Nations Unies ECE/TRADE/C/CEFACT/2010/14

Conseil économique et social

Distr. générale
27 septembre 2010
Français
Original: anglais

Commission économique pour l'Europe

Comité du commerce

Centre pour la facilitation du commerce et les transactions électroniques

Seizième session
Genève, 8-10 décembre 2010
Point 7 de l'ordre du jour provisoire
Normes et recommandations nouvelles et révisées

Recommandation n° 37: Interopérabilité des preuves numériques signées

Document présenté par le Groupe de travail de l'architecture et la construction (TBG6) pour approbation

Résumé

La présente Recommandation définit un ensemble de règles fonctionnelles qui devraient être suivies pour les preuves numériques signées, en ce qui concerne l'organisation et les liens entre le contenu signé, les certificats et les signatures des signataires. Elle est présentée par le TBG6 à la Plénière pour approbation.

Table des matières

Avant-propos

La Recommandation relative à l'interopérabilité des preuves numériques signées a pour objet de renforcer le niveau d'interopérabilité des preuves numériques signées par voie électronique afin de faciliter le développement du commerce international dématérialisé, c'est-à-dire sans papier.

À cet effet, elle définit un ensemble de règles fonctionnelles qui devraient être suivies pour les preuves numériques signées, en ce qui concerne l'organisation et les liens entre le contenu signé, les certificats et les signatures des signataires.

Elle ne vise pas les aspects juridiques des signatures électroniques, qui sont traités au niveau international dans d'autres documents tels que ceux publiés par la CNUDCI[1, 2, 3], ni la sémantique, la possibilité d'utilisation ou l'interprétation du contenu signé. Elle n'est pas incompatible avec la Recommandation n° 14 de la CEE intitulée «Authentification des documents commerciaux par des moyens autres que la signature».

Pour faciliter l'application des règles susmentionnées, l'annexe B donne des exemples de mise en œuvre technique au moyen de certaines des normes les plus récentes en matière de preuves numériques. L'annexe pourra être actualisée dans le futur pour prendre en compte d'autres applications techniques proposées.

Comme il est urgent d'améliorer l'interopérabilité dans le domaine de la vérification des preuves numériques, la Recommandation et ses annexes sont réalisées simultanément pour accélérer la mise en œuvre.

Résumé

À la différence d'un document sur support papier, un document numérique a une faible valeur probante tant qu'il n'est pas renforcé par un mécanisme, par exemple une signature électronique, qui garantit son intégrité et son authenticité.

Cependant, les normes relatives aux signatures électroniques étant très nombreuses, il peut être impossible pour le destinataire de preuves numériques signées de les vérifier, ce qui a une incidence directe sur la capacité des entreprises et des administrations à échanger en toute sécurité des documents numériques entre eux et avec leurs homologues administratifs et financiers.

Pour résoudre cette question, une démarche fonctionnelle plus que technique a été adoptée dans la présente Recommandation en ce qui concerne les preuves numériques signées, l'accent étant mis d'abord sur le «quoi», et non sur le «quand».

La vérification des preuves numériques signées doit au moins donner au vérificateur une vision claire des éléments ci-après:

- Paramètres des signatures (date, lieu, type d'engagement);
- Intégrité du contenu signé;
- Intégrité et validité des certificats des signataires;
- Crédibilité des prestataires de services de certification.

La présente Recommandation définit donc des prescriptions simples et générales relatives à la création et à leur vérification des preuves numériques signées, le but étant d'améliorer leur interopérabilité. Il convient de noter qu'une fois adoptée, la Recommandation fera, le temps passant, l'objet de demandes de modifications.

1. Recommandation n° 37: Interopérabilité des preuves numériques signées

La présente Recommandation encourage toute organisation désireuse d'échanger des preuves numériques signées avec d'autres organisations à en maximiser l'interopérabilité en observant un ensemble de principes proposés.

Les preuves numériques signées:

- DOIVENT contenir un et un seul contenu identifiable;
- DOIVENT comporter une ou plusieurs signatures;
- DOIVENT contenir sans ambiguïté toutes les identités concernées.

Chaque signature figurant dans les preuves:

- PEUT comporter une date de signature et d'autres propriétés;
- DOIT viser la totalité du contenu;
- PEUT être assortie d'une ou de plusieurs contreseings.

1.1 Avantages

La Recommandation fournit aux entreprises, aux administrations et aux organismes financiers un ensemble de prescriptions simples et normalisées concernant l'échange de documents sécurisés, auxquelles peut satisfaire toute une gamme de technologies et produits normalisés, y compris les projets sources ouverts.

Ses objectifs sont les suivants:

- Améliorer l'efficacité et la fiabilité de la vérification des preuves numériques signées reçues par une partie;
- Accroître l'interopérabilité des preuves numériques signées, ce qui renforcera la confiance;
- Offrir des moyens nombreux mais coordonnés d'augmenter le taux d'adoption des technologies sans papier.

2. Contexte

2.1 Champ d'application

1. Depuis le début des années 90, de nombreuses normes techniques ont été conçues, proposées et adoptées dans le domaine des preuves numériques signées. On en trouvera des exemples dans les notes 4 à 12[4, 5, 6, 7, 8, 9, 10, 11, 12].

2. Cependant, cette multiplicité de normes, conjuguée à de nombreuses options et à l'absence de lignes directrices quant à la façon d'appliquer des signatures numériques aux documents, n'a pas permis d'assurer l'interopérabilité des preuves numériques signées au niveau de la syntaxe, de la sémantique et du traitement.

3. Le présent document propose une nouvelle approche en ce qui concerne la création et la vérification des preuves numériques signées, une attention particulière étant prêtée aux aspects fonctionnels plutôt qu'aux aspects techniques.

4. Il sera ainsi possible de définir un profil fonctionnel commun qui simplifiera et facilitera l'échange et la vérification de documents électroniques à valeur probante.

5. La présente Recommandation offre un ensemble de prescriptions fonctionnelles visant à faciliter la conception d'applications de création et de vérification de preuves numériques signées interopérables. Elle présente également des exemples d'application à certaines des normes techniques les plus récentes concernant les preuves numériques signées.

