



Conseil économique et social

Distr. générale
5 décembre 2011
Français
Original: anglais

Commission économique pour l'Europe

Comité du commerce

Centre pour la facilitation du commerce et les transactions électroniques

Dix-huitième session

Genève, 15-17 février 2012

Point 5 de l'ordre du jour provisoire

Recommandations et normes du CEFACT-ONU

Recommandation n° 37: interopérabilité des documents numériques signés

**Établie par l'équipe de projet sur la sécurité des documents et messages
XML relevant du volet du programme à élaborer consacré à la chaîne
d'approvisionnement et soumise par le Bureau pour information**

Résumé

Le projet initial de Recommandation n° 37 de la CEE sur l'interopérabilité des preuves numériques signées a été soumis au CEFACT-ONU à sa seizième session et, ultérieurement, comme suite à la décision 10-04, soumis pour approbation durant l'intersession. Les observations reçues durant l'intersession ont été examinées à la dix-septième session. Il a été décidé de revenir à l'étape 4, «Examen public» du processus d'élaboration ouvert, jusqu'au 12 septembre 2011.

Les participants au volet du programme à élaborer consacré à la chaîne d'approvisionnement soumettent à présent une version actualisée de ce projet de recommandation pour information.

Le Bureau a également établi une note explicative (ECE/TRADE/C/CEFACT/2012/8) qui devrait servir de document de travail pour les délibérations de la Plénière à ce sujet.

Documentation antérieure:

Recommandation n° 37: interopérabilité des preuves numériques signées (ECE/TRADE/C/CEFACT/2010/14).

Table des matières

	<i>Page</i>
1. Avant-propos.....	3
2. Résumé.....	4
2.1 Contexte.....	4
2.2 Recommandation	5
2.3 Avantages et objectifs.....	5
3. Introduction.....	6
3.1 Champ d'application.....	6
3.2 Objectif.....	6
3.3 Public.....	7
4. Définitions	8
5. Recommandation	9
5.1 Caractéristiques des documents numériques signés visées par la Recommandation	9
5.2 Prescriptions fonctionnelles relatives aux caractéristiques	9
5.3 Différences entre documents numériques signés et documents sur support papier signés	10
6. Conclusion	11
7. Références.....	11

1. Avant-propos

La Recommandation relative à l'interopérabilité des documents numériques signés a pour objet de renforcer le niveau d'interopérabilité des documents numériques signés par voie électronique, qui serait l'un des moyens, dans certaines situations, de faciliter le développement du commerce international dématérialisé, c'est-à-dire sans papier.

À cet effet, elle définit un ensemble de règles fonctionnelles ayant trait aux documents numériques signés en ce qui concerne l'organisation et les liens entre le contenu signé, les identités numériques et les signatures des signataires présumés.

La présente Recommandation est destinée à être appliquée par des organisations ou des personnes qui ont décidé d'utiliser des documents numériques signés.

Les questions juridiques visées par la présente Recommandation devraient faire l'objet d'une coordination avec d'autres organisations internationales.

La présente Recommandation ne porte pas sur les aspects juridiques des signatures électroniques, qui sont traités au niveau international dans d'autres documents tels que ceux publiés par la Commission des Nations Unies pour le droit commercial international (CNUDCI), ni sur la possibilité d'utilisation ou l'interprétation du contenu signé.

Elle a été conçue de manière à ne pas être incompatible avec la Recommandation n° 14 de la CEE intitulée «Authentification des documents commerciaux par des moyens autres que la signature».

2. Résumé

2.1 Contexte

En raison de la multiplicité des normes relatives aux signatures électroniques, il peut être, sur le plan technique ou juridique, difficile pour le destinataire de documents numériques signés de les vérifier, ce qui risque dans certains cas d'avoir 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.

Dans certaines situations, l'application des normes recommandées poserait aussi des problèmes de respect des obligations et entraînerait une augmentation des coûts, ainsi que, parfois, la nécessité d'adopter des réglementations ou d'autres mécanismes juridiques, et ces éléments doivent être pris en compte lorsqu'on examine l'ensemble des avantages que l'on prévoit d'en retirer.

