Signatures numériques à partir du cloud – fondements et utilisation

PDF-TOOLS.COM
Premium PDF Technology

Sommaire

Fondements de la signature numérique

Documents et signatures électroniques

Dans les échanges commerciaux, les documents électroniques sont échangés et archivés de manière croissante et tout à fait naturelle, à l'instar de ce qui est déjà pratiqué depuis longtemps pour leurs équivalents sur papier. Les documents papier sont souvent munis de signatures manuscrites, qui confèrent aux documents une force probante définie dans le droit applicable. Afin que les documents électroniques aussi puissent être signés avec la même force probante, la législation a créé la signature électronique.

Les avantages de la signature électronique dans les processus commerciaux sont évidents :

- Amélioration des performances et de la qualité : ils permettent la signature automatisée de documents dans le courrier sortant et la vérification automatisée de signatures dans le courrier entrant.
- Sécurité juridique : ils permettent d'améliorer la force probante, notamment l'incontestabilité (non-répudiation) des données transmises par voie électronique.

Les textes de lois décrivent les propriétés d'une signature électronique. Mais les textes ne donnent pas de spécifications pour la réalisation technique. Pour la réalisation technique, l'industrie a développé une série de standards définissant la notion de signature numérique et en décrivant les propriétés.

Signature électronique

Les fonctions d'une signature électronique sont :

- **Remplacement de la signature manuscrite :** la signature électronique peut satisfaire l'exigence de la signature manuscrite au même titre que la signature manuscrite proprement dite dès lors que les conditions légales sont satisfaites.
- **Protection de l'intégrité :** les signatures électroniques ont un « effet de scellé » sur les documents numériques.
- **Authenticité :** la signature électronique permet de garantir que la personne physique ou morale peut être identifiée.
- **Autorisation :** dans le certificat, les droits et prérogatives peuvent être définis, gérés et donc attribués à la personne.

Conformément à la loi fédérale sur les services de certification et d'autres applications de certificats numériques dans le domaine de la signature électronique (SCSE), il existe deux types de certifications :

- La **signature électronique avancée** (protection de l'intégrité et identification du signataire) peut être utilisée pour les personnes physiques et morales et est affectée à un « titulaire ». Le « titulaire » peut être une personne, mais aussi une machine (serveur). Elle n'est pas équivalente à la signature manuscrite et convient notamment à la signature de documents numériques non soumis à des règles formelles légales.

- La **signature électronique qualifiée** (satisfaction aux règles formelles) est une signature électronique avancée reposant sur une unité de création de signature sécurisée et sur un certificat, valide au moment de la création, établi pour une personne spécifique. De plus, le certificat doit provenir d'un fournisseur homologué de services de certification. Le « titulaire » est toujours une personne physique.

L'ordonnance du DFF concernant les données et informations électroniques (OeIDI) règle notamment les exigences techniques, organisationnelles et procédurales envers la signature électronique concernant la création et la vérification de factures soumises à la TVA. L'ordonnance concernant la tenue et la conservation des livres de comptes (Olico) stipule que des signatures et horodateurs électroniques peuvent être utilisés pour conserver des documents enregistrés sur des supports d'information modifiables.

Pour les signatures électroniques qualifiées avec preuve d'identité, il existe en Suisse la SuisseID pour les personnes physiques.

Signature numérique

Comme nous l'avons déjà mentionné, la signature numérique est une mise en œuvre technique de la signature électronique. Elle est constituée de données que l'on affecte au document signé. Afin que les propriétés exigées dans les textes de lois puissent être garanties de manière sûre, des procédés cryptographiques sont utilisés pour la création et le contrôle de signatures numériques.

Pour générer une signature numérique, il faut les trois choses suivantes :

- Un certificat délivré au « titulaire »
- Une clé privée adaptée que ne possède que le « titulaire » et qu'il doit garder précieusement
- Le document à signer

Avec le logiciel de signature le « titulaire » peut générer une signature numérique. Le récepteur du document peut contrôler à présent la signature numérique. Pour cela, il faut les trois choses suivantes :

- Le document signé
- Le certificat du « titulaire ». En règle générale, il est intégré dans le document même.
- La signature numérique. Celle-ci est également intégrée dans le document avec le certificat.

Le récepteur peut facilement réaliser cette opération, à l'aide du logiciel de signature.

Conformément à la loi, le « titulaire » nécessite aussi une unité de création de signatures pour générer des signatures qualifiées. Du point de vue technique, il s'agit d'un appareil électronique qui conserve la clé privée en lieu sûr et la protège contre les accès non autorisés de l'extérieur. Dans la pratique, les appareils convenables utilisés sont les smartcards, les tokens USB et les HSM (Hardware Security Module). Pour des raisons pratiques, ces appareils contiennent aussi, outre la clé privée, les certificats de « titulaire » et les certificats de l'émetteur. Contrairement à la clé privée, les certificats n'ont pas besoin d'être protégés. Il est permis de les publier, puisqu'ils sont nécessaires au contrôle de la signature numérique.