6. Par commodité, on utilisera ci-après l'expression «la Recommandation» pour désigner la «Recommandation relative à l'interopérabilité des preuves numériques signées».

2.2 Objectif

7. Les caractéristiques décrites ont pour objet d'augmenter le taux de dématérialisation des documents sur support papier en facilitant la création, la validation et l'interopérabilité des documents électroniques à valeur probante et leur intégration dans des applications commerciales.

8. Du point de vue de l'utilisateur final, le recours aux signatures numériques comprend deux principaux processus:

- Signature d'un document;
- Vérification de la signature.

9. En matière d'appels d'offres et de facturation par voie électronique, la pratique montre qu'il faut résoudre un certain nombre de problèmes d'interopérabilité lorsqu'une partie signe un document avec son logiciel de certification et de signature:

- Interopérabilité des formats de signature: le logiciel de vérification est souvent incapable de traiter le format de la signature numérique reçue ou de savoir à quel fichier la signature correspond et où se trouve la signature;
- Valeur sémantique de la signature: le logiciel de vérification ou le format de la signature peut ne pas permettre de comprendre l'intention du signataire (par exemple, a-t-il voulu assurer l'intégrité de son document, approuver le contenu signé, ou autre chose?);
- Validité du certificat: le logiciel de vérification peut ne pas être capable de déterminer si le certificat est fiable ou s'il était déjà révoqué à la date de la signature.

10. L'échec de la vérification de la signature est d'une importance cruciale, par exemple avant ou pendant le stade de passation des marchés publics, puisque des soumissions pourraient être considérées comme étant non valables et rejetées par erreur.

11. Pour remédier aux deux premières catégories de problèmes, toutes les signatures produites doivent être présentées dans un format que tous les progiciels de vérification susceptibles d'être utilisés seront capables de gérer.

12. En conséquence, les principaux avantages des caractéristiques proposées pour les preuves numériques signées sont les suivants:

- Instaurer la confiance en offrant des fonctions générales permettant de créer, de vérifier et de gérer aisément les preuves numériques signées;
- Assurer l'interopérabilité des preuves numériques signées au moyen d'un dénominateur commun fonctionnel ainsi que l'indépendance à l'égard du format technique utilisé;
- Simplifier l'intégration des signatures numériques dans les applications commerciales et d'archivage, pour remplacer plus facilement une fonction d'«impression» par une fonction de «signature» ou de «certification».

2.3 Public

13. Le présent document est principalement destiné aux organisations et aux personnes souhaitant:

- Échanger des preuves numériques signées dans un environnement ouvert;
- Choisir un format de preuves numériques signées approprié à un projet de dématérialisation particulier;
- Suivre les technologies de l'information dans les domaines des signatures numériques et de l'archivage à valeur probante;
- Assurer l'interopérabilité, la réversibilité et la validité des preuves numériques signées.

3. Définitions

La présente section définit brièvement les termes et abréviations utilisés dans le document.

AdES: Advanced Electronic Signature (signature électronique avancée)

BES: Basic Electronic Signature (signature électronique de base)

CAdES: CMS Advanced Electronic Signature (signature électronique avancée à syntaxe de message cryptographique)

CEN: Comité européen de normalisation

Certificat: désigne un message de données ou un autre enregistrement confirmant le lien entre un signataire et des données afférentes à la création de signature (réf. 2)

Preuves numériques signées: document numérique pouvant être présenté comme preuve

CMS: Cryptographic Message Syntax (syntaxe de message cryptographique)

CRL: Certificate Revocation List (liste de certificats révoqués)

PSC: prestataire de services de certification: désigne une personne qui émet des certificats et peut fournir d'autres services liés aux signatures électroniques (réf. 1)

CWA: CEN Workshop Agreement

Cosignature: signature qui s'applique au même contenu qu'une autre signature

Contresignataire: personne qui détient des données afférentes à la création de contreseing et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente

Contreseing: signature qui s'applique à une signature (le contenu signé d'un contreseing est lui-même une signature); on peut aussi utiliser l'expression «signature hiérarchique»

Signature électronique: données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue (réf. 1)

EPES: Explicit Policy based Electronic Signature (signature électronique fondée sur une politique explicite)

ETSI: Institut européen des normes de télécommunication

UE: Union européenne

ISO: Organisation internationale de normalisation

OASIS: Organization for the Advancement of Structured Information Standards

OCSP: Online Certificate Status Protocol (protocole de vérification en ligne de certificat)

PAdES: PDF Advanced Electronic Signature (signature électronique avancée PDF)

PDF: Portable Data Format (format de document portable)

PKCS: Public Key Cryptographic Standard (norme de cryptographie à clef publique)

PKI: Public Key Infrastructure (infrastructure à clef publique)

RFC: Request For Comment (demande de commentaires)

SDEIR: Recommandation relative à l'interopérabilité des preuves numériques signées

Signataire: personne qui détient des données afférentes à la création de signature et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente (réf. 1)

Contenu signé: données contenues dans les preuves numériques signées qui sont signées par le ou les signataires

SSCD: Secure Signature Creation Device (dispositif sécurisé de création de signature)

Ancre de confiance: désigne un certificat qui a la confiance d'un vérificateur; souvent appelée «certificat source»

TS: spécification technique

TSL: TSP Status List (liste du statut des services de confiance)

TSP: Trusted Services Provider (prestataire de services de confiance)

XAdES: XML Advanced Electronic Signature (signature électronique avancée XML)

XML: langage de balisage extensible

XMLDSIG: XML Digital Signature (signature numérique XML)

4. Lignes directrices à l'intention des utilisateurs de la Recommandation

14. La présente section décrit les caractéristiques fonctionnelles et les règles de gestion qui constituent la Recommandation.

4.1 Caractéristiques des preuves numériques signées visées par la Recommandation

15. La Recommandation définit les caractéristiques des preuves numériques signées visant à maximiser l'interopérabilité entre la création et la vérification des preuves numériques signées.

