125)

[Déroulé du scénario 33](#_Toc275091126)

[Références 37](#_Toc275091127)

# Avertissement

Ce document est fourni uniquement à titre indicatif. MICROSOFT N’APPORTE AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, À CE DOCUMENT. Les informations figurant dans ce document, notamment les URL et les références aux sites Internet, peuvent être modifiées sans préavis. Les risques d’utiliser ce document ou ses résultats sont entièrement à la charge de l'utilisateur. Sauf indication contraire, les sociétés, les entreprises, les produits, les noms de domaine, les adresses électroniques, les logos, les personnes, les lieux et les événements utilisés dans ce document sont fictifs. Toute ressemblance avec des entreprises, noms d’entreprise, produits, noms de domaine, adresses électroniques, logos, personnes ou événements réels serait purement fortuite et involontaire.

# Licence

Le Kit de démarrage XAdES (XML Advanced Electronic Signatures) pour le Microsoft .NET Framework 3.5 est publié sous le contrat de licence de logiciel libre CeCILL-B tel que décrit à l’adresse Internet <http://www.cecill.info/licences/Licence_CeCILL-B_V1-fr.txt>.

# Objectifs du guide

Ce guide vise à présenter la signature électronique avancée XAdES et sa prise en charge dans l’environnement .NET au travers des composants exemple proposés dans le cadre de ce Kit de démarrage XAdES pour le Framework .NET 3.5 (ou ultérieur).

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)[[1]](#footnote-1) :

« *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)[[2]](#footnote-2) - [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)[[3]](#footnote-3)

# Organisation du guide

De façon à couvrir l’ensemble des considérations relatives à la mise en œuvre de la signature électronique avancée XAdES en environnement .NET, 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 et en particulier XAdES dans le contexte de ce guide.

Le document présente ensuite la génération d’une signature avancée pour un document XML ainsi que sa vérification ultérieure au travers de la bibliothèque XAdES et de l’application exemple proposées avec ce guide, et aborde diverses considérations associées en termes de mise en œuvre au travers de 3 scénarii principaux décrits dans les sections suivantes :

1. Section § Scénario 1 – Création d’une signature avancée XAdES simple ;
2. Section § Scénario 2 – Horodatage et vérification d’une signature avancée XAdES ;
3. Section § Scénario 3 – Préparation d’une signature avancée XAdES pour le stockage.

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

# Audience du guide

Ce document s’adresse aux architectes, aux développeurs et à tous ceux qui souhaitent créer ou vérifier des signatures avancées XAdES depuis l’environnement .NET. La bibliothèque *Microsoft.Xades.dll*, l’application de test *XadesTestClient.exe* illustrant les principaux cas d’utilisation et le code source fournis dans le Kit de démarrage XAdES sont conçus pour fonctionner avec d'autres implémentations conformes à la spécification XAdES (voir la section § Signature électronique avancée).

# Prérequis

Ce Kit de démarrage XAdES nécessite un ordinateur sous Windows XP SP2, Windows Vista, Windows 7, Windows Server 2003 (R2) SP1, Windows Server (R2) 2008 ou ultérieur. Veuillez installer (et compiler) le kit en suivant les consignes du document Installation du Kit de démarrage Signature Avancée XAdES.

Le lecteur doit connaître le langage C# et le Framework .NET afin de pouvoir facilement comprendre le code ainsi proposé.

# Remerciements

Nous tenons à remercier Jean Gautier (Microsoft France) pour la revue du code source exemple en langage C# du Kit de démarrage XAdES.

Nous tenons à remercier Alejandro Campos Magencio (Microsoft Espagne) pour son aide précieuse à la résolution de certains problèmes de mise en œuvre rencontrés. Vous pouvez retrouver Alejandro sur son [weblog Decrypt my World:Cryptography, Security, Debugging and more!](http://blogs.msdn.com/b/alejacma/)[[4]](#footnote-4).

# 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, etc.).

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)[[5]](#footnote-5) (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)[[6]](#footnote-6) 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 § 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.

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

Comme précédemment mentionné, 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.

### 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)[[7]](#footnote-7).

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)[[8]](#footnote-8).

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)[[9]](#footnote-9) et les membres courants dans l’article [Windows root certificate program members](http://support.microsoft.com/kb/931125/en-US)[[10]](#footnote-10).

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.

### 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 ont la validité d’une notarisation. On parle alors de signature électronique avancée, Cf. section suivante éponyme et objet central de ce guide.

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 :



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.

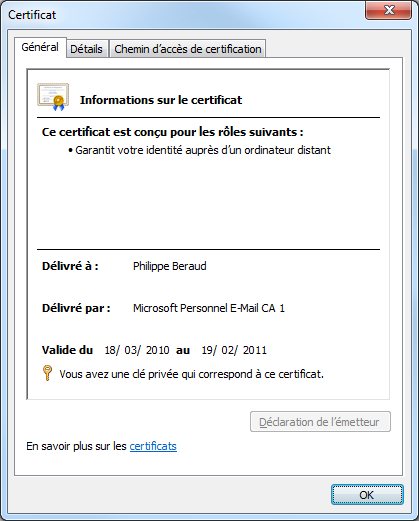


Figure . Informations sur le certificat électronique

## 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)[[11]](#footnote-11) :

« *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, le standard [RFC3275 (Extensible Markup Language) XML-Signature Syntax and Processing](http://tools.ietf.org/html/rfc3275)[[12]](#footnote-12) ou XML-DSig définit un format adapté pour les signatures électroniques.

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod Algorithm="..." />

<SignatureMethod Algorithm="..." />

<Reference URI="#data" Id="enveloped">

<DigestMethod Algorithm="..." />

<DigestValue>SyNLjOrOTANUQX7K3504GPnrPss=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>...SignatureValue>

<KeyInfo>

<X509Data>

<X509Certificate>...</X509Certificate>

</X509Data>

</KeyInfo>

<Object Id="data">...</Object>

</Signature>

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 [ETSI 101 903 XML Advanced Electronic Signatures (XAdES)](http://uri.etsi.org/01903)[[13]](#footnote-13) a été publié par le W3C en février 2003 sous forme d’une [note](http://www.w3.org/TR/XAdES/)[[14]](#footnote-14) qui étend le RFC mentionné ci-avant. Le Kit de démarrage XAdES prend en considération la version 1.1.1 du standard XAdES.

Le standard XAdES constitue un ensemble d'extensions hiérarchisées fondées sur XML-DSig et différant dans le niveau de protection offert. Le standard XAdES

Structure de la signature XAdES (sur la fondation de XML-DSig)

Figure . Extensions de la signature XAdES

La structure XML de ces extensions est la suivante :

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod />

<SignatureMethod />

<Reference URI="#**SignedPropertiesId**“/>

</SignedInfo>

<SignatureValue />

<KeyInfo />

<Object Id="XadesObjectId">

**<QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.1.1#">**

**<SignedProperties Id="SignedPropertiesId“ />**

**<UnsignedProperties />**

**</QualifyingProperties>**

</Object>

</Signature>

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.

Les nouveaux cas d’utilisation rendus ainsi possibles sont, au-delà de la non-répudiation, la contre-signature, la validité à long-terme, l’ajout d’informations additionnelles qualifiées ou non notamment au travers des propriétés de signature qualifiée telles que décrites dans le standard [ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats](http://docbox.etsi.org/EC_Files/EC_Files/ts_101733v010501p.pdf)[[15]](#footnote-15), etc.

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.