Standards pour les documents et signatures numériques

Les principaux standards de documents pour les documents numériques signés sont :

- ISO 19005 (PDF/A) : la norme ISO 19005 définit un format de fichier basé sur le PDF, appelé PDF/A. Ce format offre un mécanisme qui présente les documents électroniques de manière à ce que l'apparence visuelle reste conservée pour longtemps, indépendamment des outils et systèmes pour la réalisation, l'enregistrement et la reproduction. Aussi, le document doit-il contenir tout ce qui est nécessaire pour une visualisation claire (polices de caractères, profils de couleurs, etc.) et ne doit-il pas renvoyer, ni directement, ni indirectement, à des sources externes.
- XML : ce format a été développé pour l'échange de données à structure hiérarchique et sous forme de texte entre machines. La spécification est publiée par le W3C (World Wide Web Consortium).
- EDIFACT : c'est un standard international inter-branches pour l'échange électronique de données dans les communications commerciales. EDIFACT est l'un de plusieurs standards EDI. C'est une institution de l'ONU qui est responsable du standard EDIFACT.

L'ETSI a développé des standards pour les structures de données de signatures numériques qui satisfont les exigences pour les signatures électroniques avancées et qualifiées. Les standards sont les suivants :

- PAdES (PDF Advanced Electronic Signature Profiles)
- CAdES (CMS Advanced Electronic Signatures)
- XAdES (XML Advanced Electronic Signatures)

Les signatures numériques sont utilisées essentiellement dans les applications suivantes : l'échange de documents et l'archivage. Pour la conservation à long terme de documents, la signature numérique doit satisfaire des exigences supplémentaires. La première exigence concerne le contrôle de validité à long terme du certificat. On l'appelle LTV (Long Term Validation). D'une part, les mesures standards de l'ETSI décrivent des mesures contre les attaques envers les procédés cryptographiques qui deviennent possibles par la capacité de calcul sans cesse croissante. D'autre part, une signature numérique avec LTV comprend aussi les données suivantes :

- Trust Chain : le certificat de l'éditeur, y compris tous les certificats intermédiaires constituant ensemble une chaîne de confiance.
- OCSP Response : données certifiant la validité d'un certificat par l'éditeur au moment de la signature.

Pour les informations LTV, la signature du service OCSP doit être disponible au moment de la création de la signature. Elle n'est plus requise pour le contrôle ultérieur. Cela garantit que ces signatures peuvent aussi être contrôlées à long terme.
Pour les signatures numériques sans propriété LTV, c'est exactement l'inverse. Il n'est pas nécessaire qu'un service soit disponible pour les générer. Les services OCSP doit toutefois être accessible pour le contrôle.

La deuxième exigence concerne le contrôle du moment de la signature. Pour cela, la signature numérique doit aussi comporter les données suivantes :

- TSP Response : données d'un service d'horodatage certifiant le moment de la signature.

Sans horodatage, on ne peut plus prouver ultérieurement le moment de la signature. Le service TSP doit toujours être disponible au moment de la signature. Aucun service TSP n'est requis pour le contrôle.

Fonction et utilisation du service de signature à partir du cloud

Quelle est la fonction du service ?

La fonction principale d'un service de signature consiste à générer des données de signature complètes en raison d'une requête de signature par un client signature. La requête de signature est générée en raison du document à signer d'une part et de l'authentification du client d'autre part. Le service renvoie les données de signature au client signature où elles sont ensuite reliées au document initial pour obtenir le document signé.

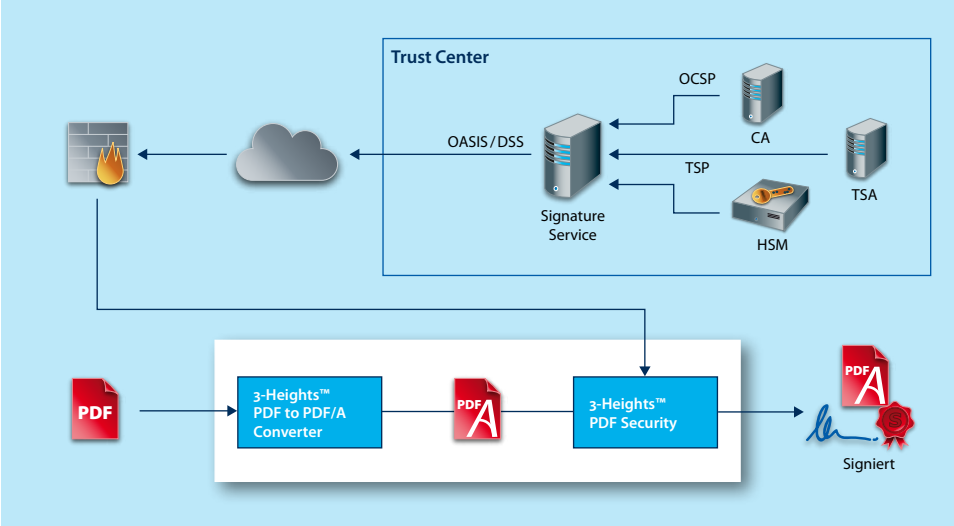


Illustration 1 : Un service central pour la création et le contrôle de signatures numériques