16. Les caractéristiques sont décrites comme étant un ensemble de règles fonctionnelles.

4.2 Caractéristiques fonctionnelles

17. Les caractéristiques fonctionnelles des preuves numériques signées proposées sont les suivantes:

- Un et un seul contenu signé assorti du type de contenu et d'un nom facultatif;
- Signatures et cosignatures du contenu signé;
- Contreseings en tant que propriétés non signées d'une signature ou d'un contreseing;
- Propriétés signées d'une signature ou d'un contreseing:

- Date de signature: indique le moment où le signataire affirme avoir effectué le processus de signature;
- Lieu où se trouve le signataire: indique une mnémonique relative à une adresse liée au signataire en un lieu géographique particulier (par exemple une ville);
- Référence à une politique de signature qui décrit le rôle et les engagements précis que le signataire entend assumer pour les données signées;
- Type d'engagement lié à la signature: indique explicitement à un vérificateur le type spécifique d'engagement pris par le signataire à la signature des données;
- Rôle(s) du signataire: indique le ou les rôles ou la ou les positions déclarés par le signataire à la signature des données;
- Références au certificat du signataire et à ses certificateurs;

- Estampilles temporelles en tant que propriétés non signées d'une signature ou d'un contreseing;
- Certificats des signataires et des contresignataires et de leurs certificateurs.

4.3 Différences entre preuves numériques et preuves sur support papier

18. Les deux types de preuves présentent de nombreuses caractéristiques communes, mais il existe aussi des différences importantes telles que les suivantes:

- L'identité des signataires ne figure pas toujours sur les preuves sur support papier;
- L'identité des ancêtres du signataire ne figure généralement pas sur les preuves sur papier;
- En revanche, les preuves signées sur support papier comportent généralement une signature manuscrite, tandis qu'une signature numérique figurant sur un document électronique n'est pas censée être représentée graphiquement. En règle générale, seul un programme informatique peut effectuer les calculs mathématiques complexes indispensables pour vérifier une signature numérique.

4.4 Mise en œuvre de la Recommandation

19. Pour les lignes directrices concernant la mise en œuvre de la Recommandation et destinées aux utilisateurs, prière de se reporter aux annexes A et B.

5. Conclusion

20. Les caractéristiques des preuves numériques signées exposées dans le présent document ont pour objet de généraliser la dématérialisation des documents sur support papier en simplifiant et en facilitant la création, la vérification et l'échange de messages numériques sécurisés à valeur probante ainsi que leur intégration dans des applications commerciales.

Annexe A (non normative): Règles de mise en œuvre fonctionnelle

A.1 Niveaux

La Recommandation définit l'importance de certaines prescriptions au moyen de niveaux, qui sont au nombre de deux dans la présente version:

- Le «niveau de base» est le niveau le plus simple à mettre en œuvre;
- Le «niveau 1» constitue une version plus contraignante de la Recommandation et offre une meilleure interopérabilité, par exemple en imposant une date de signature signée pour chaque signature, ainsi que des références signées pour tous les certificateurs et leurs certificats.

A.2 Mots clefs

Les mots clefs «DOIT», «NE DOIT PAS», «EXIGÉ», «DEVRAIT», «NE DEVRAIT PAS», «DEVRA», «RECOMMANDÉ», «PEUT» et «FACULTATIF» dans le présent document (en majuscules) sont à interpréter comme décrits dans la RFC (Request For Comments) 2119[13].

A.3 Profils d'application

La spécification définit deux profils d'application:

- Applications de création conformes à la Recommandation;
- Applications de vérification conformes à la Recommandation.

A.4 Prescriptions

Les 18 prescriptions de la Recommandation sont décrites ci-après. Elles ne sont pas mises en œuvre par toutes les normes techniques relatives aux signatures numériques existant au moment de la publication du présent document. Par conséquent, il est recommandé au lecteur de vérifier si la norme technique retenue pour la mise en œuvre prend en charge les prescriptions choisies. Prière de se reporter à l'annexe technique pour des précisions concernant certaines mises en œuvre proposées.

P1. Les preuves numériques signées DOIVENT comporter un et un seul contenu signé comprenant des données, le type de contenu et un nom FACULTATIF.

P2. Les preuves numériques signées DOIVENT comporter au moins une signature. Au moins cinq (co)signatures DOIVENT être prises en charge par une application de création ou de vérification conforme. Si des cosignatures supplémentaires sont présentes et que l'application de vérification ne les accepte pas, la vérification DOIT être déclarée incomplète.

P3. Chaque signature DOIT viser l'ensemble du contenu signé, à savoir les données, le type de contenu et un nom FACULTATIF.

P4. Une signature PEUT être faite par un ou plusieurs contresignataires. Au moins cinq contreseings d'une signature DOIVENT être pris en charge par une application de création ou de vérification conforme. Si des contreseings supplémentaires sont présents et que l'application de vérification ne les prend pas en charge, la vérification doit être déclarée incomplète.

P5. Un contreseing DOIT correspondre à une et une seule signature et à un ou un seul contreseing, et NE DOIT PAS viser le contenu signé ou autre chose. Un contreseing

DOIT être inclus en tant que propriété non signée de la signature ou du contreseing auquel il correspond.

P6. Un contreseing PEUT être fait par un ou plusieurs contresignataires. Au moins un contreseing d'un contreseing DOIT être pris en charge par une application de création ou de vérification conforme. Si des niveaux supplémentaires de contreseing sont présents et que l'application de vérification ne les accepte pas, la vérification doit être déclarée incomplète.

P7. Une signature ou un contreseing PEUT être horodaté au maximum par une seule estampille temporelle, qui DOIT être incorporée en tant que propriété non signée de la signature ou du contreseing.

P8. Les preuves numériques signées DOIVENT comporter les certificats des signataires et des contresignataires visés par les références signées mentionnées dans la prescription [P9].

P9. Une signature ou un contreseing DOIT comporter une référence signée non ambiguë aux certificats du signataire ou du contresignataire. Cette exigence a pour objet de lier sans ambiguïté le signataire à sa signature et de s'assurer que le vérificateur n'a pas besoin de «deviner» le certificat du signataire ou du contresignataire pour pouvoir vérifier la signature.

