



Méthodes d'Authentification Fiables

Pour les Transactions avec Signatures Électroniques








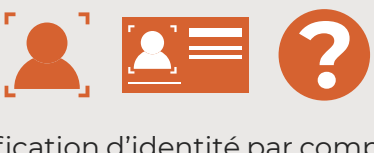
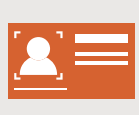


 <p>AUTHENTIFICATION PAR COURRIEL</p> <p>Le signataire reçoit un courriel l'invitant à accéder à la cérémonie de signature numérique en cliquant sur un lien. L'authentification du signataire se produit lorsqu'il peut accéder à son compte courriel.</p>	 <p>IDENTIFIANTS D'OUVERTURE DE SESSION</p> <p>Le signataire est authentifié par le système de l'expéditeur avant de lui donner accès à la transaction. L'ouverture d'une session exige un nom d'utilisateur et un mot de passe valides.</p>	 <p>AUTHENTIFICATION PAR MESSAGE TEXTE</p> <p>Vérifier l'identité d'un signataire en lui envoyant un seul code sécurisé par message texte à son numéro de téléphone mobile. Le signataire entre le code dans la page de connexion pour avoir accès aux documents à signer.</p>	 <p>DÉFI DE LA QUESTION SECRÈTE</p> <p>Le signataire doit répondre correctement à des questions d'identification. Celles-ci sont désignées comme des « secrets partagés » car les questions et les réponses sont établies au préalable.</p>	 <p>VÉRIFICATION D'IDENTITÉ GOUVERNEMENTALE</p> <p>Vérifier à distance les personnes inconnues en utilisant les pièces d'identité gouvernementales (p. ex., permis de conduire, passeport, etc.). OneSpan Sign optimise la vérification d'identité numérique pour capturer, extraire et analyser les données d'identité afin d'authentifier les documents d'identité émis par les gouvernements.</p>
 <p>COMPARAISON BIOMÉTRIQUE</p> <p>La comparaison biométrique est généralement utilisée lors de transactions à haut risque et de grande valeur avec des signataires inconnus. Les signataires peuvent prendre un autoportrait et il sera comparé à la photo qui figure sur la pièce d'identité émise par leur gouvernement pour vérifier leur identité en quelques secondes.</p>	 <p>AUTHENTIFICATION BASÉE SUR DES CONNAISSANCES (KBA) DYNAMIQUE</p> <p>Lorsque le service de signature électronique est intégré à un service de vérification d'identité par un tiers tel qu'Equifax, le signataire reçoit des questions de connaissances à la volée.</p>	 <p>CARTES INTELLIGENTES ET IDENTIFIANTS DÉRIVÉS</p> <p>Les employés fédéraux et les entrepreneurs doivent utiliser une carte intelligente ou des identifiants mobiles dérivés lors d'une signature électronique. C'est une forme d'authentification multifactorielle : la carte ou l'appareil mobile intelligent, combiné au NIP de l'utilisateur.</p>	 <p>CERTIFICATS NUMÉRIQUES</p> <p>Émis par des tiers tels que des prestataires de services de confiance ou des autorités de certification, les certificats numériques sont utilisés au moment de la signature pour valider l'identité de l'utilisateur.</p>	 <p>DIGIPASS</p> <p>Digipass® est une solution d'authentification multifactorielle qui génère des mots de passe à usage unique (OTP) qui devront être utilisés avec une autre méthode d'authentification, tel qu'un NIP ou une empreinte digitale.</p>

Définition de l'Authentification
 Utilisées seules ou combinées, les méthodes d'authentification vérifient l'identité d'une personne qui doit participer à une transaction fiable.

Catégories d'Authentification

 <p>Savoir</p> <p>CE QUE VOUS SAVEZ (p. ex., un mot de passe)</p>	 <p>Avoir</p> <p>CE QUE VOUS AVEZ (p. ex., un authentifiant matériel ou logiciel, une carte intelligente émise par le gouvernement, un appareil mobile)</p>	 <p>Être</p> <p>QUI VOUS ÊTES (p. ex., biométrie comme l'empreinte digitale ou la reconnaissance faciale)</p>
--	--	---

Exemples d'Authentification de Signatures Électroniques

 <p>Canal</p>	 <p>Transaction</p>	 <p>Méthode d'Authentification</p>
 <p>EN LIGNE</p>	<p>DEMANDE DE PRÊT HYPOTHÉCAIRE</p> <p>ÉVALUATION DE RENDEMENT DES EMPLOYÉS À L'INTERNE</p> <p>CONTRAT DE FOURNISSEUR</p>	 <p>Identifiants d'ouverture de session ou adresse de courriel valide sur le portail de la banque + mot de passe à usage unique sur message texte</p>  <p>SSO Authentification unique (SSO) ou authentification par courriel</p> <p>***** Nom d'utilisateur et mot de passe + numéro d'identification du fournisseur</p>
 <p>MOBILE</p>	<p>OUVERTURE DE COMPTE DE BANQUE</p> <p>PROCÉDURE POUR EMPLOYÉS DU GOUVERNEMENT (DEMANDE DE VACANCES)</p>	 <p>Vérification d'identité par comparaison biométrique, vérification de pièces d'identité gouvernementales ou KBA (nouveau client)</p>  <p>SSO Authentification unique (les employés fédéraux utilisent aussi une carte intelligente ou un identifiant dérivé)</p>
 <p>CENTRE D'APPELS</p>	<p>RÉCLAMATION D'ASSURANCES</p>	 <p>Adresse de courriel valide ou identifiants d'ouverture de session du portail de la clientèle</p> <p>*****</p>

SOCIAL MEDIA



© 2021 OneSpan North America Inc., tous droits réservés. Digipass® et Cronto® sont des marques déposées ou non de OneSpan North America Inc. et/ou de OneSpan International GmbH aux États-Unis et dans d'autres pays. Toutes les autres marques ou noms commerciaux cités ci-contre sont la propriété de leurs propriétaires respectifs. OneSpan se réserve le droit de modifier les spécifications à tout moment, sans préavis. Les renseignements fournis par OneSpan dans ce document sont réputés exacts et fiables. Toutefois, OneSpan ne saurait être tenue responsable des préjudices subis du fait de leur utilisation, ni de la violation de brevets ou autres droits de tiers liés à leur utilisation. Dernière mise à jour : Septembre 2021

OneSpan.com

INFO-L1-AUTHENTIFICATION-METHODS-FR-0000021