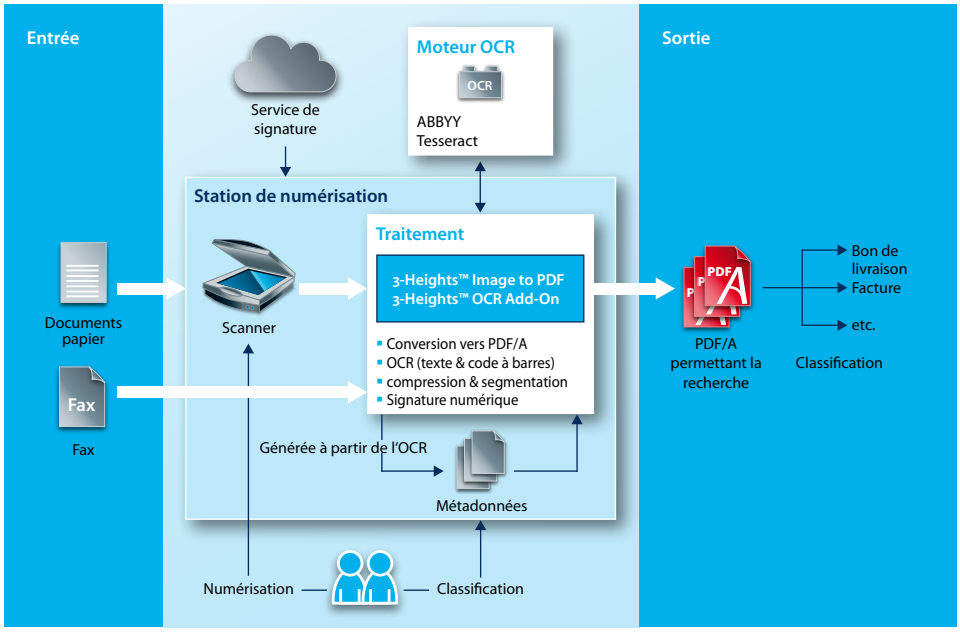
Le document proprement dit n'est pas transmis au service, mais une valeur hash (une sorte d'empreinte digitale) de celui-ci. La valeur hash ne permet pas de déduire le contenu du document. Cela garantit la confidentialité du document dans toutes applications imaginables, telles que dossiers de patients, données bancaires, dessins de conception, etc.
L'authentification mutuelle du client et du serveur et de la transaction se fait par des liaisons sécurisées (TLS). La liaison sécurisée est protégée par un certificat de client et un certificat de serveur. Cette mesure permet d'affecter les signatures sans équivoque à un client.
Le service exploite pour chaque client les clés et certificats personnels requis dans un environnement sécurisé et digne de confiance. Le service génère ainsi les signatures individuelles. Il prend en charge des certificats d'organisation avancés selon SCSE et OeIDI ainsi que des certificats qualifiés sur la base de la SuisseID. Les certificats sont renouvelés automatiquement par le service lorsque la validité arrive à échéance.
Au choix, le service peut aussi générer des signatures valides à long terme (LTV) et intégrer un horodatage.
La structure redondante du service garantit une disponibilité élevée.
Le service est exploité par un éditeur de certificats accrédité qui garantit le respect de tous les règlements nécessaires.

Où utilise-t-on le service ?

Dans l'entreprise, le service de signature peut être utilisé partout où des signatures électroniques devraient ou doivent être générées. Certains exemples typiques sont décrits ci-après.