P10-niveau de base. Les preuves numériques signées PEUVENT comporter les certificats des certificateurs des signataires ou des contresignataires visés ou non par les références signées mentionnées dans la prescription [P11-niveau de base].

P10-niveau 1. Les preuves numériques signées DOIVENT comporter les certificats des certificateurs de tous les signataires et contresignataires visés par les références signées mentionnées dans la prescription [P11-niveau 1].

P11-niveau de base. Une signature ou un contreseing PEUT comporter des références signées aux certificats des certificateurs du signataire ou du contresignataire, le but étant de fournir au vérificateur des informations pour vérifier le certificat du signataire ou du contresignataire.

P11-niveau 1. Une signature ou un contreseing DOIT comporter toutes les références signées aux certificats des certificateurs du signataire ou du contresignataire. Cette exigence permet de s'assurer que le vérificateur n'a pas besoin de «chercher» le certificat d'un certificateur pour vérifier le certificat du signataire ou du contresignataire.

P12-niveau de base. Une signature ou un contreseing PEUT comporter une date de signature signée.

P12-niveau 1. Une signature ou un contreseing DOIT comporter une date de signature signée.

P13. Une signature ou un contreseing PEUT comporter au maximum un lieu de signature signé.

P14. Une signature ou un contreseing PEUT comporter au maximum une politique de signature signée.

P15. Une signature ou un contreseing PEUT comporter un ou plusieurs rôles signés liés au signataire.

P16-niveau de base. Une signature ou un contreseing PEUT comporter au maximum un type d'engagement signé.

P16-niveau 1. S'il est présent, le type d'engagement DOIT être l'un des suivants (les types d'engagement énumérés dans la présente prescription ont été repris des normes CAdES et XAdES, la liste pouvant évoluer à l'avenir):

- Preuve de création, indiquant que le signataire a créé le contenu signé, mais ne l'a pas approuvé ou n'en est pas l'expéditeur. Ce type particulier de consentement est important compte tenu de la nécessité de garantir parfois l'intégrité et l'authenticité d'un document sans faire intervenir un autre type d'engagement. C'est le cas des factures électroniques[14], qui doivent être protégées uniquement au niveau de l'intégrité et de l'authenticité. Un autre exemple où ce type d'engagement est utile est le cas des contrats qui doivent d'abord être protégés uniquement au niveau de l'intégrité et de l'authenticité par l'initiateur et ensuite approuvés par le destinataire (contrat de travail par exemple);
- Preuve d'approbation, indiquant que le signataire a approuvé le contenu signé;
- Preuve de l'origine, indiquant que le signataire reconnaît avoir créé, approuvé et expédié le contenu signé;
- Preuve de l'expéditeur, indiquant que l'entité fournissant l'indication est l'expéditeur du contenu signé mais ne l'a pas nécessairement créé;
- Preuve de réception, indiquant que le signataire reconnaît avoir reçu le contenu signé;
- Preuve de délivrance, indiquant que l'autorité d'horodatage fournissant l'indication a remis le contenu signé dans une unité de stockage locale accessible au destinataire du contenu signé.

P17-niveau de base. Une signature ou un contreseing PEUT comporter d'autres propriétés signées dont la prise en charge par une application de vérification conforme à la Recommandation est FACULTATIVE.

P17-niveau 1. Une signature ou un contreseing NE DOIT PAS comporter d'autres propriétés signées.

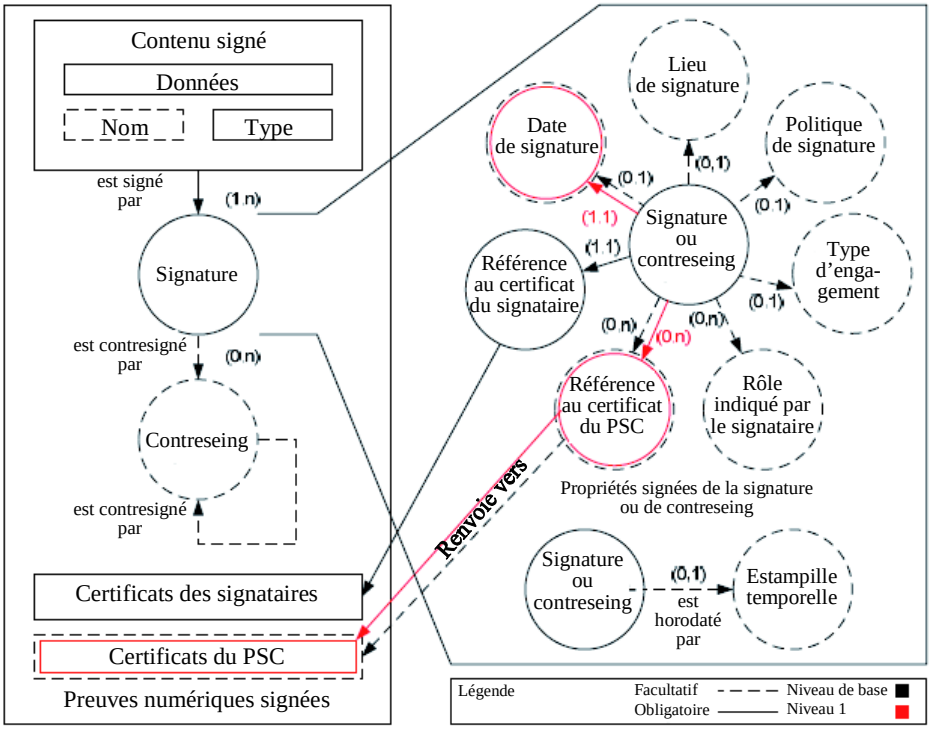
P18. Une signature ou un contreseing PEUT comporter d'autres propriétés non signées, dont la prise en charge par une application de vérification conforme à la Recommandation est FACULTATIVE. La présence de propriétés non signées non prises en charge NE DOIT PAS influer sur l'interprétation de la signature par le vérificateur.