Le tableau suivant liste les niveaux disponibles dans les composants du Kit de démarrage XAdES, à savoir  la bibliothèque *Microsoft.Xades.dll* et l’application de test *XadesTestClient.exe* :

Tableau . 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 |

La possibilité avec les composants du Kit de démarrage XAdES 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 de l’application exemple, 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)[[16]](#footnote-16). La mise en œuvre précise de cette fonctionnalité est décrite dans la section § Scénario 2 – Horodatage et vérification d’une signature avancée XAdES de ce guide.

## 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 est recevable 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.

Un tel prestataire doit obtenir, dans le cadre de son activité d’opérateur de service de confiance, la certification [ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates](http://docbox.etsi.org/EC_Files/EC_Files/ts_101456v010101p.pdf)[[17]](#footnote-17) pour émettre des certificats qualifiés.

Le [didacticiel Microsoft QuEST (Qualified Electronic Signatures Tutorial)](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf)[[18]](#footnote-18) (en anglais) sur les signatures électroniques qualifiées publié en 2004 peut être consulté à titre de complément. Il couvre les aspects légaux, technique ainsi que les politiques, processus et procédures à mettre en œuvre. La [présentation technique](http://download.microsoft.com/download/a/c/3/ac39eebf-96a1-40c1-bbd4-45825ab81b21/QuEST_Technical_Blueprint(Version1.00June2004).pdf)[[19]](#footnote-19) et le [glossaire](http://download.microsoft.com/download/a/c/3/ac39eebf-96a1-40c1-bbd4-45825ab81b21/QuEST_Glossary(Version1.00June2004).pdf)[[20]](#footnote-20) sont disponibles en français.

# Signatures avancées XAdES avec le Framework .NET

Ce chapitre s’intéresse à la mise en œuvre du standard XAdES avec le Framework .NET via les composants exemple proposés par le Kit de démarrage XAdES.

En effet, ce kit propose, à titre d’illustration de mise en œuvre, un code source exemple complet en C#, qui une fois compilé, permet de produire les composants suivants :

* La bibliothèque exemple *Microsoft.Xades.dll* offrant une implémentation du standard XAdES,
* Le fichier d’aide *Microsoft.Xades.chm* précisant les différentes classes, méthodes et propriétés de la bibliothèque précédente,
* L’application de test exemple *XadesTestClient.exe* illustrant les principaux cas d’utilisation.

## Principes de mise en œuvre avec le Kit de démarrage XAdES

La prise en charge de XAdES est possible avec le Framework .NET à partir de la version 1.1 sur la base des classes de l’[espace de noms *System.Security.Cryptography.Xml*](http://msdn.microsoft.com/en-us/library/system.security.cryptography.xml(VS.71).aspx)[[21]](#footnote-21) correspondant à l’implémentation XML-DSig.

En effet, comme le standard XAdES étend le support du standard XML-DSig, le support de XAdES avec le Framework .NET suppose d’étendre l’implémentation du standard XML-DSig au sein du Framework .NET telle que définie au travers de la classe wrapper [*SignedXml*](http://msdn.microsoft.com/en-us/library/system.security.cryptography.xml.signedxml.aspx)*[[22]](#footnote-22)* de *System.Security.Cryptography.Xml*.

**Avertissement**

Il convient de noter en préalable que la classe *SignedXml* vise uniquement à adhérer à la spécification XML-DSig, Cf. extrait de la documentation MSDN de la classe :

« *The SignedXml class is the main class used for XML signing and verification (XMLDSIG) in the .NET Framework. XMLDSIG is a standards-based, interoperable way to sign and verify all or part of an XML document or other data that is addressable from a Uniform Resource Identifier (URI). The .NET Framework XMLDSIG classes implement the World Wide Web Consortium (W3C) specification for XML signing and verification located at* [*http://www.w3.org/TR/xmldsig-core/*](http://www.w3.org/TR/xmldsig-core/) *.* »

Cette classe n'a donc pas connaissance de XAdES, SOAP, SAML ou de tout autre niveau supérieur protocole XML. En conséquence, si la classe *SignedXml* est utilisée pour n'importe quel autre protocole autre que XML-DSig comme ici avec XAdES, le scénario n'est pas supporté par le support Microsoft.

Ceci suppose de créer, pour cela, une classe dérivée de la classe wrapper *SignedXml* et de redéfinir la méthode *GetIdElement*().

En effet, la mise en œuvre de XAdES suppose de pouvoir signer des éléments se trouvant dans un élément Object. Malheureusement, la classe *SignedXml* ne permet pas de référencer les éléments enfants d'un élément *Object*. Lors du calcul de la signature, une exception est alors levée.

Une redéfinition de la méthode *GetIdElement*() permet d’intégrer cette capacité. Celle-ci doit permettre de retourner un objet *XmlElement* possédant un attribut Id avec une valeur donnée. Il convient donc de parcourir les éléments Object et de tester leurs enfants si la méthode de base n'a retourné aucun élément.

public class XadesSignedXml : System.Security.Cryptography.Xml.SignedXml

{

public XadesSignedXml(XmlDocument doc)

: base(doc)

{

}

…

public override XmlElement GetIdElement(XmlDocument document, string idValue)

{

XmlElement elem = base.GetIdElement(document, idValue);

if (elem == null)

{

XmlNode node1;

foreach (DataObject data in base.Signature.ObjectList)

{

foreach (XmlNode node in data.Data)

{

node1 = node.SelectSingleNode("//SignedProperties[@Id='" + idValue + "']");

if (node1 != null)

{

return (XmlElement) node1;

}

}

}

}

return elem;

}

…

}

L’implémentation de la spécification technique XAdES peut dès lors s’établir sur cette base.

Le [programme Reflector](http://reflector.red-gate.com/download.aspx?TreatAsUpdate=1)[[23]](#footnote-23) permet d’observer les modalités associées en considérant la classe *MS.Internal.IO.Packaging.CustomSignedXml* dans l’assembly *WindowsBase.dll*. Une illustration de l’approche est également proposée dans le document [La signature électronique avec .NET](http://stormimon.developpez.com/dotnet/signature-electronique/)[[24]](#footnote-24).

Par ailleurs, pour faciliter la mise en œuvre de XAdES avec un modèle de sérialisation identique à la classe *SignedXml*, il est également souhaitable de redéfinir les méthodes suivantes :

* *GetXml*(): sérialisation du modèle objet en XML,
* LoadXml() : hydratation/dé-sérialisation du modèle objet à partir du XML.

Et d’intégrer le support de la validation du [schéma XAdES](http://uri.etsi.org/01903/v1.1.1/XAdES.xsd)[[25]](#footnote-25).

Enfin, les éléments XAdES sont relativement imbriqués comme illustré ci-après :

<Object>

<QualifyingProperties>

<SignedProperties>

<SignedSignatureProperties>

<SignatureProductionPlace>

<City>Issy les Moulineaux</City>

</SignatureProductionPlace>

</SignedSignatureProperties>

</SignedProperties>

</QualifyingProperties>

</Object>

Il est donc souhaitable d’offrir une instanciation automatique du graphe d’objets imbriqués et d’offrir sur cette base une notation en point avec une assistance IntelliSense dans Visual Studio 2010.

xadesObject.QualifyingProperties.SignedSignatureProperties.SignatureProductionPlace.City = “Issy les Moulineaux”;

Enfin, comme décrit dans le document [XML Advanced Electronic Signatures (XAdES) - Implementation and Interoperability](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.137.1977&rep=rep1&type=pdf)[[26]](#footnote-26), il est nécessaire d’ajouter le préfixe « *ds* » à l’ensemble des balises XML-DSig :

« *To distinguish between elements from the XAdES namespace and elements from the XMLDSig namespace, the namespace prefix “ds” is used for all elements that are in the XMLDSig namespace, e.g. <ds:Signature>. The XAdES namespace is treated as the default namespace, therefore there is no namespace prefix added to elements of the XAdES namespace.*

*...*

*XAdES Example*

*This appendix shows an XAdES-A signature with OCSP revocation values and <SigAndRefsTimeStamp> and signature that was produced during the XAdES-PLUGTESTSTM by IAIK’s XAdES implementation.*

*<?xml version="1.0" encoding="UTF−8"?>*

*<ds:Signature Id="IAIK−XAdES−A−5" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">*

*<ds:SignedInfo Id="SignedInfo">*

… »

Pour autant, une limitation connue de la classe *SignedXml* est que cette dernière ne peut pas générer de signatures avec un préfixe d'espace de noms pour les balises XML-DSig. Comme l’approche suggérée ici repose sur une classe dérivée de la classe *SignedXml*, autrement dit utilise la classe *SignedXml* comme classe de base, celle-ci souffre de la même limitation.