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

La vérification des documents numériques signés ne devrait exiger des parties aucun accord de procédure préalable afin que le vérificateur ait une vision claire des quelques éléments d'information ci-après:

- Paramètres des signatures (date, lieu, type d'engagement);
- Intégrité du contenu signé, lorsque cela est expressément prévu;
- Intégrité et validité des identités numériques des signataires présumés et niveau de garantie qu'elles sont censées fournir, en vertu des déclarations de pratiques adoptées par les services de certification présumés, des accords entre les utilisateurs et des prescriptions réglementaires applicables;
- Crédibilité des prestataires de services de certification présumés.

La présente Recommandation contient un ensemble de prescriptions fonctionnelles relatives à la création et à la vérification des documents numériques signés, le but étant d'améliorer leur interopérabilité. Il convient de noter qu'une fois adoptée, la Recommandation pourrait faire, le temps passant, l'objet de demandes de modifications.

Outre les questions particulières soulevées ici, la Recommandation porte sur l'interopérabilité fonctionnelle et n'a pas été analysée dans une perspective juridique générale ou par rapport à des lois nationales particulières; le respect de ces normes ne donne aucune garantie de la recevabilité ou du caractère exécutoire d'un document numérique signé, quelle que soit la juridiction concernée.

Dans la perspective des administrations publiques, des parlements, des magistrats, des entités chargées de la mise en œuvre, des utilisateurs, et d'autres intéressés, la Recommandation ne vise pas à résoudre la question de savoir si son application sera légalement reconnue en vertu du droit interne de l'un ou l'autre pays ou dans le cadre de transactions transfrontalières. L'utilisation des méthodes élaborées dans la présente Recommandation n'a pas nécessairement une plus grande incidence en tant qu'élément de preuve dans une procédure judiciaire que d'autres méthodes reconnues pour fournir ou authentifier de telles informations en tant que preuves.

2.2 Recommandation

La présente Recommandation encourage toute organisation ou partie qui choisit d'échanger des documents numériques signés avec d'autres à observer les principes ci-après afin d'en maximiser l'interopérabilité:

Les documents numériques signés:

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

Chaque signature figurant dans le document numérique:

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

Les mots clefs «DEVOIR» et «POUVOIR» utilisés dans la présente section doivent être interprétés comme suit:

- DEVOIR: signifie que la prescription est une exigence absolue de la spécification;
- POUVOIR: signifie que la prescription est facultative. Une application qui *n'inclut pas* une option particulière doit être susceptible d'interagir avec une autre application qui *l'inclut*, bien qu'éventuellement avec des fonctionnalités réduites.

De même, une application qui *inclut* une option particulière doit être susceptible d'interagir avec une autre application qui *ne l'inclut pas* (sauf, bien sûr, pour la fonction que cette option propose).

2.3 Avantages et objectifs

La Recommandation propose aux entreprises, aux administrations et aux organismes financiers un ensemble de prescriptions fonctionnelles normalisées visant à améliorer l'interopérabilité lors de la création et de la vérification des documents numériques signés, dès lors que des normes et des solutions technologiques conformes sont adoptées et appliquées en tenant compte des coûts liés aux réglementations, à la mise en place des infrastructures et au fonctionnement pour les utilisateurs.

Ces avantages peuvent être obtenus avec des technologies et des produits largement disponibles actuellement, y compris les projets sources ouverts.

Les objectifs de la Recommandation sont les suivants:

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

3. Introduction

3.1 Champ d'application

Depuis le début des années 90, de nombreuses normes techniques ont été conçues, proposées et adoptées dans le domaine des documents numériques signés. On en trouvera des exemples à la Section 7 – Références.

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 numériques, n'a pas permis d'assurer l'interopérabilité des documents numériques signés au niveau de la syntaxe, de la sémantique et du traitement.

L'objet de la présente Recommandation est de proposer une approche particulière en ce qui concerne la création et la vérification de documents numériques signés, une attention particulière étant prêtée aux aspects fonctionnels plutôt qu'aux aspects techniques.

En étant axée sur les aspects fonctionnels, dans les secteurs pour lesquels elle est considérée comme une solution appropriée, et lorsque cela est jugé acceptable par les parties associées, la présente Recommandation permet de définir un profil fonctionnel commun de document numérique signé. Ce profil d'application sectoriel de la Recommandation, sous réserve d'autres facteurs tels que les coûts, le cadre réglementaire, les pratiques sectorielles, etc., peut simplifier et faciliter la création et la vérification de documents numériques signés.

La présente Recommandation n'affecte pas la capacité des parties de choisir d'autres méthodes que les systèmes ou les parties peuvent adopter pour atteindre des objectifs comparables.