A.5 Représentation schématique des preuves numériques conformes à la Recommandation

On trouvera dans la présente section une représentation schématique de la structure et de l'organisation des preuves en question.

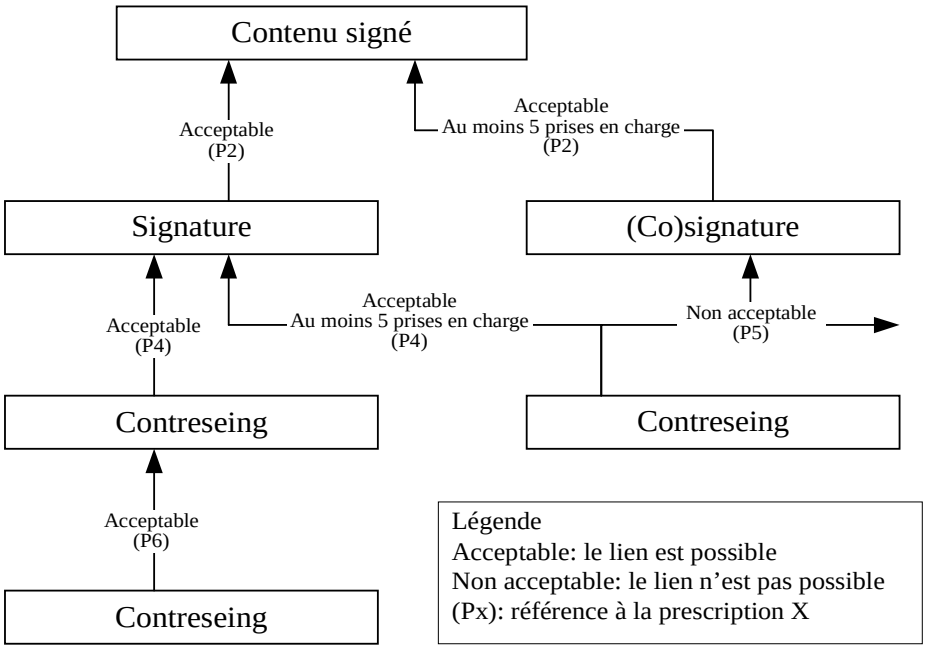
La figure ci-après montre la structure et l'organisation générales des preuves numériques signées conformes à la Recommandation. Les prescriptions 17 et 18 ne sont pas représentées.

Preuves numériques conformes à la Recommandation: représentation de la structure et de l'organisation générales



La figure ci-dessous représente les liens entre les signatures, les cosignatures et les contreseings des preuves numériques conformes à la Recommandation.

Preuves numériques conformes à la Recommandation: représentation des liens entre les signatures



A.6 Processus de vérification conforme à la Recommandation

La vérification des preuves numériques signées peut être effectuée par le signataire, le destinataire du message ou toute tierce partie intéressée.

A.6.1 Statut de la vérification

La vérification des preuves numériques signées comprend deux étapes:

- Vérification des prescriptions P1 et P2, applicables aux preuves numériques signées dans leur ensemble;
- Vérification de chaque signature appliquée aux preuves numériques signées.

La vérification des preuves numériques signées DOIT indiquer un statut, dont la valeur est:

- SUCCÈS: les preuves numériques signées ont été vérifiées avec succès, ce qui signifie que les prescriptions P1 et P2 ont été remplies et que toutes les signatures ont été vérifiées avec succès.
- ÉCHEC: lorsque les prescriptions P1 et/ou P2 ne sont pas remplies et/ou lorsque la vérification d'une ou de plusieurs signatures s'est soldée par un échec, toutes les causes de cet échec DOIVENT être indiquées.

A.6.2 Processus de vérification des signatures

Les informations concernant la référence temporelle utilisée pendant le processus de vérification d'une signature permettent de s'assurer de la validité de la signature au moment de sa création. Cette référence temporelle varie selon la politique de validation des signatures appliquée et les valeurs pouvant être utilisées sont les suivantes:

- Estampille temporelle fournie par une source de confiance;
- Moment où le signataire a affirmé avoir effectué le processus de signature;
- Moment indiqué par le vérificateur.

Le processus de vérification recommandé pour chaque signature ou contreseing figurant dans les preuves numériques signées comprend les étapes suivantes:

1. Extraire de la signature le certificat du signataire et vérifier qu'il s'applique à la signature. Vérifier l'intégrité du contenu signé.

2. Définir la référence temporelle de la vérification de la signature selon la politique de validation des signatures retenue.

3. Si la référence temporelle de la vérification de la signature est fournie par une estampille temporelle, la signature de cette dernière doit être vérifiée.

4. Vérifier l'intégrité de tous les certificats utilisés dans la signature à l'aide des certificats présents dans la signature ou de tout autre moyen à la disposition du vérificateur.

5. Vérifier que tous les certificats utilisés pour la signature sont valables par rapport à la référence temporelle de la vérification de la signature définie dans l'étape 2.

6. Vérifier si les informations de révocation sont valables par rapport à la référence temporelle de la vérification de la signature définie dans l'étape 2, pour chaque certificat utilisé dans l'étape 4, à l'aide des informations figurant éventuellement dans la signature et à condition qu'elles soient appropriées.

7. Rendre compte au vérificateur du résultat du processus de vérification, y compris la référence temporelle de la signature utilisée (définie dans l'étape 2) et le certificat du signataire et, lorsqu'elles sont présentes, les informations suivantes:

- Date et heure de la signature;
- Lieu où se trouve le signataire;
- Rôle(s) indiqué(s) lié(s) au signataire;
- Politique de signature ou référence y afférente;
- Type d'engagement.

Les informations en matière de révocation DEVRAIENT prendre en compte un délai de grâce, à savoir le temps nécessaire pour rendre publiques les informations en question.

Au cours du processus de vérification de la signature, les prescriptions P3 à P18 DOIVENT également être remplies le cas échéant.

Si une prescription supplémentaire relative au processus de vérification est présente dans la politique de signature ou dans la politique du prestataire de services de certification, elle DEVRAIT être prise en compte.