Comme la classe *SignedXml* ne nous permet pas de préciser un préfixe d'espace de noms, de sorte que nous ne pouvons pas générer la signature dont nous avons besoin avec la classe par défaut : l’ajout d’un préfixe après que la signature générée est facile, mais ceci casse de fait la signature !

L'option suivie par le Kit de démarrage XAdES pour résoudre ce problème consiste à réécrire certaines des méthodes de la classe *SignedXml* de façon à ajouter ce support de l'espace de noms comme décrit dans le [fil de discussion Signature namespace prefix](http://social.msdn.microsoft.com/Forums/en-US/xmlandnetfx/thread/e57fcba9-3b42-4a63-acb9-aedf06e29cd8)[[27]](#footnote-27).

La bibliothèque *Microsoft.Xades.dll* au travers de la classe *XadesSignedXml* propose tous ces éléments, **aux limites de supportabilité près évoquées ci-avant.**

## Organisation du Kit de démarrage XAdES

Le Kit de démarrage XAdES intègre dans le sous-répertoire *Source* du répertoire d’installation du kit une solution Visual Studio 2010 *Microsoft.Xades.sln* qui comprend deux projets principaux :

1. Le projet *Library.csproj* dans le sous-dossier *Library* et qui correspond comme son nom l’indique à la bibliothèque *Microsoft.Xades.dll*,
2. Le projet *TestClient.csproj* dans le sous-dossier *TestClient* pour l’application de test *XadesTestClient.exe*.

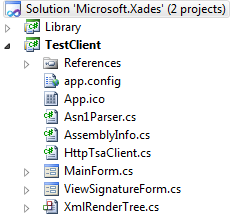


Figure . Solution Microsoft.Xades.sln

Le projet *Library* regroupe l’ensemble des classes relatives au support du standard XAdES sur la base de l’implémentation XLM-Dsig du Framework .NET (Cf. section précédente).

Le projet *TestClient* permet d’illustrer la mise en œuvre de cette bibliothèque. Le chapitre suivant § Scénarios de mise en œuvre du Kit de démarrage XAdES couvre les principaux cas d’utilisation.

## Compilation des composants du Kit de démarrage XAdES

Les composants *Microsoft.Xades.dll* et *XadesTestClient.exe* du Kit de démarrage XAdES peuvent être compilés en utilisant Visual Studio 2010 ou la commande *msbuild* à la ligne de commande. Les deux procédures sont décrites dans cette section.

note_dd Remarque :

Avant de compiler ou d’exécuter les composants du Kit de démarrage XAdES, assurez-vous que vous avez effectué une fois la procédure d’installation décrite dans le document Installation du Kit de démarrage XAdES.

### Compilation des composants à la ligne de commande

procedure_ddPour compiler les composants *Microsoft.Xades.dll* et *XadesTestClient.exe* via la ligne de commande, veuillez suivre ces étapes :

1. Ouvrez la ligne de commande du SDK et placez-vous dans le sous-répertoire *Source* du répertoire d’installation du Kit de démarrage XAdES.
2. Saisissez *msbuild* à la ligne de commande. Les composants *Microsoft.Xades.dll* et *XadesTestClient.exe* du Kit de démarrage XAdES sont compilés dans le sous-répertoire *Source\bin\[Debug|Release]*. Le sous-répertoire *Debug* ou *Release* dépend de votre choix lors de la compilation (mode Débogage ou non).

### Compilation des composants en utilisant Visual Studio 2010

procedure_ddPour compiler les composants *Microsoft.Xades.dll* et *XadesTestClient.exe* via Visual Studio 2010, veuillez suivre ces étapes :

1. Ouvrez Windows Explorer et placez-vous dans le sous-répertoire *Source* du répertoire d’installation du Kit de démarrage XAdES.
2. Double-cliquez sur l’icône du fichier *Microsoft.Xades.sln* situé dans le sous-répertoire *Source* pour ouvrir le fichier dans l’environnement Visual Studio.
3. Dans le menu **Build**, choisissez **Rebuild Solution**.

-ou-

Appuyez sur la touche F6 depuis l’environnement Visual Studio.

Tous les composants *Microsoft.Xades.dll* et *XadesTestClient.exe* du Kit de démarrage XAdES sont compilés dans le sous-répertoire *Source\bin\[Debug|Release]*. Le sous-répertoire *Debug* ou *Release* dépend de votre choix lors de la compilation (mode **Debug** ou non).

## Exécution des composants du Kit de démarrage XAdES

procedure_ddEffectuez les opérations suivantes :

1. Exécutez l’application de test *XadesTestClient.exe* à partir du sous-répertoire *Source\bin\[Debug|Release]*, sous le répertoire où vous avez installé le Kit de démarrage XAdES.

-ou-

Appuyez sur CTRL + F5 depuis l’environnement Visual Studio.

La fenêtre suivante s’ouvre. Vous pouvez consulter le chapitre § Scénarios de mise en œuvre du Kit de démarrage XAdES pour une description de l’utilisation de l’application.

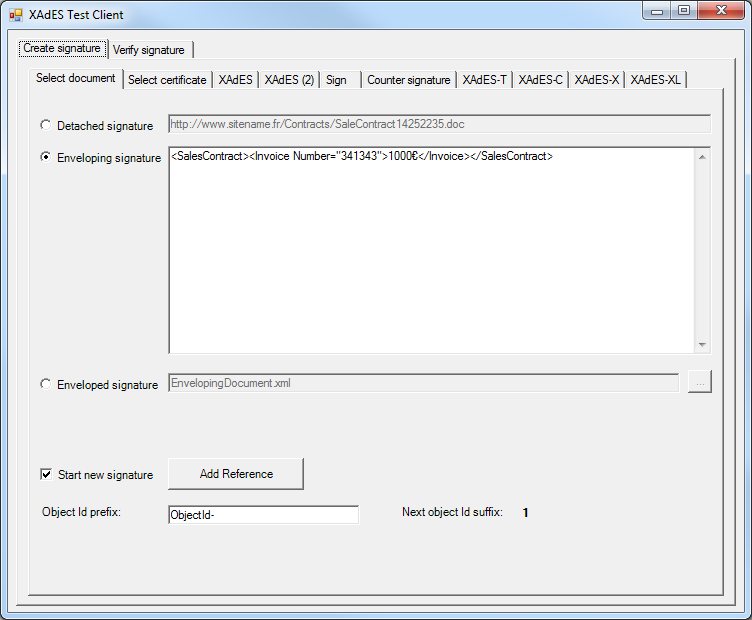


Figure . Application de test XAdES Test Client

### Débogage des composants

procedure_dd Effectuez les opérations suivantes pour le débogage d’un exemple :

1. Choisissez le mode **Debug** (par défaut) et compilez la solution Microsoft.Xades.sln (par le menu ou par le raccourci approprié).

