COMITE OUEST AFRICAIN D'ORGANISATION ET DE NORMALISATION BANCAIRE ET FINANCIERE

**Conseil Exécutif**
---
**Secrétariat Exécutif**
---

## NEWSLETTER N°2 : LA SIGNATURE ELECTRONIQUE

Une signature est une marque permettant d'identifier l'auteur d'un document, d'une œuvre : ainsi un auteur signe ses écrits. Une signature peut aussi être apposée sur un document pour signifier son approbation par le signataire. Il en est ainsi des contrats ou de tout document commercial.

La signature peut être manuscrite, le signataire appose un graphisme par lequel il s'identifie. Elle est dite numérique quand elle est faite directement par une application comme Adobe Reader, et numérisée quand elle est faite sur un papier puis scannée et ajoutée à un document.

Avec le développement de l'économie numérique, on parle de plus en plus de signature électronique. La signature électronique est elle la transposition dans le monde numérique de la signature manuscrite ?

Notre newsletter de ce trimestre est donc consacrée à la signature électronique. De la création d'une signature électronique à son rôle en passant par l'horodatage, le certificat électronique, ce sont autant de termes que nous aborderons dans cette newsletter.

### QU'EST CE QUE LA SIGNATURE ELECTRONIQUE ?

Selon la Commission des Nations Unies pour le Droit Commercial International : *« Une signature électronique est une valeur numérique apposée à un message de données et qui, grâce à une procédure mathématique bien connue associée à la clé cryptographique*[1] *publique de l'expéditeur, permet de déterminer que cette valeur numérique a été créée à partir de la clé cryptographique privée de l'expéditeur.*

*Les procédures mathématiques utilisées pour créer les signatures électroniques sont fondées sur le chiffrement de la clé publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du message de telle sorte qu'une personne disposant du message initial et de la clé publique de l'expéditeur peut déterminer avec exactitude :*

- *si la transformation a été opérée à l'aide de la clé privée correspondant à celle de l'expéditeur ;*
- *si le message initial a été altéré une fois sa transformation opérée».*

1 La cryptographie : ensemble des techniques permettant de protéger une communication au moyen d'un code secret (chiffrement). Elle peut être faite à partir des clés symétriques ou asymétriques. Dans ce dernier cas, il y aura une clé publique et une privée. La première est habituellement utilisée pour le chiffrement et la clé privée, pour le déchiffrement. Ainsi, tout utilisateur peut envoyer un message secret à l'aide de la clé publique du destinataire pour en chiffrer le contenu, tandis que le destinataire pourra déchiffrer ce message avec sa clé privée, étant seul à la connaître.

## POURQUOI UNE SIGNATURE ELECTRONIQUE ?

La signature électronique permet de parachever le processus de dématérialisation des documents en garantissant l'authentification de l'auteur du message, la confidentialité du message, son intégrité et sa non répudiation.

## COMMENT CREE-T-ON UNE SIGNATURE ELECTRONIQUE ?

Pour qu'une entreprise dispose d'une signature électronique, elle doit introduire auprès d'une société prestataire de services de certification électronique (PSCE) une demande de certificat électronique, document dématérialisé comportant des informations techniques et d'identification.

Le PSCE est chargé de créer, de délivrer et de gérer des certificats électroniques. Pour ce faire, il établit un lien entre l'utilisateur (le futur signataire) et le certificat qu'il va émettre pour lui, en s'assurant préalablement, par l'examen de pièces d'identité et le cas échéant, selon le niveau de sécurité, par une rencontre en face-à-face, de la véracité des informations fournies par le demandeur. Il signe ensuite le certificat (avec sa propre clé), garantissant ainsi l'intégrité et la véracité des informations contenues dans les certificats qu'il émet.

Des évaluations de la conformité des prestations proposées par les PSCE sont réalisées par un Organisme accrédité par une Autorité compétente à cet effet.

## L'HORODATAGE ELECTRONIQUE

L'horodatage électronique n'est pas pris en compte par tous les certificats électroniques, même s'il tend à s'imposer de plus en plus dans le monde de la signature numérique. Il consiste à apposer à un fichier une date fiable sous la forme d'un jeton d'horodatage (c'est l'équivalent du cachet dateur) garantissant ainsi l'existence d'un fichier de même que son intégrité à une date donnée.

## LA SIGNATURE ELECTRONIQUE DANS L'UEMOA

Le Règlement N°15/2002/CM/UEMOA du 19 septembre 2002 relatif aux systèmes de paiement dans les Etats membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA) a reconnu une valeur probante à l'écrit sous forme électronique en introduisant notamment la notion de signature électronique. Ce texte précise entre autres, les conditions de création, de conservation, de fiabilité et de sécurité d'une signature électronique ainsi que celles de qualification du dispositif de vérification y relatif et du certificat électronique.