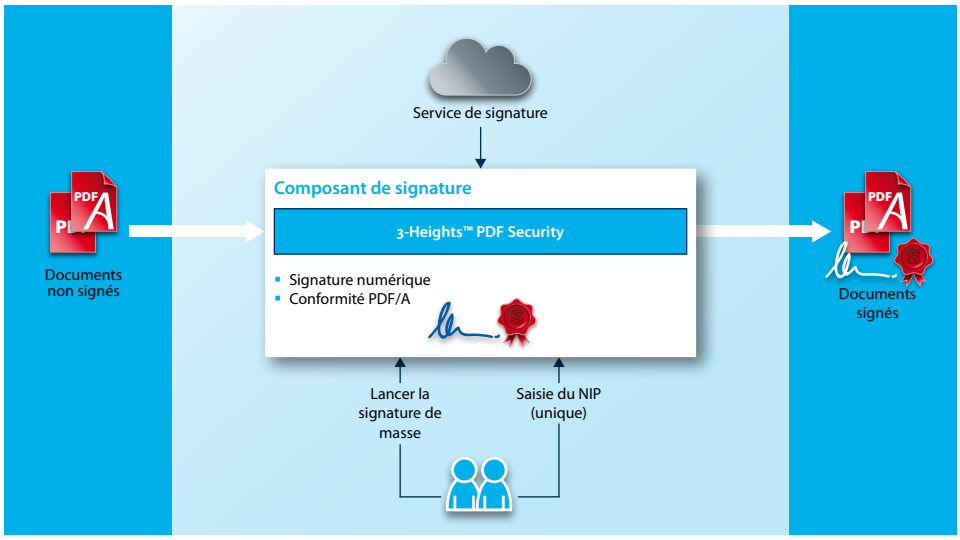
Protection de l'intégrité à la réception du courrier

Les documents papier apparaissant dans le courrier entrant d'une entreprise peuvent être numérisés, transformés selon PDF/A et signés avec un horodatage. La même chose s'applique à la réception de tous les échanges de fax entre l'entreprise et ses partenaires commerciaux. Cette mesure garantit l'intégrité des documents reçus dans les processus en aval.



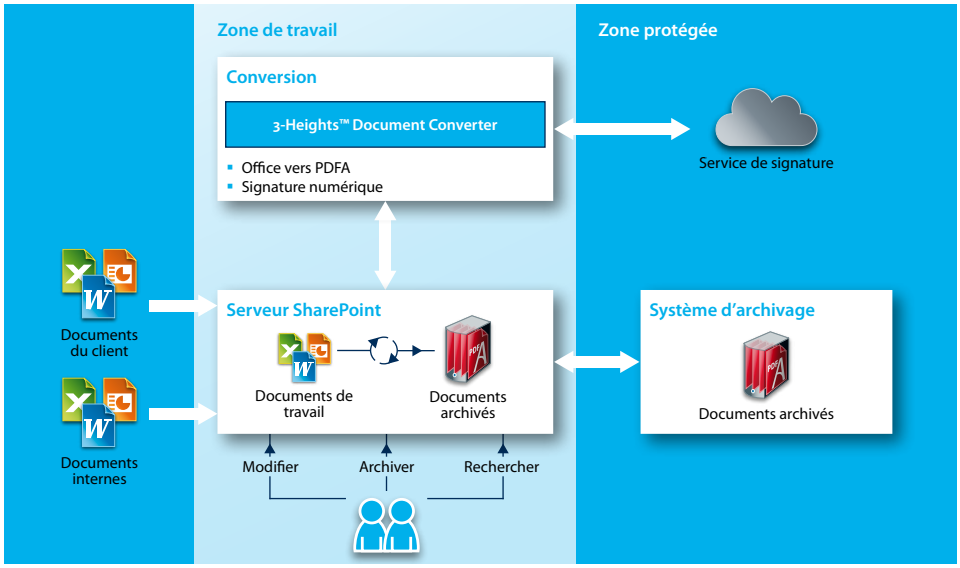
Documents conforme à l'OeIDI dans le courrier sortant

Dans le courrier sortant, les documents non signés, tels que les factures, sont convertis en PDF/A et munis d'une signature conforme à l'OeIDI.



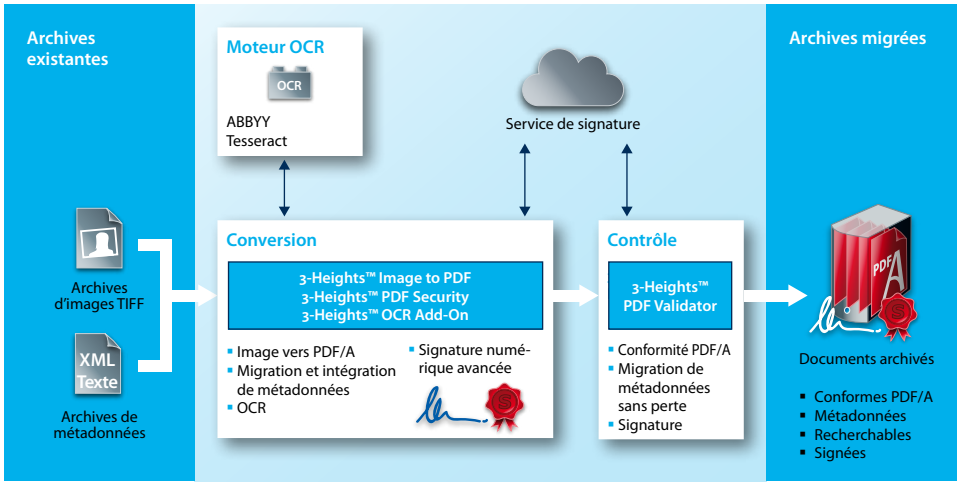
Archivage de documents de travail finaux