Il est alors possible de placer des points d’arrêt dans le code de l’application de test *XadesTestClient.exe* et/ou de la bibliothèque *Microsoft.Xades.dll* et d’autoriser les points d’arrêt sur les exceptions.

1. Cliquez-droit sur le projet *Test* de l’application de test et choisissez **Debug**, puis **Start new instance**.

-ou-

Appuyez sur la touche F5 depuis l’environnement Visual Studio.

## Génération de la documentation du Kit de démarrage XAdES

Une fois ces éléments en place, le projet *Microsoft.Xades.shfb* situé dans le dossier *Help*, situé dans le sous-répertoire *Source* du répertoire d’extraction du Kit de démarrage XAdES, permet de reconstruire avec l’environnement Sandcastle Help File Builder (SHFB) un fichier *Microsoft.Xades.chm* contenant la documentation du code.

Il convient d’activer préalablement la génération d’un fichier de documentation XML pour la bibliothèque *Microsoft.Xades.dll*.

procedure_ddPour cela, procédez comme suit :

1. Sélectionnez l’onglet **Build** depuis les propriétés du projet, cochez la case à cocher **XML documentation file** et précisez le nom du fichier de documentation dans le champ adjacent.

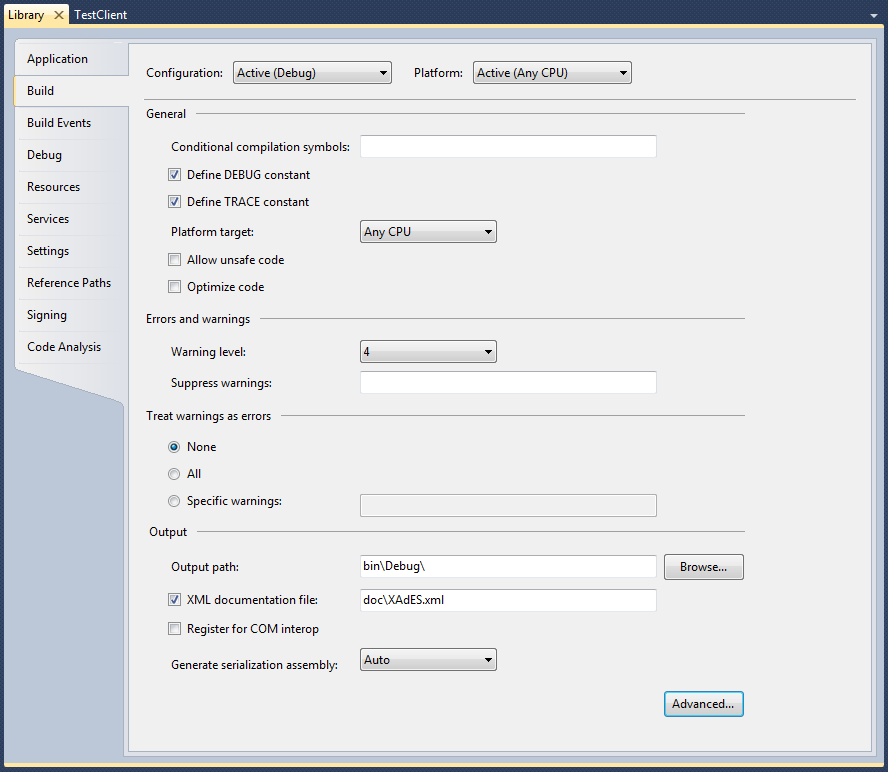


Figure . Génération du fichier de documentation au format XML

Dans la pratique, l’environnement Sandcastle Help File Builder (SHFB) constitue une interface utilisateur permettant de gérer facilement, et surtout, rapidement la « plomberie » interne de *Sandcastle* (relativement lourde à mettre en œuvre).

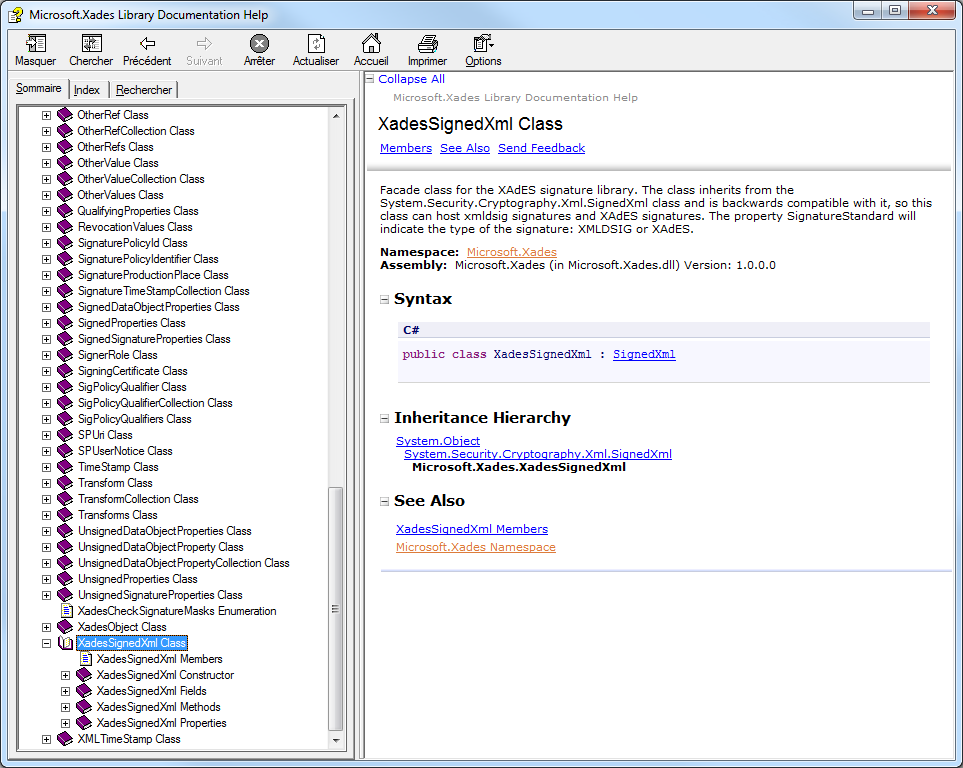


Figure . Documentation de la bibliothèque Microsoft.Xades.dll

**Note** :



Pour de plus amples informations sur le projet SandCastle et SHFB, et au-delà de la documentation proposée sur le site afférant de la forge Codeplex, nous vous conseillons de consulter, dans un premier temps (ou de façon connexe), le [tutoriel Bien commenter et documenter son code en C#](ftp://ftp-developpez.com/vincentlaine/dotnet/comdoc.pdf)[[28]](#footnote-28) ainsi que le [blog Sandcastle - Documentation compiler](http://blogs.msdn.com/sandcastle/)[[29]](#footnote-29) dédié à ce projet.

# Scénarios de mise en œuvre du Kit de démarrage XAdES

Les composants du Kit de démarrage XAdES, en l’occurrence la bibliothèque *Microsoft.Xades.dll* et l’application *XadesTestClient.exe*, sont destinés à aider les développeurs à concevoir des applications XAdES.

De façon à en faciliter la découverte, les scénarios suivants illustrent les principaux cas d’utilisation au travers de l’application de test ainsi proposée. Cette application permet en effet de créer les différents types de signatures XAdES du standard éponyme. Ce chapitre précise pour chacun des 3 scénarios les modalités de mise en œuvre effective.

## Scénario 1 – Création d’une signature avancée XAdES simple

### Objectif du scénario

Ce scénario illustre comment créer une signature XAdES au niveau d’une machine cliente.

