JDN
Business
Banque - assurance

La signature électronique peut freiner efficacement l'usurpation d'identité

Chronique de Julien Stern
Universign

Mis à jour le 26/03/20 11:45

La signature électronique gagne du terrain à mesure que les entreprises se digitalisent. Néanmoins, nombreux sont ceux à se demander s'il n'existe pas un risque d'usurpation d'identité lors d'une signature électronique.

La valeur juridique de la signature électronique est reconnue en France mais sous certaines conditions. Pour la démontrer, il faut identifier de manière fiable le signataire et garantir l'intégrité du document signé. Il s'agit d'une opération à caractère légal. En France, l'article 1367 du Code civil définit la signature électronique comme une preuve aussi efficiente que la signature manuscrite. La signature électronique est donc admise en cour de justice dès lors que sa fiabilité est reconnue.

Différents niveaux de signature pour différents niveaux de protection

Le règlement eIDAS est à l'origine de trois niveaux de signature : simple, avancée et qualifiée. Ces trois niveaux de signature sont mis en œuvre grâce à différents moyens d'identification électronique permettant de mieux maîtriser les risques d'usurpation d'identité. Mais la signature électronique ne se limite pas à une question technique. Il s'agit bel et bien d'une opération à caractère légal qui ne doit pas se faire au détriment de l'expérience utilisateur. C'est pourquoi le marché a vu naître un quatrième niveau : avancé avec certificat qualifié.

La signature électronique simple est émise sans certificat personnel au nom du signataire et sur la base d'informations personnelles (numéro de téléphone, email) renseignées par la personne souhaitant faire signer le document. Le processus de signature simple peut être renforcé et acquérir une valeur légale plus importante grâce à l'ajout d'une étape d'authentification au moyen d'un code SMS reçu par les signataires.

La signature avancée quant à elle requiert des moyens d'identification plus poussés et nécessite la création d'un certificat émis au nom du signataire et contenant des informations collectées grâce à l'envoi de sa pièce d'identité. Le justificatif d'identité est contrôlé par un PSCo. Le niveau d'identification est ici plus élevé. Là encore, l'étape d'authentification au moyen d'un code SMS est indispensable à la signature.

La signature avancée avec certificat qualifié s'effectue avec un certificat nécessitant l'envoi d'un document d'identité et un face-à-face entre le futur titulaire du certificat et l'opérateur d'enregistrement. Ce dernier procédera au contrôle physique de l'identité du signataire en plus de sa pièce d'identité, s'assurant ainsi de l'exactitude des informations s'y trouvant. Comme pour la signature simple et avancée, l'authentification avec un code SMS est également indispensable à la signature.

La signature qualifiée est réalisée quant à elle avec un certificat qualifié et un dispositif qualifié de création de signatures. Elle bénéficie d'une présomption de fiabilité. Le procédé d'identification est dans ce cas présumé fiable,

entraînant un renversement de la charge de la preuve. La personne mettant en cause l'identification devra alors prouver que celle-ci est erronée.

En résumé, plus le niveau de sécurité d'une signature augmente, plus les points de contrôle (à distance ou en face-à-face) de l'identité du signataire sont nombreux, réduisant ainsi le risque d'une usurpation d'identité. De plus, l'horodatage apporte également un niveau de sécurité supplémentaire et contribue ainsi à assurer l'intégrité du document signé. En effet, il garantit l'existence d'un fichier à une date donnée sans modification depuis (principe d'intégrité).