



La confiance au-delà du signataire

L'importance de la fiabilité des documents, des signatures numériques vérifiables et de la capacité des destinataires à vérifier les documents sur lesquels ils se fondent.

Par Nada Belhadfa • Portage CyberTech

La question clé n'est pas seulement de savoir si le signataire est digne de confiance, mais si le document reste digne de confiance après avoir quitté ses mains.

Tous les professionnels reconnaissent que les signatures, les sceaux, les approbations et les titres de compétence ne sont pas de simples éléments décoratifs. Ils représentent la responsabilité, l'autorité et la confiance. Aujourd'hui, cependant, les documents importants sont couramment partagés, copiés, stockés, réutilisés et considérés comme fiables par des personnes qui n'ont peut-être aucun lien avec l'auteur original. Un document peut transiter par plusieurs organisations et rester en circulation pendant des années après sa création.

Le défi ne réside pas dans la fiabilité du signataire d'origine. Le défi consiste à déterminer si cette confiance demeure vérifiable une fois que le document échappe au contrôle du signataire.

Par exemple, un document professionnel peut être préparé pour un client, révisé par des conseillers, soumis aux autorités ou à des organismes gouvernementaux, utilisé comme référence par des institutions financières, puis consulté des années plus tard par des personnes qui n'ont joué aucun rôle dans sa création.

C'est là que le risque survient. Alors que l'approbation, la signature ou les titres de compétence demeurent associés au document, le signataire, lui, en est dissocié. Une fois qu'un fichier est partagé, copié ou modifié, l'apparence de confiance peut persister, mais la preuve sous-jacente peut ne plus exister. Par conséquent, la fiabilité du document devient incertaine.

1 La confiance doit être vérifiable

Lorsqu'un document est contesté, les questions sont d'ordre pratique :

- Ce document a-t-il vraiment été approuvé ou signé par la personne dont le nom y figure ?
- Cette personne était-elle autorisée à approuver ou à signer à ce moment-là ?
- Y a-t-il eu des changements depuis que le document a été finalisé ?
- Ces réponses peuvent-elles encore être vérifiées des années plus tard ?

Il ne s'agit pas seulement de questions d'ordre technologique. Ce sont des questions de confiance.

Ce sont les questions qui importent aux clients, aux organisations, aux institutions financières, aux organismes gouvernementaux, aux assureurs, aux avocats, aux tribunaux, aux organismes de réglementation, aux vérificateurs et au grand public lorsque la fiabilité d'un document est en jeu.

Quatre principes devraient guider l'évaluation de tout document officiel :

- Identité
- Autorisation
- Intégrité
- Pérennité (capacité à pouvoir être ouvert et lu pendant des décennies)

Si l'un de ces principes ne peut être démontré, la confiance commence à s'éroder.

2 La plupart des problèmes ne proviennent pas du piratage

L'une des plus grandes idées fausses est que la fraude documentaire doit nécessairement impliquer une cybercriminalité sophistiquée. En pratique, de nombreux problèmes découlent simplement du traitement courant des documents :

- Un document est converti en image.
- Un PDF signé est inséré dans un autre fichier.
- Un rapport antérieur est réutilisé et modifié.
- L'image d'une signature ou d'un sceau est copiée à partir d'un document existant.

Dans chaque cas, le document peut toujours paraître légitime. La signature peut toujours sembler familière. L'approbation peut toujours

paraître authentique. Mais la capacité de vérifier de façon indépendante l'origine du document, l'autorité du signataire et l'intégrité du document peut avoir été compromise

Le problème ne réside pas toujours dans une intention malveillante. Parfois, ce sont simplement les processus de travail qui sont en cause. Parfois, c'est par commodité. Parfois, c'est un destinataire qui ne sait pas quoi vérifier.

Le résultat est le même : des décisions importantes sont prises sur la base de documents pour lesquels il n'existe peut-être plus de preuves suffisantes.