Ce scénario prend en compte divers aspects du standard XAdES Cf. section § Signature électronique avancée).

note_dd Remarque :

Avant de dérouler ce scénario, assurez-vous que vous avez effectué une fois les procédures d’installation et de compilation décrites dans le document Installation du Kit de démarrage XAdES.

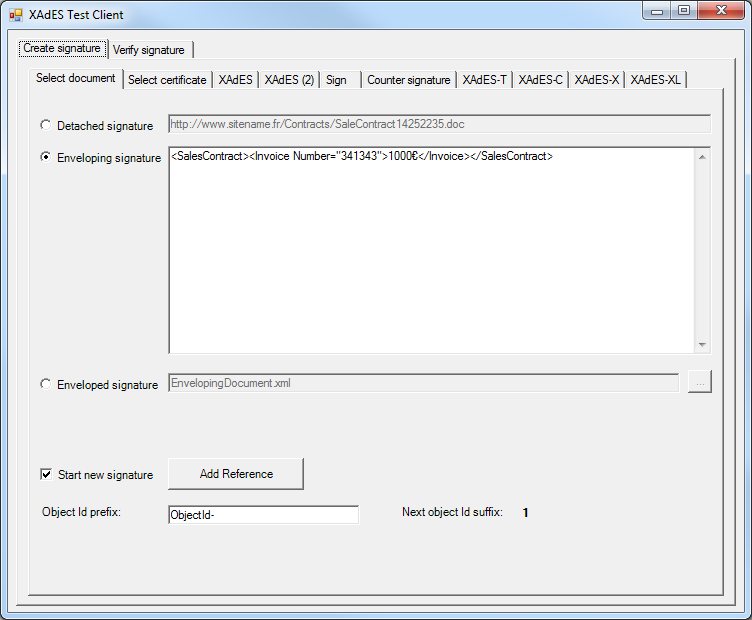
### Déroulé du scénario

#### Etape 1

Pour réaliser cette étape du scénario, veuillez procéder comme suit :



1. Exécutez l’application de test *XadesTestClient.exe*.
2. Sélectionnez l’onglet **Create signature** (si celui-ci ne l’est pas déjà).
3. Au sein de l’onglet **Create signature**, sélectionnez l’onglet **Select document** (si celui-ci ne l’est pas déjà).
4. Sélectionnez le type de relation entre le document et la signature (Cf. entouré 1 dans la capture ci-après) :
   1. Signature détachée (case **Detached signature**) : le fichier de signature résultant pointera vers le document externe (détaché) ;
   2. Signature enveloppante (case **Enveloping signature**) : la signature résultante contient (enveloppe) les données XML qui sont signée ;
   3. Signature enveloppée (case **Enveloped signature**) : la signature résultante est stockée (enveloppée) au sein du document XML signé.
5. Cliquez sur le bouton **Add Reference** pour ajouter le document (Cf. entouré 2 dans la capture ci-après).



**2**

**1**

Figure . Etape 1 du scénario 1

note_dd Remarque :

De façon optionnelle, vous pouvez ajouter des références supplémentaires en décochant le drapeau **Start new signature** et en cliquant sur le bouton **Add Reference** une seconde, troisième, etc. fois.

Description : important_ddImportant :

Avant de cliquer une première fois sur le bouton Add Reference, la case à cocher Start new signature doit impérativement être cochée de façon à ce qu’une initialisation adaptée puisse être effectuée.

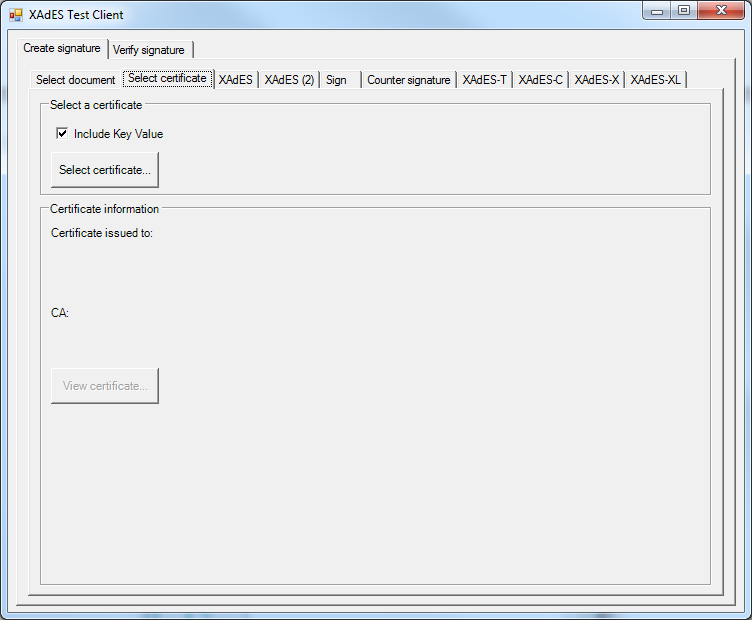
note_dd Remarque :

De façon optionnelle, vous pouvez modifier le préfixe utilisé pour l’identificateur Object (champs **Object Id prefix**).

#### Etape 2

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Sélectionnez l’onglet **Select certificate**.
2. Cliquez sur le bouton **Select certificate** (Cf. entouré 3 dans la capture ci-après).



**3**

Figure . Etape 2 du scénario 1

Vous êtes alors invité à sélectionner l’un des certificats présents dans votre magasin de certificat.

1. Sélectionnez le certificat de signature souhaité ; il peut s’agir d’un certificat présent sur carte à puce.

L’iconographie utilisée par la boîte de dialogue **Windows Security** est la suivante :

| Icône | Type de certificat |
| --- | --- |
|  | Représente un certificat logiciel. |
|  | Représente un certificat stocké sur carte à puce. |

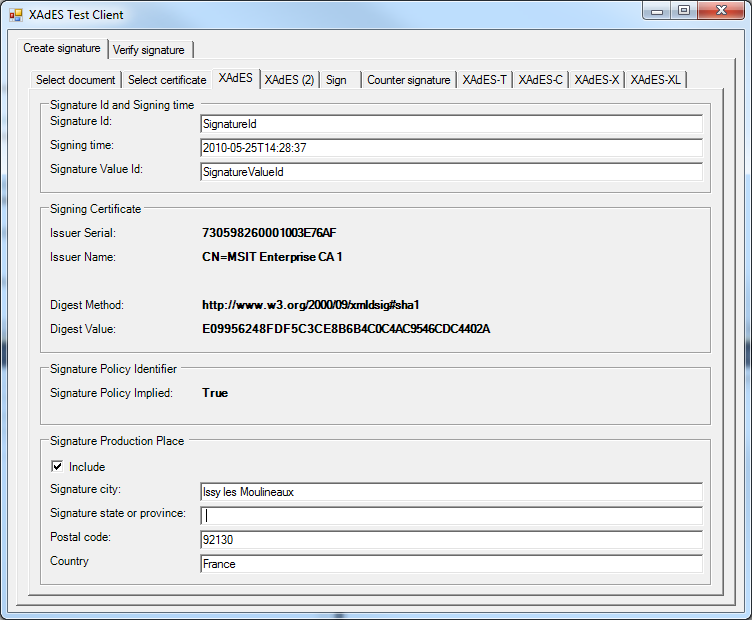
note_dd Remarque :

De façon optionnelle, si vous décochez la case **Include Key Value**, l’information relative à la clé publique n’est pas ajoutée à la signature. Dans l’implémentation proposée de l’application XadesTestClient.exe, vous ne serez pas alors en mesure de vérifier la signature ainsi créée.

#### Etape 3

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Sélectionnez l’onglet **XAdES**.
2. Cochez la case **Include** de la section **Signature Production Place** (Cf. entouré 4 dans la capture ci-après) et précisez les données souhaitées.