La présente Recommandation offre un ensemble de prescriptions fonctionnelles visant à promouvoir l'interopérabilité lors de la création et de la vérification de documents numériques signés dans la mesure applicable à des secteurs particuliers et convenue par les parties concernées.

3.2 Objectif

La présente Recommandation a pour objet de faciliter l'échange et la vérification des documents numériques signés susceptibles d'avoir une valeur non négligeable pour les entreprises en assurant ou favorisant leur interopérabilité, dans la mesure applicable à des secteurs particuliers et convenue par les parties concernées. Son application devrait augmenter le taux de dématérialisation des documents, en facilitant la création, la validation et l'interopérabilité des documents numériques signés.

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

- Détermination de la partie du contenu visé par la signature numérique;
- Signature du ou des document(s) approprié(s) ou parties de document(s);
- Vérification de la ou des signature(s) du document, y compris la détection de ses ou de leurs paramètres.

En matière d'appels d'offres et de facturation par voie électronique, certaines pratiques régionales montrent qu'il faut résoudre plusieurs problèmes d'interopérabilité lorsqu'une partie signe un document avec son logiciel d'identification 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 encore 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 de l'identité numérique: le logiciel de vérification peut ne pas être capable de déterminer si l'identité numérique est fiable ou si elle était valable à la date et l'heure de la signature.

L'échec de la vérification de la signature est d'une grande importance, 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 ou des procédures de vérification pourraient être appliquées et avoir une incidence sur les délais tout en réduisant le montant des économies qu'il est prévu de réaliser grâce à l'utilisation des signatures numériques.

Pour remédier aux deux premières catégories de problèmes, il peut être nécessaire de présenter toutes les signatures produites dans un format que tous les logiciels de vérification utilisés seront capables de gérer.

En conséquence, les principaux avantages des caractéristiques proposées pour les documents numériques signés sont les suivants:

- Instaurer la confiance en offrant des fonctions générales permettant de créer, de vérifier et de gérer aisément les documents numériques signés;
- Favoriser l'interopérabilité des documents numériques signés 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».

3.3 Public

Le présent document est principalement destiné aux organisations, aux parties et aux systèmes visant à:

- Échanger des documents numériques signés;
- Choisir un format de documents numériques signés approprié à un projet de dématérialisation particulier;
- Suivre les technologies de l'information dans les domaines des signatures et de l'archivage numériques;
- Assurer l'interopérabilité des documents numériques signés.

4. Définitions

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

AdES: Advanced Electronic Signature (signature électronique avancée)

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

Document numérique signé: document ou toute autre information numérique pouvant être utilisé pour démontrer la fiabilité ou la non-corruption de l'information signée, ou bien accord entre parties ou utilisation par un système de procédures pour ce faire. Il ne permet pas d'identifier une partie ayant effectivement pris des mesures sans appliquer de procédures et de technologie supplémentaires

CMS: Cryptographic Message Syntax (syntaxe de message cryptographique)

Cosignature: signature qui s'applique au même contenu qu'une autre signature, ou moyen comparable d'identifier une partie associée conformément aux pratiques applicables dans le secteur

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, ou moyen comparable d'identifier une partie associée conformément aux pratiques applicables dans le secteur

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»

Message de données: information créée, transmise, reçue ou conservée par des moyens électroniques, magnétiques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégramme, le télex ou la télécopie (Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, art. 4. Définitions)

Document numérique: document sous forme numérique utilisé pour transmettre des informations afin que son utilisateur puisse en prendre connaissance ou les traiter

CCE ou Convention de l'ONU sur le commerce électronique: Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005); *Documents officiels de l'Assemblée générale, soixantième session, A/RES/60/21* (aussi appelée Convention de l'ONU sur le commerce électronique ou CCE)

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 (référence 1)

ETSI: Institut européen des normes de télécommunication

UE: Union européenne

Information: inclut tous les types de fichiers [faut-il une définition de «fichiers»?] et contenus numériques, notamment, mais non exclusivement, des «documents ainsi que tout type de message de données»

IETF: Internet Engineering Task Force (Groupe d'étude sur l'ingénierie Internet)

ISO: Organisation internationale de normalisation

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)

RFC: Request For Comment (demande de commentaires)

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

Contenu signé: données contenues dans le document numérique signé qui est signé par le ou les signataires présumé(s)

TS: spécification technique

CNUDCI: Commission des Nations Unies pour le droit commercial international

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

XML: langage de balisage extensible

XMLDSIG: XML Digital Signature (signature numérique XML)

5. Recommandation

La présente section décrit la Recommandation.