Les documents de travail ayant atteint l'état final dans leur cycle de vie et destinés à l'archivage sont convertis en PDF/A et signés numériquement par la même occasion. Le processus de traitement des documents est souvent pris en charge avec un serveur SharePoint. À l'aide d'une extension, la conversion en PDF/A et l'application de la signature numérique à partir du cloud peuvent être automatisées.



Migration d'archives retraçable

Des archives existantes avec des images TIFF, JPEG et autres ainsi que des données d'indice séparées sont transformées en PDF/A et munies en même temps d'une signature à partir du cloud. La signature garantit la traçabilité de la migration.



Quels sont les avantages d'un service de signature ?

Le service de signature offre de nets avantages économiques et techniques par rapport à des solutions autonomes. Les principaux sont résumés ici.

Durée d'introduction courte	La mise en place d'une infrastructure de signature avec un serveur et des clients dans une entreprise exige du savoir-faire, la formation du personnel et du temps. L'utilisation du service de signature réduit considérablement ce temps car il n'est pas nécessaire de monter une infrastructure de serveur et il ne faut mettre en place que les clients signature, qui sont bien plus simples.
Réduction des coûts d'investissement et d'exploitation	Il n'est plus nécessaire d'acquérir des HSM, des certificats et des tokens pour chaque collaborateur. De même, il n'y a pas de coûts pour l'exploitation de serveurs ni pour le renouvellement de certificats. Les certificats expirés peuvent revenir cher, surtout s'ils entraînent un arrêt de l'exploitation.
Omniprésence, indépendance du lieu, pas de tokens	Le service de signature permet de signer partout des documents et des données sans devoir disposer de tokens et de lecteurs de carte. Les appareils mobiles se répandant de manière croissante, c'est souvent la seule possibilité de pouvoir lire des signatures électroniques. Les signatures peuvent être effectuées via le réseau, par exemple des postes de travail à domicile.
Conformité / réglementations	Le service est exploité par un éditeur de certificats accrédité qui garantit le respect de tous les règlements nécessaires (SCSE). Le service génère aussi bien des signatures avancées selon OeIDI que des signatures qualifiées correspondant à la SuisseID.
Disponibilité élevée	De par la configuration redondante du matériel, l'exploitant du service garantit une disponibilité élevée du service.
Qualité élevée, conformité aux standards	Le prestataire du service garantit l'évolution et l'adaptation continues des signatures numériques aux derniers standards industriels (ISO, ETSI).
Sécurité	Le service exploite des clés et certificats personnels dans un environnement sécurisé et digne de confiance. Les certificats sont renouvelés automatiquement par le service lorsque la validité arrive à échéance.
Confidentialité	Le service de signature permet de signer des données et documents du niveau de confidentialité le plus élevé car les données ne quittent jamais l'entreprise pour l'opération de signature.
Faible exposition aux attaques	L'utilisation du service augmente la résistance aux attaques de firewall car un seul protocole à base de XML est utilisé. Les solutions autonomes requièrent l'accès à plusieurs protocoles OCSP et TSP, à la technique de sécurité plus complexe. De plus, la liaison entre le client signature et le service de signature est protégée par l'authentification TLS mutuelle.
Modularité	Le service peut traiter de quelques requêtes de signature jusqu'à des millions par jour.

Tableau 2 : Les avantages d'un service de signature à partir du cloud

Logiciel pour l'utilisation du service de signature à partir du cloud

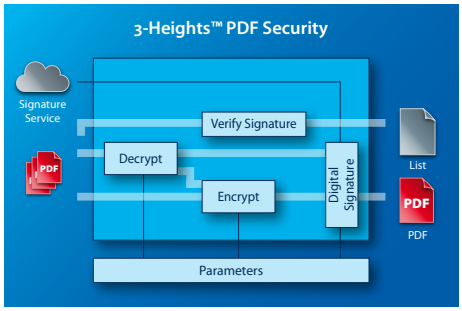
Fonction du client de signature

Le client signature est un composant de logiciel capable de signer les données et documents à l'aide du service de signature à partir du cloud. Le client signature communique avec le service à l'aide du protocole OASIS/DSS. Il génère des requêtes de signature correctes, vérifie la réponse et intègre le résultat dans les fichiers à signer ou le document à signer.

Le client signature fait partie constituante des produits décrits ci-après.