L'Instruction n°141-04-07 du 30 avril 2007 de Monsieur le Gouverneur de la BCEAO, identifie la procédure d'accréditation des organismes d'évaluation et la procédure de qualification des prestataires de services de certification dans les systèmes de paiement de l'UEMOA.

Au regard de ces dispositions, des travaux ont été réalisés en vue de la mise en place d'une signature électronique sécurisée dans l'UEMOA sous l'égide de la Banque Centrale en 2011/2012. Trois (3) options avaient été identifiées :

**Option 1 : la BCEAO est désignée comme organisme d'accréditation,** donc création d'un nouveau métier au sein de la Banque Centrale qui exigerait la mise en place d'une structure indépendante pour des besoins d'impartialité. Cette option fut donc écartée par les Autorités de la BCEAO.

**Option 2 : l'accréditation est faite par le Système Ouest Africain d'Accréditation (SOAC),** instauré par la Commission de l'UEMOA et chargé d'accréditer les laboratoires, organismes de certification et d'inspection de la zone. Cette option favoriserait la création de compétences régionales dans le secteur. Toutefois, sa mise en œuvre requiert des financements.

**Option 3 : l'accréditation est faite par des organismes étrangers d'accréditation** : cette option immédiatement opérationnelle ne permet cependant pas de s'approprier les compétences de façon durable dans l'Union et pourrait conduire à la coexistence de différents systèmes qui, par leur hétérogénéité, ne sont pas facilement interopérables.

Aucune décision n'a été prise à ce jour, même s'il a été envisagé de combiner les options 2 et 3. A noter que le SOAC a lancé ses activités le 27 mars 2018 à Abidjan, pays de son siège.

## INITIATIVES NATIONALES

**Bénin :** c'est en 2017 que le pays a adopté une loi portant code du numérique au Bénin, qui régit le champ de la communication électronique, de la signature électronique et de la protection des données personnelles.

**Burkina Faso :** en 2009, une loi portant réglementation des services de transaction électroniques au Burkina Faso a été adoptée et l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) est devenue l'autorité d'accréditation en matière de certification électronique.

**Côte d'Ivoire :** la loi N°2013-546 du 30 juillet 2013 relative aux transactions électroniques et son décret d'application N°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique régissent le secteur de la signature et du certificat électroniques. Trois PSCE sont agréés par l'Autorité de Régulation des Télécommunications en Côte d'Ivoire : Cryptoneo, Document Knowledge Business Solutions et International Telecom Assistance.

**Mali :** en 2016, le pays s'est doté d'une loi portant sur les transactions, échanges et services électroniques. Ce texte prévoit un mécanisme de contrôle et de vérification en vue de s'assurer de l'identification des utilisateurs. Il prévoit également la création d'un cadre institutionnel chargé de promouvoir la gestion de la certification et de la signature électronique.

**Sénégal :** en 2008, le Sénégal a adopté une loi sur les transactions électroniques et la signature électronique. En 2014 le gouvernement a adopté le système de signature électronique et de chiffrement comme moyen privilégié d'authentification des personnes et de garantie de la confidentialité des échanges électroniques.

A cet effet, l'Agence De l'Informatique de l'Etat (ADIE) a initié, en rapport avec tous les acteurs concernés, le projet permettant de doter le Sénégal d'une Infrastructure nationale de Gestion des Clés (IGC), ouverte à l'ensemble des autorités et structures de l'État. L'objectif est la mise en œuvre des dispositifs nécessaires pour assurer la délivrance et la gestion des certificats électroniques au Sénégal, notamment en termes d'infrastructure, de réglementation et d'organisation. Deux PSCE, à savoir GAINDE 2000 et SenTrust exercent au Sénégal.

**Togo :** la loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques de même que son décret d'application ont été adoptés. L'objectif visé par ces textes est de permettre la reconnaissance juridique des certificats et signatures électroniques émanant de pays tiers, de réglementer les conditions d'exercice des prestataires de services de confiance et de régir les dispositions relatives à la signature et au certificat électronique.

En définitive, la mise en place de la signature électronique sécurisée dans la zone UEMOA est une nécessité dans une optique de mise en conformité des échanges électroniques avec les standards internationaux. Les textes réglementaires élaborés en 2002 et 2007 témoignent de la volonté des autorités communautaires à prendre en charge cette question. Toutefois les schémas prévus n'ont pu être expérimentés à ce jour, conduisant les Etats à s'engager dans des initiatives nationales. La multiplication des textes nationaux et les niveaux différents d'utilisation de la signature électronique par les Etats justifient pleinement que les travaux en vue d'une d'harmonisation des pratiques soient menées à défaut d'une solution communautaire.