Le résultat[15] du processus de vérification de la signature est le suivant:

- SUCCÈS lorsque toutes les étapes de la vérification se sont déroulées correctement;
- ÉCHEC lorsqu'une ou plusieurs des étapes de vérification se sont soldées par un échec;
- INCOMPLET lorsque certaines informations exigées pour le processus de vérification ne sont pas disponibles.

Lorsque le processus de vérification de la signature se solde par un échec ou ne peut pas s'achever, la ou les causes de l'échec DOIVENT être clairement signalées au vérificateur. Le processus DEVRAIT tenter d'achever la vérification même en cas d'erreur et DEVRAIT fournir un rapport complet sur le problème détecté.

A.7 Compatibilité en amont

Toute modification des caractéristiques doit garantir une compatibilité en amont. Il est exclu de concevoir des modifications qui rendraient incompatibles, illégales ou non interopérables les preuves numériques signées créées conformément aux versions précédentes.

A.8 Évolution possible des caractéristiques conformes à la Recommandation

Les caractéristiques des preuves numériques signées pourront être améliorées grâce aux nombreux progrès réalisés dans ce domaine.

Il serait alors possible d'incorporer les données nécessaires pour une vérification à long terme des preuves numériques signées (système AdES-A (réf. 15) (niveau 2) ou mécanismes de vérification de la validité des certificats des signataires comme le système TSL (liste du statut des services de confiance)[16] (niveau 2)).

Les versions futures de la Recommandation devraient aussi pouvoir prendre en compte les propriétés du certificat lui-même (certificats qualifiés, SSCD (dispositif sécurisé de création de signature), etc.).

De même, une future amélioration de la Recommandation pourrait faciliter l'élaboration des systèmes ci-après:

- Signature attachée (signature détachée et regroupement de multiples contenus signés)[17];
- Cinématique des signatures.

Annexe B (non normative): Lignes directrices pour la mise en œuvre technique de la Recommandation relative à l'interopérabilité des preuves numériques signées

Les caractéristiques décrites dans la Recommandation doivent être utilisées conjointement avec une mise en œuvre technique pour l'application des règles et des caractéristiques.

B.1 Vue d'ensemble des modèles de mise en œuvre

Trois normes de signature numérique ont déjà été étudiées et évaluées avec succès pour la mise en œuvre de la Recommandation:

- La norme XAdES fondée sur la spécification ETSI TS 101 903 v1.4.1. Le format des preuves numériques signées est désigné par le terme X-SDEIR dans le reste du document. La mise en œuvre sera décrite dans une future mise à jour de cette annexe technique;
- La norme CAdES fondée sur la spécification ETSI TS 101 733 v1.8.1. Le format des preuves numériques signées est désigné par le terme C-SDEIR dans le reste du document. La mise en œuvre est décrite dans la section B.4: Description du format C-SDEIR;
- La norme PAdES fondée sur la spécification ETSI TS 102 778 v1.1.1. Le format des preuves numériques signées est désigné par le terme P-SDEIR dans le reste du document. La mise en œuvre est décrite dans la section B.5: Description du format P-SDEIR.

Les normes relatives aux signatures numériques susmentionnées ont été étudiées pour la mise en œuvre technique de la Recommandation pour les raisons suivantes:

- Elles sont conformes à la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[18];
- Elles sont référencées en tant que normes ETSI;
- Un comité technique de l'ISO (ISO/TC 154[19]) œuvre actuellement à la normalisation de ces formats dans le cadre de l'ISO:
    - Format XAdES: ISO/CD 14533-2[20];
    - Format CAdES: ISO/CD 14533-1[21];
    - Format PAdES: ISO 32000-2[22].

B.2 Comparaison des exemples de mise en œuvre

L'existence de plusieurs mises en œuvre techniques offre aux développeurs d'applications la possibilité de choisir le format de preuves numériques signées le plus adapté à leurs besoins.

Le format X-SDEIR est particulièrement adapté au contenu XML (stocké en clair) et à la nécessité d'intégrer des signatures numériques dans des applications commerciales. Il est compatible avec le format de signature XAdES mentionné dans le Référentiel général d'interopérabilité de l'administration française[23].

Le format C-SDEIR convient bien pour le contenu binaire des signatures (stocké sans transformation). La capacité de détacher aisément le contenu signé des signatures offre

une certaine souplesse en matière de stockage et de vérification des preuves numériques signées.

Le format P-SDEIR est très approprié aux applications qui mettent l'accent sur le contenu du document du point de vue de la vérification de la signature, mais il est réservé au contenu signé de type PDF.

B.3 Description du format X-SDEIR

Cette description sera donnée dans une future version de la présente annexe technique.

B.4 Description du format C-SDEIR

Les différentes formes de signature CAdES DOIVENT présenter les caractéristiques ci-après pour être conformes à la Recommandation:

- CAdES-BES: cette caractéristique DOIT être présente ainsi qu'une référence au certificat du signataire pour être conforme au niveau de base de la Recommandation. Par ailleurs, pour être conforme au niveau 1 de la Recommandation, la signature DOIT comporter une référence à la chaîne de certification complète du signataire, et les preuves numériques signées DOIVENT contenir tous les certificats mentionnés;
- CAdES-EPES: si une politique de signature doit être utilisée, le format de la signature DEVRAIT être conforme au format CAdES-EPES et DEVRAIT être fourni conjointement avec l'identificateur OID, l'adresse URI, l'empreinte et l'algorithme de la politique à laquelle l'URI fait référence;
- CAdES-T: il convient d'utiliser ce format si une signature doit comporter une estampille temporelle.