3-Heights™ PDF Security

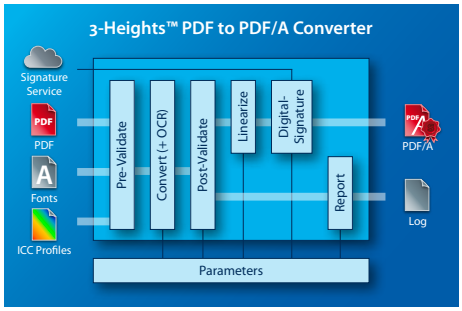
Le composant 3-Heights™ PDF Security offre deux fonctions principales : le cryptage et la signature numérique pour les documents PDF. L'élément fonctionnel « signature numérique » comporte :



- Signature conforme de PDF et PDF/A (PAdES Part 2)
- Vérification de la validité de signatures dans un document PDF
- Signatures d'utilisateur, signatures d'auteur (MDP) et signatures d'horodatage
- Signature électronique simple, avancée ou qualifiée
- Signature de longue durée (LTV) avec chaîne de confiance intégrée, horodatage et information de contrôle quant à la validité du certificat
- Prise en charge de services de signature à partir du cloud via OASIS/DSS et d'appareils de signature de masse (HSM) via PKCS#11
- Listage et rétablissement des révisions
- Signatures invisibles et visibles
- Configuration de la signature visible

3-Heights™ PDF to PDF/A Converter

Le 3-Heights™ PDF to PDF/A Converter repose sur le composant 3-Heights™ PDF Security et offre les fonctions supplémentaires suivantes :



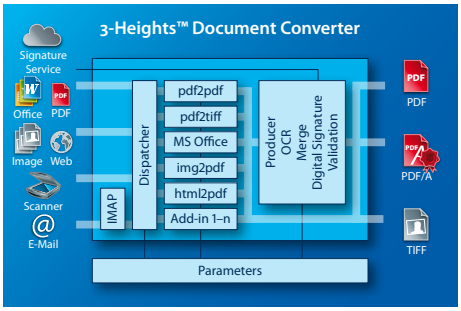
- Conversion de documents PDF selon PDF/A-1, PDF/A-2 ou PDF/A-3
- Validation de documents entrants
- Validation de documents sortants
- Intégration automatisée et configurable de profils de couleurs pour l'utilisation d'espaces colorés dépendant des appareils

- Intégration automatique et configurable de polices de caractères : intégration comme sous-groupe afin de limiter la taille du fichier, ou intégration de toute la police afin de pouvoir éditer le fichier ultérieurement
- Création automatique de métadonnées ou intégration de celles-ci à partir de sources externes
- Connexion d'un moteur OCR (Abbyy ou Tesseract) pour la reconnaissance de texte; en option, enregistrement du texte reconnu comme fichier texte

3-Heights™ Document Converter

Le convertisseur de documents 3-Heights™ est une solution utilisable dans toute l'entreprise pour la conversion de tous les formats de fichier courants en PDF/A, PDF et TIFF. L'application la plus courante consiste à convertir des documents Microsoft Office en PDF ou PDF/A pour l'archivage avec ajout optionnel d'une signature à partir du cloud.
Elle permet de traiter les exigences les plus diverses dans le domaine de la conversion, notamment :

- archivage de documents MS Office en PDF/A
- archivage d'images telles que TIFF, JPEG et autres formats d'image
- archivage de sites Internet
- archivage d'e-mails
- uniformisation de la multitude de formats à travers toute l'entreprise



Interfaces pour l'intégration de l'application

Pour l'intégration de postes de travail d'ordinateurs à serveur exploitant des applications qui veulent utiliser les produits 3-Heights™, il existe une série d'interfaces. Les principales sont :

- **Webservice :** le service Web permet de signer des documents provenant de l'Intranet, d'une application ou d'un appareil mobile.
- **Interface de programmation (API) :** ce composant permet l'intégration programmatique du service dans des applications. Il offre des interfaces pour les technologies Java, C, COM et .NET. Le composant est également disponible pour d'autres plateformes telles que Linux, Sun OS, AIX, HP-UX, Mac OS/X, etc.
- **Command Line Tool :** cet outil est un programme autonome pouvant être exécuté directement de la ligne de commande sans autres conditions. Il permet d'automatiser les déroulements à l'aide de la langue de commande (Shell Command) sans qu'il faille un environnement de développement. Le programme de lignes de commande est également disponible pour d'autres plateformes telles que Linux, Sun OS, AIX, HP-UX, Mac OS/X, etc.