3 Toutes les signatures ne se valent pas

Pour la plupart des destinataires, les différentes méthodes de signature peuvent sembler similaires :

- Une signature numérisée
- Une image collée
- Un certificat de signature numérique auto-émis
- Une signature numérique appuyée par un fournisseur d'identité ou une autorité d'accréditation reconnue

Visuellement, les différences peuvent être subtiles. Sur le plan juridique, bon nombre de ces méthodes peuvent être valides. Cependant, elles ne sont pas toutes équivalentes du point de vue de la fiabilité, de la vérification indépendante et du fardeau de la preuve.

Dans un contexte de documents électroniques, les questions clés sont les suivantes :

- La signature est-elle légitime ?
- Le document a-t-il été modifié depuis sa signature ?
- Le signataire possédait-il l'autorité, les titres de compétence ou les autorisations nécessaires pour approuver le document ?

La force d'une méthode de signature numérique ne réside pas dans son apparence, mais dans ce qu'elle permet de prouver.

4 Protection du public, imputabilité et responsabilité juridique

Au fond, il est question d'imputabilité, de confiance et de responsabilité juridique. Les organisations responsables de la surveillance, de la conformité, de l'agrément ou de la gouvernance ont besoin de mécanismes fiables pour s'assurer que les documents

sont dignes de confiance et que les personnes autorisées peuvent être distinguées de celles qui donnent simplement l'apparence d'être légitimes.

Pour les signataires et les détenteurs de documents, les avantages sont tout aussi importants. Les signatures numériques appuyées par des cadres de confiance en matière d'identité et d'accréditation contribuent à établir la preuve de l'identité, de l'autorité, du moment de la signature, de l'intégrité et de la juridiction applicable. Elles réduisent également le fardeau qui incombe aux organisations et aux destinataires en permettant la vérification au moment où l'on s'y fie, sans hypothèses ni vérifications manuelles répétées.

5 L'importance de l'écosystème

La confiance numérique ne fonctionne pas en vase clos. Les créateurs de documents doivent utiliser des méthodes reconnues. Les organisations chargées de délivrer, de gérer ou de valider les titres de compétence numériques doivent maintenir des processus fiables. Les destinataires doivent être disposés et capables de valider ce qu'ils reçoivent.

Si l'un de ces éléments fait défaut, la confiance s'effondre. Un document électronique correctement signé n'a qu'une valeur limitée si le destinataire ne peut pas le valider. Or, même un destinataire disposé à effectuer cette vérification ne peut confirmer l'autorité du signataire si le titre de compétence n'a pas été délivré par une source de confiance.

6

Liste de vérification pratique avant de se fier à un document

Avant de se fier à un document électronique signé, les destinataires devraient être en mesure de répondre à quelques questions de base :

- Le signataire possédait-il l'expertise, l'autorité ou le mandat nécessaires pour approuver le document ?
- Le signataire était-il autorisé au moment de la signature ?
- Le document a-t-il été signé à l'aide d'une méthode reconnue et vérifiable ?
- Le titre de compétence a-t-il été délivré par une autorité de confiance ?
- Le document a-t-il été modifié depuis sa finalisation ?

Si la réponse à l'une de ces questions est « Je ne sais pas », la confiance est compromise.

Cela ne signifie pas nécessairement que le signataire a agi de manière inappropriée. Cela signifie que le destinataire ne peut pas démontrer de façon indépendante que les conditions requises pour s'y fier sont remplies.

Conclusion

La responsabilité est rarement déterminée par l'intention seule. Elle est déterminée par ce qui peut être démontré. Les signatures numériques appuyées par des autorités de confiance en matière d'identité et d'accréditation n'empêchent pas toutes les erreurs; elles permettent toutefois de rendre la responsabilité visible. Elles aident à démontrer qui a signé, en vertu de quelle autorité et si le document est demeuré intact après la signature. Les documents circulent souvent bien plus loin que les personnes qui les créent. La question est de savoir si la confiance qui leur est associée les accompagne. C'est pourquoi la vérification indépendante de l'identité, de l'autorité, des titres de compétence et de l'intégrité du document reste importante longtemps après que le document a quitté les mains de son créateur.

Assurez la fiabilité de vos documents

Pour en savoir plus sur la vérification de l'authenticité des documents et pour accéder à nos outils gratuits de validation des signatures, visitez notre site Web.

<https://www.portagecybertech.com>

Scannez pour en savoir plus