Pour être conforme au niveau de base de la Recommandation, les données signées (SignedData) contenues dans les preuves numériques de type C-SDEIR DOIVENT satisfaire à toutes les conditions suivantes:

- Le champ «encapContentInfo» DOIT comporter le contenu signé dans le champ «eContent»;
- Le champ «certificates» DOIT contenir le certificat de chaque signature du signataire;
- Le champ «clrs» NE DOIT PAS contenir de liste de certificats révoqués (CRL);
- Le champ «signerInfos» DOIT contenir la signature et, si elles sont présentes, les cosignatures;
- Le champ «signedAttrs» de chaque champ «SignerInfo» DOIT satisfaire aux exigences suivantes:
    - Un attribut «contentType» DOIT être présent et DOIT contenir l'identificateur d'objet «id-signedData» (1.2.840.113549.1.7.2);
    - Un attribut «messageDigest» DOIT être présent;
    - Un attribut «signing-certificate-v2» DOIT être présent et DOIT faire référence au certificat du signataire;
    - Un attribut «content-hints» DOIT être présent. Le champ «contentType» DOIT contenir l'identificateur d'objet «id-data» (1.2.840.113549.1.7.1) et le champ «contentDescription» DOIT satisfaire aux exigences suivantes:

- Une information sur le type de contenu DOIT être présente et DOIT contenir le type MIME du contenu signé (par exemple, «Content-Type: text/plain»);
- Une description de contenu est FACULTATIVE. Si elle est présente, elle DOIT contenir le nom de fichier du contenu signé (par exemple «Content-Description: JCFV201.txt»).

- Un attribut «signing-time» PEUT être présent pour contenir le moment auquel le signataire affirme avoir effectué le processus de signature;
- Un attribut «signer-location» PEUT être présent pour contenir une mnémonique concernant une adresse liée au signataire en un lieu géographique donné;
- Un attribut «signature-policy-identifier» PEUT être présent pour contenir la politique de signature. S'il est présent, il peut contenir le champ «signaturePolicyImplied» (pour une politique implicite) ou «signaturePolicyId» (pour une politique explicite). Si le champ «signaturePolicyId» est présent, le champ «sigPolicyQualifiers» est FACULTATIF, mais s'il est présent, il DOIT contenir un qualificateur «spuri» pour spécifier l'URL lorsqu'une copie de la politique de signature PEUT être obtenue;
- Un attribut «signer-attributes» PEUT être présent. S'il est présent, il DOIT contenir le champ «claimedAttributes» qui contient une suite de rôles indiqués par le signataire, mais non signés. Chaque rôle DOIT être codé en UTF8String;
- Un attribut «commitment-type-indication» PEUT être présent. S'il est présent, le champ «commitmentTypeidentifier» DOIT contenir l'une des valeurs suivantes:
  - id-cti-ets-proofOfOrigin OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1}
  - id-cti-ets-proofOfReceipt OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 2}
  - id-cti-ets-proofOfDelivery OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3}
  - id-cti-ets-proofOfSender OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 4}
  - id-cti-ets-proofOfApproval OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5}
  - id-cti-ets-proofOfCreation OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6}
- D'autres attributs NE DOIVENT PAS être présents.

- Le champ «unsignedAttrs» de chaque élément «SignerInfo» DOIT satisfaire aux exigences suivantes:
  - Un attribut «counter-signature» PEUT être présent. S'il est présent, il DOIT contenir un ou plusieurs contreseings de la signature correspondante;

- Un attribut «signature-timestamp» PEUT être présent. S'il est présent, il DOIT contenir un jeton d'horodatage;
- D'autres attributs PEUVENT être présents.

Outre les caractéristiques d'une signature C-SDEIR de niveau de base, une signature C-SDEIR de niveau 1 DOIT aussi respecter les spécifications ci-après:

- Le champ «certificates» DOIT contenir tous les certificats du chemin de certification du signataire pour chaque signature;
- Pour chaque élément «SignerInfo»:
  - L'attribut signé «signing-time» DOIT être présent;
  - L'attribut signé «signing-certificate-v2» DOIT faire référence à tous les certificats du chemin de certification du signataire.

Aucune syntaxe particulière n'étant précisée dans la spécification, toute application capable de vérifier une signature CAdES peut valider les preuves numériques C-SDEIR.

B.5 Description du format P-SDEIR

B.5.1 Généralités

Un document PDF peut intégrer de multiples signatures numériques et offrir toutes les qualités nécessaires des preuves numériques conformes à la Recommandation. La présente section décrit les caractéristiques des signatures numériques PDF nécessaires pour répondre aux prescriptions de base et de niveau 1 de la Recommandation.

Le profil de signature PDF conforme à la Recommandation est le profil de signature de base PAdES défini dans la spécification ETSI TS 102 7786-2[24] et il est équivalent au format de signature PDF défini dans la norme ISO/DIS 32000-1.

Il convient de noter que cette mise en œuvre ne prend pas en charge:

- Les contreseings (prescription P4 de la Recommandation);
- La politique de signature (prescription P14 de la Recommandation);
- Les rôles indiqués (prescription P15 de la Recommandation).

Notes concernant la mise en œuvre:

- Si le document doit être imprimé, des données supplémentaires devraient être imprimées sur le document pour que le lecteur puisse vérifier l'authenticité et l'intégrité du document;
- Concernant les signatures visibles, des travaux sont actuellement menés par l'Institut européen des normes de télécommunication (ETSI) et l'Organisation for the Advancement of Structured Information Standards (OASIS), mais cet aspect ne relève pas actuellement du champ d'application de la Recommandation.

B.5.2 Spécifications concernant le format de signature de base PAdES (P-SDEIR)

Le format de signature P-SDEIR correspond à deux types différents de signatures invisibles PDF définis au paragraphe 8.7 de la référence ISO 32000-1:

- Une signature conforme à la Recommandation sans type d'engagement ou assortie d'un type d'engagement différent du type «preuve de création» DOIT être mise en œuvre en tant que «signature de document (ou ordinaire)»;

- Une signature conforme à la Recommandation présentant un type d'engagement «preuve de création» DOIT être mise en œuvre en tant que «signature MDP (détection et prévention des modifications), également appelée signature de l'auteur ou signature de certification». La signature MDP est de type 2.

Aucune syntaxe particulière n'étant précisée, toute application capable de vérifier une signature de base PAdES peut vérifier des preuves numériques signées de niveau de base P-SDEIR.