Glossaire

Termes

Hash	Une valeur hash (en abrégé : un hash) est un nombre calculé à partir d'une quantité quelconque de données telles que des documents, certificats, messages, etc. Ce nombre est souvent bien plus court que les données initiales (env. 20 octets). La caractéristique de la valeur hash est qu'elle est la même pour des données identiques et qu'elle est très probablement sans équivoque pour des données différentes. De plus, la valeur hash ne permet plus de déduire les valeurs initiales. Le calcul recourt à des algorithmes hash tels que SHA-1 ou SHA-2.
Clé	Le certificat comprend une clé publique (Public Key) utilisée pour le contrôle de la signature. La clé publique doit correspondre à une clé privée (Private Key) utilisée pour générer la signature et devant être conservée en lieu sûr.
Signature, signer	Données permettant d'assurer l'intégrité et l'authenticité d'un document. Pour l'essentiel, la signature est réalisée comme suit : la valeur hash des données à signer est déterminée, puis cryptée avec la clé privée. La signature est placée dans un message CMS avec les certificats et les informations de contrôle, puis intégrée au choix dans le document signé.
Token	Un « récipient » (partie de HSM, clé USB, smartcard, etc.) des contenant des clés privées et protégeant contre les accès non autorisés. Pour des raisons pratiques, le token comprend souvent aussi des certificats adaptés et des clés publiques qui ne nécessitent pas de protection.
Vérification, vérifier	Une signature est vérifiée comme suit : la signature est extraite du document, puis décryptée avec la clé publique. On obtient ainsi la valeur hash des données au moment de la signature. Ensuite la valeur hash des données signées est recréée et comparée à la valeur hash de la signature. Si les deux valeurs coïncident, les données n'ont pas été modifiées et sont dignes de confiance (contrôle d'intégrité). On peut aussi extraire le certificat du message de signature et identifier ainsi le signataire (contrôle d'identité). D'autres contrôles concernant la validité du certificat et l'horodatage sont possibles en fonction du type de signature.
Cryptage	Les données sont cryptées afin que des tiers ne puissent pas y accéder. Pour la communication entre l'émetteur et le destinataire, ce dernier génère une paire de clés, l'une privée et l'autre publique. Si l'émetteur crypte à présent les données avec la clé publique, seul le destinataire peut décrypter les données car il reste le seul détenteur de la clé

	privée. Le cryptage recourt à des algorithmes de RSA avec des longueurs de clé actuelles de 2048 bits. C'est sur cette technique que reposent les procédés usuels pour les signatures numériques.
Certificat	Un certificat est justificatif de l'identité d'une personne physique ou morale. De plus, un certificat comprend une clé publique pour laquelle la personne détient la clé privée correspondante. Cette clé privée permet à la personne de générer des signatures numériques. Toute personne peut vérifier cette signature à l'aide du certificat.

Abréviations

ASN.1	**Abstract Syntax Notation #1 :** langue de description pour la syntaxe de messages numériques. Des standards adaptés (par ex. X 690) sont utilisés pour le codage binaire des messages.
BER	**Basic Encoding Rules :** règles d'utilisation simple pour le codage binaire de messages numériques.
CA	**Certification Authority:** éditeur accrédité de certificats.
CAdES	**CMS Advanced Electronic Signatures :** un standard ETSI pour la normalisation de signatures basées sur CMS.
CMS	**Cryptographic Message Syntax :** format de messages basé sur la syntaxe ASN 1 (souvent appelé aussi PKCS#7)
CRL	**Certificate Revocation List :** liste de certificats révoqués publiée par l'organisme émetteur.
DER	**Distinguished Encoding Rules :** règles pour le codage binaire et sans équivoque de message numériques à base de BER.
EDIFACT	**Electronic Data Interchange For Administration, Commerce and Transport :** un standard international inter-branches pour l'échange électronique de données dans les communications commerciales.
DFF	**Département fédéral des finances :** cette autorité suisse informe de la structure, des missions et des thèmes actuels de l'administration financière.
ETSI	**European Telecommunications Standards Institute :** organisme européen pour la normalisation, notamment de signatures numériques.