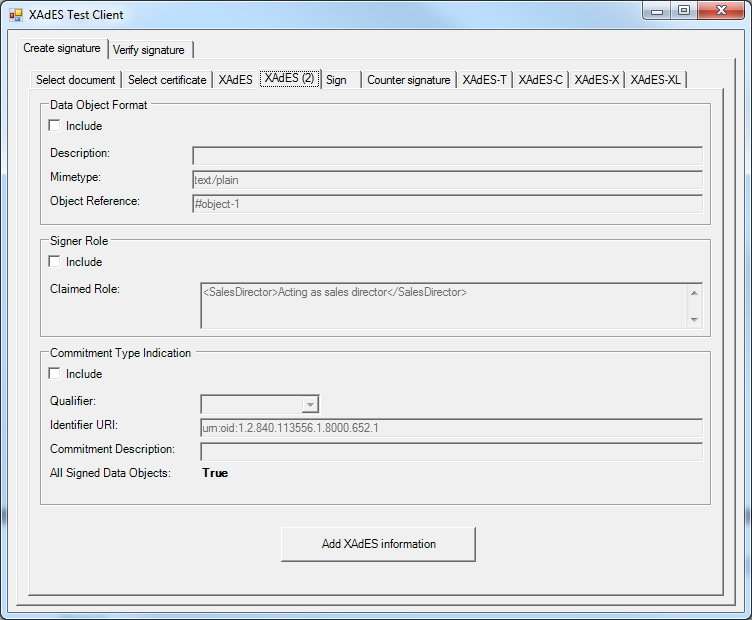
**4**

Figure . Etape 3 du scénario 1

#### Etape 4

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Sélectionnez l’onglet **XAdES (2)**.
2. Cliquez sur le bouton **Add XAdES info** pour ajouter l’information XAdES à la signature (Cf. entouré 5 dans la capture ci-après).



**5**

Figure . Etape 4 du scénario 1

note_dd Remarque :

De façon optionnelle, vous pouvez cocher les différentes cases **Include** et préciser les données associées aux contrôles ainsi activés.

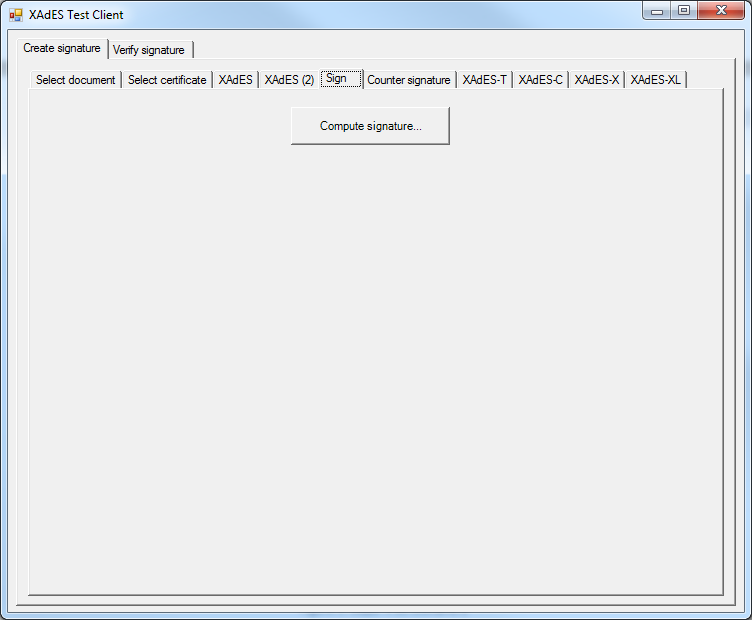
Description : important_ddImportant :

Toutes les données XAdES possibles qui peuvent être créées avec la bibliothèque *Microsoft.Xades.dll* ne peuvent pas forcément l’être avec l’application de test *XadesTestClient.exe*. Vous pouvez consulter la documentation *Microsoft.Xades.chm* (Cf. section § Génération de la documentation du code source de la bibliothèque Microsoft.Xades.dll du Kit de démarrage XAdES) de façon à considérer l’ensemble des possibilités offertes par la bibliothèque *Microsoft.Xades.dll*.

#### Etape 5

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Sélectionnez l’onglet **Sign**.
2. Cliquez sur le bouton **Compute signature** (Cf. entouré 6 dans la capture ci-après).



**6**

Figure . Etape 5 du scénario 1

Une boîte de dialogue s’ouvre alors avec la signature ainsi générée. Vous pouvez alors sauvegarder la signature en cliquant sur le bouton **Save signature** en précisant le chemin et nom du fichier XML pour la sauvegarde.

Vous avez créé à ce stade une signature XAdES élémentaire pour le ou les documents que vous avez référencés et toute l’information XAdES que vous avez sélectionnée.

## Scénario 2 – Horodatage et vérification d’une signature avancée XAdES

### Objectif du scénario

Ce scénario illustre comment vérifier une signature existante et ajouter un horodatage.

A l’instar du précédent scenario, ce dernier prend en compte divers aspects du standard XAdES (Cf. section § Signature électronique avancée).

note_dd Remarque :

Avant de dérouler ce scénario, assurez-vous que vous avez effectué une fois les procédures d’installation et de compilation décrites dans le document Installation du Kit de démarrage XAdES.

### Déroulé du scénario

#### Etape 1

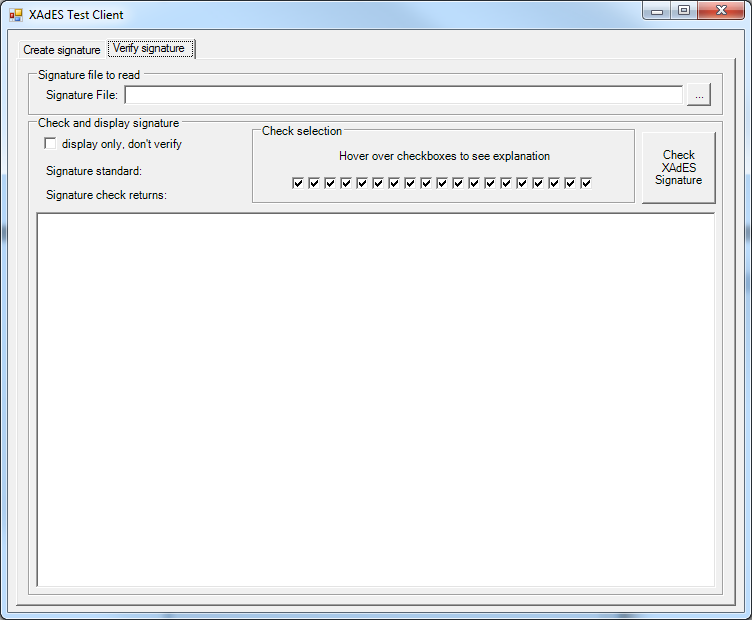
Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Exécutez l’application de test *XadesTestClient.exe*.
2. Sélectionnez l’onglet **Verify signature** (si celui-ci ne l’est pas déjà).
3. Sélectionnez le fichier de signature créé dans le scénario précédent (Cf. section § Scénario 1 – Création d’une signature avancée XAdES simple) en cliquant sur le bouton **…** (Cf. entouré 1 dans la capture ci-après).
4. Laissez les différentes cases cochées de façon à réaliser l’ensemble des tests sur la signature (Cf. entouré 2 dans la capture ci-après).

note_dd Remarque :

De façon optionnelle, vous pouvez décocher certains tests de façon à les retirer du jeu de tests.

1. Cliquez sur le bouton **Check XAdES Signature** (Cf. entouré 3 dans la capture ci-après) pour vérifier la signature sur la base du jeu de tests ainsi sélectionné. Si tel est le cas, le libellé **Signature check returns** doit indiquer **True**.