B.5.2.1 Spécifications concernant le niveau de base du format P-SDEIR

Les caractéristiques d'une signature de niveau de base P-SDEIR sont les suivantes (conformément à la référence ISO 32000-1):

1. La signature est codée selon la syntaxe de message cryptographique (CMS) telle que définie par le format PKCS#7 (voir la RFC 2315[25]);

2. Le «sous-filtre» utilisé est «adbe.pkcs7.detached»;

3. La signature PEUT contenir une estampille temporelle telle que définie dans la RFC 3161[26];

4. La signature NE DOIT PAS contenir de réponse OCSP[27] ou de CRL[28] en tant qu'attribut signé;

5. La signature DOIT contenir le certificat du signataire;

6. La signature DOIT être apposée sur le certificat de signature, de l'une des manières suivantes:

   - Ajout d'un attribut signé (non défini dans la référence ISO 32000-1) contenant le certificat de signature ESS V2. Cet attribut DOIT contenir une référence au certificat du signataire;

   - Ajout manuel de l'empreinte digitale du certificat de signature dans le document lui-même.

1. La signature PEUT contenir la date de signature, le lieu de signature et un motif;

2. Le motif DOIT correspondre à la valeur du type d'engagement utilisé pour certifier les preuves numériques signées sous la forme [CommitmentType=<CommitmentTypeIdentifier>] <Libellé>, ce dernier élément étant une chaîne décrivant le type d'engagement dans la langue du signataire et lorsque l'élément «CommitmentTypeIdentifier» peut prendre les valeurs ci-après: «proof_of_origin», «proof_of_receipt», «proof_of_delivery», «proof_of_approval», «proof_of_sender». Exemple: «[CommitmentType=proof_of_receipt] Preuve de réception».

B.5.2.2 Spécifications concernant le niveau 1 du format P-SDEIR

Une signature P-SDEIR de niveau 1 DOIT en outre être conforme aux spécifications suivantes:

- La prescription 5 de la section 0 s'applique à tous les certificats du chemin de certification du signataire;

- La prescription 6 de la section 0 s'applique à tous les certificats du chemin de certification du signataire.

Annexe C (normative): Algorithmes cryptographiques

Comme la puissance des algorithmes cryptographiques évolue dans le temps, il est important que les personnes qui mettent en œuvre des applications conformes à la Recommandation prennent en compte cette évolution.

On trouvera dans la présente annexe des conseils pour la mise en place et l'actualisation des algorithmes de création et de vérification de signatures.

Pour la création de signatures, les applications conformes à la Recommandation DEVRAIENT au moins prendre en charge les algorithmes ci-après:

- Algorithmes de hachage: SHA-256;
- Algorithmes de signature: RSA 2048.

Pour la vérification des signatures, les applications conformes à la Recommandation DOIVENT au moins prendre en charge les algorithmes ci-après:

- Algorithmes de hachage: SHA-256;
- Algorithmes de signature: RSA 2048.

Pour la vérification des signatures, les applications conformes à la Recommandation DEVRAIENT au moins prendre en charge les algorithmes ci-après:

- Algorithmes de hachage: SHA-1;
- Algorithmes de signature: RSA 1024.

Si une mise en œuvre particulière de la Recommandation au moyen d'algorithmes spéciaux (à savoir des courbes elliptiques) est exigée, il est recommandé de se référer à la spécification ETSI TS 102 176[29].

Références

[1] Loi type sur le commerce électronique adoptée par la Commission des Nations Unies pour le droit commercial international: http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf.

[2] Loi type de la Commission des Nations Unies pour le droit commercial international sur les signatures électroniques: http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf.

[3] Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques: http://www.uncitral.org/pdf/french/texts/electcom/08-55699_Ebook.pdf.

[4] PKCS#7: http://www.rsa.com/rsalabs/node.asp?id=2129.

[5] S/MIME: http://www.ietf.org/rfc/rfc3851.txt.

[6] CMS: http://www.ietf.org/rfc/rfc3852.txt.

[7] XMLDSIG: http://www.w3.org/TR/xmldsig-core/.

[8] CAdES (ETSI TS 101 733): http://www.etsi.org.

[9] Signature numérique EANCOM: http://www.gs1.org/docs/ecom/eancom/eancom_Digital_Signature.pdf.

[10] Signature des documents PDF (ISO/DIS 32000): http://www.adobe.com/devnet/pdf/pdf_reference.html ou http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502.

[11] XAdES (ETSI TS 101 903): http://www.etsi.org.

[12] PAdES (ETSI TS 102 778): http://www.etsi.org.

[13] Mots clefs: http://www.faqs.org/rfcs/rfc2119.html.

[14] Directive 2001/115/CE du Conseil: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:32001L0115:FR:HTML (7)-2-c).

[15] Document CWA 14171 concernant la vérification des signatures électroniques: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf.

[16] Liste concernant le statut des prestataires de services de confiance (ETSI TS 102 231): http://www.etsi.org.

[17] Travaux de l'ETSI concernant les signatures attachées (en cours): http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=31946.

[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FR:HTML.

[19] ISO/TC 154: http://www.iso.org/iso/iso_technical_committee.html?commid=53186.

[20] ISO/CD 14533-2: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56025.

[21] ISO/CD 14533-1: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56024.

[22] ISO 32000-2 http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=37&ics2=100&ics3=99&csnumber=53041.

[23] Format de signature numérique XAdES de l'administration française: http://www.references.modernisation.gouv.fr/sites/default/files/FormatdeSignature_Xades_V1_0.pdf.

[24] PAdES Basic (ETSI TS 102 778-2): http://www.etsi.org.

[25] RFC 2315: http://www.ietf.org/rfc/rfc2315.txt.

[26] Horodatage: RFC 3161: http://www.ietf.org/rfc/rfc3161.txt & X9.95: http://www.x9.org/news/pr050701.

[27] Protocole de vérification en ligne de certificats: http://www.ietf.org/rfc/rfc2560.txt.

[28] Liste des certificats révoqués: http://www.ietf.org/rfc/rfc5280.txt.

[29] Algorithmes et paramètres relatifs aux signatures électroniques sécurisées (ETSI TS 102 176): http://www.etsi.org.