5.1 Caractéristiques des documents numériques signés visées par la Recommandation

La Recommandation définit les caractéristiques des documents numériques signés visant à maximiser l'interopérabilité entre la création et la vérification des documents numériques signés.

Les caractéristiques sont décrites comme étant un ensemble de prescriptions fonctionnelles.

5.2 Prescriptions fonctionnelles relatives aux caractéristiques

Le présent paragraphe décrit les prescriptions fonctionnelles relatives aux caractéristiques proposées des documents numériques signés.

Les mots clefs «DEVOIR» et «POUVOIR» utilisés dans la présente section doivent être interprétés comme suit:

- DEVOIR: signifie que la prescription est une exigence absolue de la spécification;
- POUVOIR: signifie que la prescription est réellement facultative. Une application qui n'inclut pas une option particulière DOIT être susceptible d'interagir avec une autre application qui l'inclut, bien qu'éventuellement avec des fonctionnalités réduites. Dans le même ordre d'idées, une application qui inclut une option particulière DOIT être susceptible d'interagir avec une autre application qui ne l'inclut pas (sauf, bien sûr, pour la fonction que cette option propose).

Un document numérique signé conforme aux caractéristiques proposées des documents numériques signés:

- DOIT contenir un et un seul contenu identifiable ainsi que le type de contenu et un nom facultatif;
- DOIT comporter une ou plusieurs signatures;
- DOIT contenir sans ambiguïté toutes les identités numériques concernées.

Chaque signature figurant dans le document numérique signé conforme aux caractéristiques proposées des documents numériques signés:

- DOIT viser la totalité du contenu;
- PEUT comporter des attributs, qui doivent être visés par la signature, tels que:
 - La date de signature: indique le moment où le signataire présumé affirme avoir effectué le processus de signature;
 - Lieu où se trouve le signataire: indique une mnémonique relative à une adresse liée au signataire présumé 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 présumé entend assumer pour le document signé;
 - Type d'engagement lié à la signature: indique explicitement à un vérificateur le type spécifique d'engagement pris par le signataire présumé à la signature du document;
 - Rôle(s) du signataire présumé: indique le ou les rôles ou la ou les positions déclarés par le signataire présumé à la signature du document;
 - Références à l'identité numérique du signataire présumé et à ses certificateurs présumés;
- PEUT être assortie d'un ou de plusieurs contreseings;
- PEUT contenir une estampille temporelle.

5.3 Différences entre documents numériques signés et documents sur support papier signés

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

- L'identité des signataires présumés ne figure pas toujours sur les documents sur support papier;
- L'identité des certificateurs présumés du signataire présumé ne figure généralement pas sur les documents sur support papier;
- En revanche, les documents sur support papier signés comportent souvent une signature manuscrite, bien que des signatures apposées au moyen d'un timbre ou d'une pièce jointe soient aussi fréquemment utilisées dans le commerce, tandis qu'une signature numérique figurant sur un document électronique numérique n'est pas censée être représentée graphiquement, à moins que d'autres technologies telles que la dynamique de signature soient également employées. En règle générale, seul un programme informatique peut effectuer les calculs mathématiques complexes indispensables pour vérifier une signature numérique.

6. Conclusion

Les caractéristiques des documents numériques signés exposées dans le présent document ont pour objet, dans la mesure déterminée par les organisations, les systèmes ou les parties, de: a) généraliser la dématérialisation des documents sur support papier en simplifiant (tout en tenant compte des dispositifs réglementaires et infrastructurels et des coûts correspondants) et en facilitant la création et la vérification de documents numériques signés; et b) contribuer à leur intégration dans des applications commerciales dans des contextes ou des situations où cela est nécessaire ou convenu entre les parties.

7. Références

PKCS#7: <http://www.rsa.com/rsalabs/node.asp?id=2129>

S/MIME: <http://www.ietf.org/rfc/rfc3851.txt>

CMS: <http://www.ietf.org/rfc/rfc3852.txt>

XMLDSIG: <http://www.w3.org/TR/xmlsig-core/>

CAdES (ETSI TS 101 733): <http://www.etsi.org>

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

PDF signé (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

XAdES (ETSI TS 101 903): <http://www.etsi.org>

PAdES (ETSI TS 102 778): <http://www.etsi.org>