**3**

**2**

**1**

Figure . Etape 1 du scénario 2

#### Etape 2

Depuis l’application de test *XadesTestClient.exe* précédente en cours d’exécution, vous allez injecter un horodatage dans la signature venant d’être vérifiée.

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

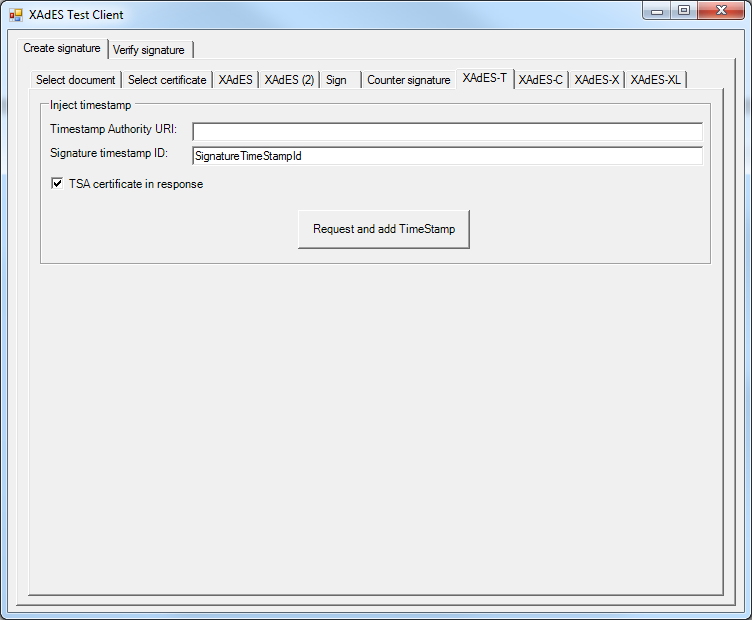
1. Sélectionnez l’onglet **Create signature**.
2. Au sein de l’onglet **Create signature**, sélectionnez l’onglet **XAdES-T**.
3. Précisez l’adresse (URL) du serveur d’horodatage (Cf. entouré 4 dans la capture ci-après).

note_dd Remarque :

Si vous ne disposez pas d'un serveur d’horodatage, vous pouvez essayer de trouver un serveur d’horodatage de test sur Internet. Pour cela, vous pouvez effectuer une recherche sur la toile avec la requête « *TSA test server RFC 3161* ».

Assurez-vous au préalable que vous disposez bien des permissions au niveau du serveur sélectionné avant d'effectuer l'essai.

1. Cliquez sur le bouton **Request and add Timestamp** (Cf. entouré 5 dans la capture ci-après) pour envoyer une demande d’horodatage au serveur et injecter l’horodatage dans la signature.



**5**

**4**

Figure . Etape 2 du scénario 2

Une boîte de dialogue contextuelle s’ouvre. Vous pouvez voir l'horodatage inséré et l’enregistrer.

## Scénario 3 – Préparation d’une signature avancée XAdES pour le stockage

### Objectif du scénario

Ce scénario illustre comment ajouter des données à une signature existante horodatée en vue d’un stockage prolongé.

Comme précédemment, ce scénario prend en compte divers aspects du standard XAdES Cf. section § Signature électronique avancée) et permet de parcourir les diverses fonctionnalités de l’application de test *XadesTestClient.exe*.

note_dd Remarque :

Avant de dérouler ce scénario, assurez-vous que vous avez effectué une fois les procédures d’installation et de compilation décrites dans le document Installation du Kit de démarrage XAdES.

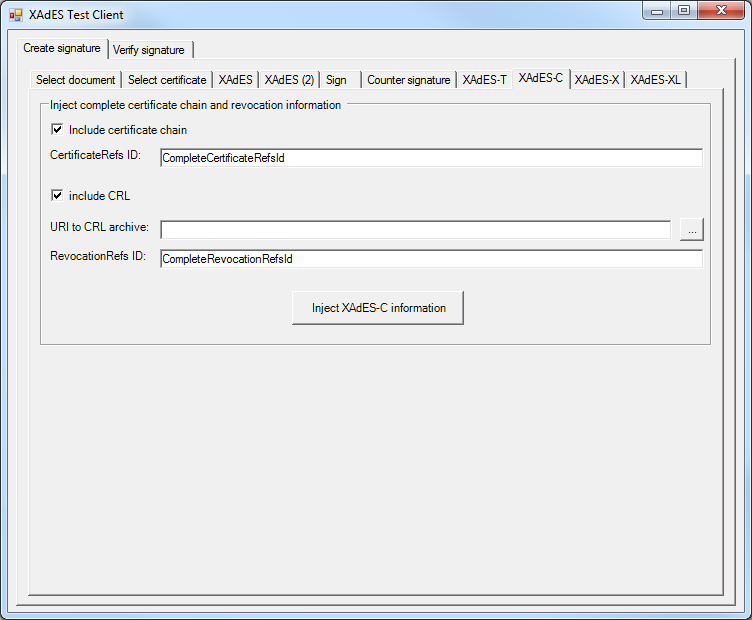
### Déroulé du scénario

#### Etape 1

Cette étape s’inscrit directement à la suite du scénario 2 (Cf. section § Scénario 2 – Horodatage et vérification d’une signature avancée XAdES). Vous pouvez également partir de la vérification de la signature XAdES-T.

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Sélectionnez l’onglet **Create signature**.
2. Au sein de l’onglet **Create signature**, sélectionnez l’onglet **XAdES-C**.
3. Cochez la case **Include certificate chain** (Cf. entouré 1 dans la capture ci-après).
4. Cochez la case **Include CRL** (Cf. entouré 2 dans la capture ci-après).
5. Sélectionnez le fichier de liste de révocation pour la signature sélectionnée (Cf. entouré 3 dans la capture ci-après). Cette étape suppose que vous disposez du fichier en question sur le disque local ou sur un partage réseau accessible.
6. Cliquez sur le bouton **Inject XAdES-C information** (Cf. entouré 4 dans la capture ci-après) pour créer une signature XAdES-C.



**2**

**1**

**3**

**4**

Figure . Etape 1 du scénario 3

1. Fermez la boîte de dialogue contextuelle qui s’est ouverte.

note_dd Remarque :

A ce stade, vous n’avez pas besoin de sauvegarder la signature si vous souhaitez poursuivre le scénario.

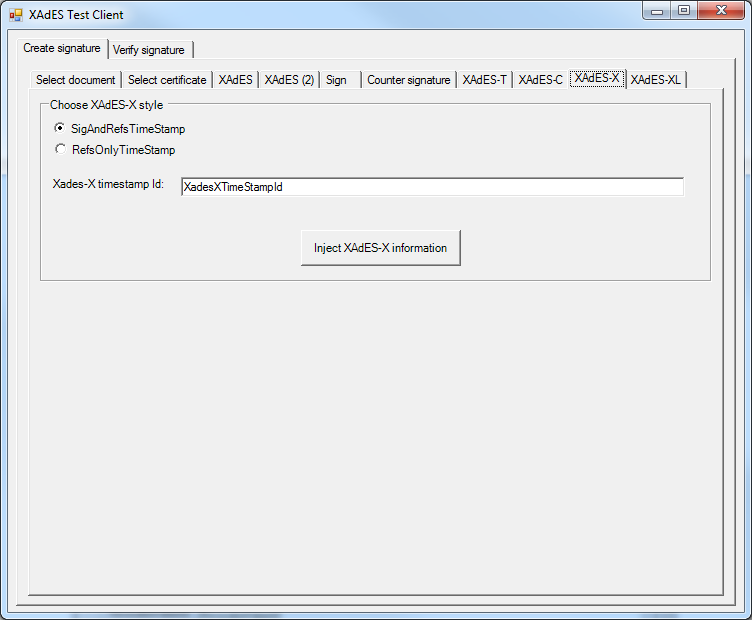
#### Etape 2

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Au sein de l’onglet **Create signature**, sélectionnez l’onglet **XAdES-X**.