HSM	**Hardware Security Module :** appareil pour l'enregistrement interne de clés privées ainsi que pour le cryptage et le décryptage.
ISO	**International Standards Organisation :** organisme international de normalisation, notamment de PDF et PDF/A. Dans l'ISO, la Suisse est représentée par l'Association Suisse de Normalisation (SNV).
LTV	**Long Term Validation :** l'enrichissement de signatures numériques par des données supplémentaires afin de les rendre vérifiables à long terme sans services en ligne. Les données supplémentaires sont constituées de la chaîne de confiance des certificats, du certificat de titulaire jusqu'au certificat racine de l'éditeur, ainsi que d'informations justifiant la validité des certificats au moment de la signature.
OASIS/DSS	**Organization for the Advancement of Structured Information Standards / Digital Signing Services :** un standard de l'organisme OASIS pour des services de signature à base de syntaxe XML.
OCSP	**Online Certificate Status Protocol :** protocole pour l'interrogation en ligne de l'état de validité d'un certificat donné à base de syntaxe ASN 1.
PAdES	**PDF Advanced Electronic Signature Profiles :** un standard ETSI pour la configuration de structures CMS et leur intégration dans des documents PDF.
PDF	**Portable Document Format :** un format de fichier standardisé par l'ISO (ISO-32000) pour l'échange de documents. Pour les utilisations fréquentes de PDF, il existe des sous-standards spécifiques, tels que PDF/A (ISO-19005) pour l'archivage de documents numériques.
PIN	**Personal Identification Number :** numéro de code secret nécessaire pour l'accès à un token.
PKCS	**Public Key Cryptography Standards :** une série de standards propriétaires de RSA Security Incorporated. Les normes les plus courantes sont : cryptage de signatures (PKCS#1), format de messages pour signatures (PKCS#7), interface vers token (PKCS#11) et format de fichier pour clés et certificats (PKCS#12).
QES	**Qualified Electronic Signature :** signature électronique qualifiée.
TLS	**Transport Layer Security :** évolution de Secure Sockets Layer (SSL), un protocole de cryptage hybride pour la transmission de données sécurisée sur Internet.

TSA	**Time Stamp Authority :** fournisseur accrédité de services d'horodatage.
TSP	**Time Stamp Protocol :** protocole pour l'interrogation en ligne d'horodatages cryptographiques à base syntaxe ANS.1.
XAdES	**XML Advanced Electronic Signatures :** un standard ETSI pour la création de signatures et leur intégration dans des données XML.
XML	**Extensible Markup Language :** format pour l'échange de données à structure hiérarchique et sous forme de texte entre machines.
X.509	Standard ITU-T pour une infrastructure Public Key permettant de créer des certificats numériques basés sur la syntaxe ASN.1.
X.690	Standard ITU-T pour le codage de messages numériques basés sur la syntaxe ASN.1. Basic Encoding Rules (BER), Canonical Encoding Rules (CER) et Distinguished Encoding Rules (DER).

A propos PDF Tools SA

Avec une clientèle comprenant plus de 4000 entreprises et organisations dans 60 pays, PDF Tools SA est le leader mondial des solutions logiciel et des composants de programmation pour les produits PDF et PDF/A.

Il y a plus de 15 ans, Hans Bärfuss, le fondateur et PDG de PDF Tools SA, a utilisé la technologie PDF dans les projets de ses clients. Depuis, PDF et PDF/A sont devenus des formats efficaces et très répandus, une norme ISO qui offre des possibilités d'application presque illimitées. En même temps, PDF Tools SA, qui a influencé de façon décisive l'élaboration de la norme ISO PDF/A pour l'archivage électronique à long terme, s'est imposée comme l'une des principales entreprises du marché de la technologie PDF.

En qualité de représentant suisse dans le comité ISO chargé des formats PDF/A et PDF, l'entreprise met directement son savoir au service du développement des produits. Le résultat est une gamme de produits haut de gamme et ultra performants, conformes à la devise 3-Heights™ de l'équipe de développement, composée d'ingénieurs qualifiés.

La gamme de produits de la société PDF Tools SA inclut des composants et des solutions, sans oublier des services. Les produits supportent l'ensemble du flux de documents, de la matière première à leur signature et leur archivage à long terme dans le respect des directives légales en passant par le processus de scannage. Un avantage des composants et solutions est leur large gamme d'interfaces, qui permet une intégration simple et sans aucune complication dans des environnements existants.

Les produits sont optimisés en permanence afin de répondre aux demandes croissantes du marché. Grâce à la prise en charge de l'assistance par les développeurs, ceux-ci détectent rapidement les tendances et les besoins des clients et apportent leur expertise dans la planification des extensions et des composants.

Tous les produits sont développés sur le site de la société PDF Tools SA, en Suisse. L'entreprise s'abstient délibérément d'externaliser les tâches de programmation afin de centraliser sur un même site l'ensemble du processus de développement.

Cette stratégie, validée par la popularité des produits de PDF Tools SA sur le marché, doit permettre de satisfaire les exigences en termes de technologie 3-Heights™ et de rester fidèle aux principes de l'entreprise. Parmi ses clients, on trouve des multinationales renommées de tous les secteurs d'activité. Pour l'équipe de développeurs, ce succès est le plus grand compliment possible et un véritable encouragement à poursuivre leur engagement dans l'univers PDF et PDF/A.

PDF Tools SA | Kasernenstrasse 1 | 8184 Bachenbülach | Suisse
Tél: +41 43 411 44 51 | Fax: +41 43 411 44 55
pdfsales@pdf-tools.com | www.pdf-tools.com

PDF-TOOLS.COM
Premium PDF Technology

Livre-blanc-Signature_Service-FR-20140630