Les boutons radio **SigAndRefsTimeStamp** et **RefsOnlyTimeStamp** vous permettent de spécifier le type de signature XAdES-T souhaité (Cf. entouré 5 dans la capture ci-après).

1. Cliquez sur le bouton **Inject XAdES-X information** (Cf. entouré 6 dans la capture ci-après) pour créer une signature XAdES-X.



**6**

**5**

Figure . Etape 2 du scénario 3

note_dd Remarque :

La demande d’horodatage est transmise au serveur d’horodatage précisé dans l’onglet **XAdES-T**.

1. Comme à l’étape précédente, fermez simplement la boîte de dialogue contextuelle qui s’est ouverte.

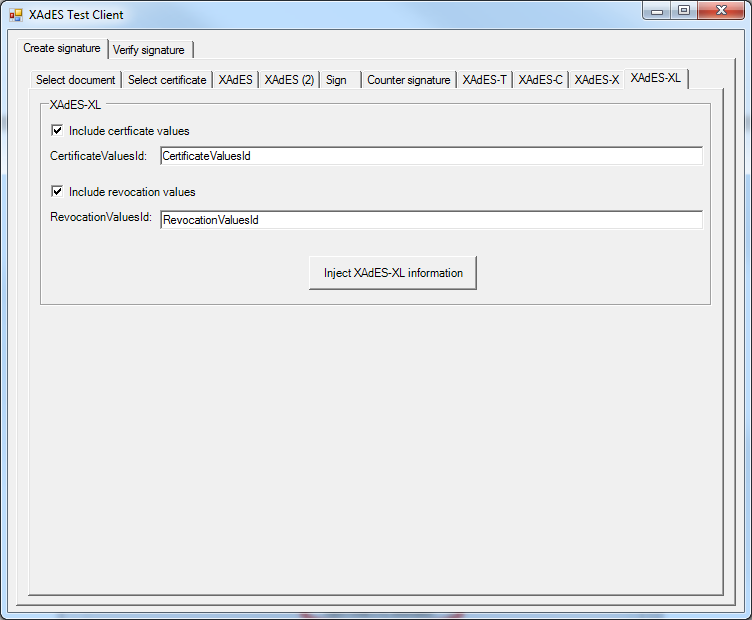
note_dd Remarque :

A ce stade, vous n’avez pas besoin de sauvegarder la signature si vous souhaitez poursuivre le scénario.

#### Etape 3

Description : procedure_ddPour réaliser cette étape du scénario, veuillez procéder comme suit :

1. Au sein de l’onglet **Create signature**, sélectionnez l’onglet **XAdES-XL**.
2. Cochez la case **Include certificate values** (Cf. entouré 7 dans la capture ci-après).
3. Cochez la case **Include revocation values** (Cf. entouré 8 dans la capture ci-après).
4. Cliquez sur le bouton **Inject XAdES-XL information** (Cf. entouré 9 dans la capture ci-après) pour créer une signature XAdES-X-L.



**7**

**9**

**8**

Figure . Etape 3 du scénario 3

Une boîte de dialogue contextuelle s’ouvre. Vous pouvez stocker (enregistrer) la signature XAdES-X-L.

# Références

ETSI 101 903 XML Advanced Electronic Signatures (XAdES) : <http://uri.etsi.org/01903>

W3C XML Advanced Electronic Signatures (XAdES) : <http://www.w3.org/TR/XAdES/>

1. 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-1)
2. 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-2)
3. 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-3)
4. Weblog Decrypt my World:Cryptography, Security, Debugging and more! : http://blogs.msdn.com/b/alejacma/ [↑](#footnote-ref-4)
5. 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-5)
6. 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-6)
7. Article MSDN Asymmetric Keys : http://msdn.microsoft.com/en-us/library/aa387460(VS.85).aspx [↑](#footnote-ref-7)
8. Site Active Directory Certificate Services : http://go.microsoft.com/fwlink/?LinkId=119113 [↑](#footnote-ref-8)
9. Article MICROSOFT ROOT CERTIFICATE PROGRAM : http://technet.microsoft.com/fr-fr/library/cc751157(en-us).aspx [↑](#footnote-ref-9)
10. Article WINDOWS ROOT CERTIFICATE PROGRAM MEMBERS : http://support.microsoft.com/kb/931125/en-US [↑](#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. RFC3275 (Extensible Markup Language) XML-Signature Syntax and Processing : http://tools.ietf.org/html/rfc3275 [↑](#footnote-ref-12)
13. ETSI 101 903 XML Advanced Electronic Signatures (XAdES) : http://uri.etsi.org/01903 [↑](#footnote-ref-13)
14. W3C XML Advanced Electronic Signatures (XAdES) : http://www.w3.org/TR/XAdES/ [↑](#footnote-ref-14)
15. ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats : http://docbox.etsi.org//EC\_Files/EC\_Files/ts\_101733v010501p.pdf [↑](#footnote-ref-15)
16. RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) : http://tools.ietf.org/html/rfc3161 [↑](#footnote-ref-16)
17. 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-17)
18. Didacticiel Microsoft QuEST (Qualified Electronic Signatures Tutorial) : http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf [↑](#footnote-ref-18)
19. QuEST Didacticiel sur les signatures électroniques qualifiées – Présentation technique : http://download.microsoft.com/download/a/c/3/ac39eebf-96a1-40c1-bbd4-45825ab81b21/QuEST\_Technical\_Blueprint(Version1.00June2004).pdf [↑](#footnote-ref-19)
20. QuEST Didacticiel sur les signatures électroniques qualifiées – Glossaire et abréviations : http://download.microsoft.com/download/a/c/3/ac39eebf-96a1-40c1-bbd4-45825ab81b21/QuEST\_Glossary(Version1.00June2004).pdf [↑](#footnote-ref-20)
21. Espace de noms *System.Security.Cryptography.Xml* : http://msdn.microsoft.com/en-us/library/system.security.cryptography.xml(VS.71).aspx [↑](#footnote-ref-21)
22. Classe SignedXml : http://msdn.microsoft.com/en-us/library/system.security.cryptography.xml.signedxml.aspx [↑](#footnote-ref-22)
23. Programme Reflector : http://reflector.red-gate.com/download.aspx?TreatAsUpdate=1 [↑](#footnote-ref-23)
24. La signature électronique avec .NET : http://stormimon.developpez.com/dotnet/signature-electronique/ [↑](#footnote-ref-24)
25. Schéma XAdES : http://uri.etsi.org/01903/v1.1.1/XAdES.xsd [↑](#footnote-ref-25)
26. Thèse XML Advanced Electronic Signatures (XAdES) - Implementation and Interoperability: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.137.1977&rep=rep1&type=pdf [↑](#footnote-ref-26)
27. Fil de discussion Signature namespace prefix : http://social.msdn.microsoft.com/Forums/en-US/xmlandnetfx/thread/e57fcba9-3b42-4a63-acb9-aedf06e29cd8 [↑](#footnote-ref-27)
28. Tutoriel Bien commenter et documenter son code en C# : ftp://ftp-developpez.com/vincentlaine/dotnet/comdoc.pdf [↑](#footnote-ref-28)
29. Blog Sandcastle - Documentation compiler: http://blogs.msdn.com/sandcastle/ [↑](#footnote-ref-29)