Digitale Signaturen aus der Cloud
Grundlagen und Anwendung

PDF-TOOLS.COM
Premium PDF Technology

Inhaltsverzeichnis

Grundlagen der digitalen Signatur

Elektronische Dokumente und Unterschriften

Im Geschäftsverkehr werden zunehmend elektronische Dokumente mit einer Selbstverständlichkeit ausgetauscht und archiviert, so wie es für ihre Gegenstücke in Papier schon lange gemacht wird. Die Papierdokumente werden oft mit handschriftlichen Unterschriften versehen, welche den Dokumenten eine im geltenden Recht definierte Beweiskraft verleihen. Damit auch elektronische Dokumente mit der gleichen Beweiskraft unterschrieben werden können, hat die Gesetzgebung die elektronische Signatur geschaffen.

Die Vorteile der elektronischen Signatur in Geschäftsprozessen sind offensichtlich:

- Leistungs- und Qualitätssteigerung: Sie ermöglichen das automatisierte Unterschreiben von Dokumenten im Postausgang und das automatisierte Prüfen von Unterschriften im Posteingang.
- Rechtssicherheit: Sie ermöglichen eine Verbesserung der Beweiskraft, insbesondere der Nichtabstreitbarkeit (non-repudiation) der elektronisch übermittelten Daten.

In den Gesetzestexten werden die Eigenschaften einer elektronischen Signatur beschrieben. Die Texte geben jedoch keine Vorgaben für die technische Umsetzung. Für die technische Realisierung hat die Industrie eine Reihe von Standards entwickelt, welche den Begriff der digitalen Signatur definieren und deren Eigenschaften beschreiben.

Elektronische Signatur

Die Funktionen einer elektronischen Signatur sind:

- **Ersatz der handschriftlichen Unterschrift:** Die elektronische Signatur kann dem Erfordernis der handschriftlichen Unterschrift gleich gerecht werden wie die handschriftliche Unterschrift selbst, sofern die gesetzlichen Voraussetzungen dafür erfüllt sind.
- **Integritätsschutz:** Elektronische Signaturen haben einen „Versiegelungseffekt" für digitale Dokumente.
- **Authentizität:** Mit der elektronischen Signatur kann sichergestellt werden, dass die natürliche oder juristische Person identifiziert werden kann.
- **Autorisierung:** Rechte und Befugnisse können im Zertifikat festgelegt, verwaltet und damit der Person zugeordnet werden.

Gemäss dem Bundesgesetz über die Zertifizierungsdienste und anderer Anwendungen digitaler Zertifikate im Bereich der elektronischen Signatur (ZertES) gibt es zwei Arten von Signaturen:

- Die **fortgeschrittene elektronische Signatur** (Integritätsschutz und Identifikation des Signierenden) kann für natürliche wie juristische Personen eingesetzt werden und ist auf einen „Inhaber" zugeordnet. „Inhaber" kann eine Person, aber auch eine Maschine (Server) sein. Sie ist der eigenhändigen Unterschrift nicht gleichgestellt und eignet sich insbesondere zur Signatur von digitalen Dokumenten, bei denen keine gesetzlichen Formvorschriften vorliegen.

- Die **qualifizierte elektronische Signatur** (Erfüllung der Formvorschriften) ist eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit und auf einem zum Zeitpunkt der Erstellung gültigen qualifizierten Zertifikat, ausgestellt auf eine spezifische Person, beruht. Zudem muss das Zertifikat von einem anerkannten Anbieter von Zertifizierungsdiensten stammen. Der „Inhaber" ist immer eine natürliche Person.

Die Verordnung des EFD über elektronische Daten und Informationen (ElDI-V) regelt unter anderem die technischen, organisatorischen und verfahrenstechnischen Anforderungen an die elektronische Signatur zur Erzeugung und Überprüfung von mehrwertsteuerpflichtigen Rechnungen. Die Geschäftsbücherverordnung (GeBüV) schreibt vor, dass zur Aufbewahrung von Unterlagen, die auf veränderbaren Informationsträgern gespeichert werden, elektronische Signaturen und Zeitstempel zum Einsatz kommen können.

Für qualifizierte elektronische Signaturen mit Identitätsnachweis gibt es in der Schweiz für natürliche Personen die SuisseID.

Digitale Signatur

Die digitale Signatur ist, wie oben erwähnt, eine technische Umsetzung der elektronischen Signatur. Sie besteht aus Daten, welche man dem signierten Dokument zuordnet. Damit die in den Gesetzestexten geforderten Eigenschaften mit Sicherheit gewährleistet werden können, werden zur Erzeugung und Prüfung von digitalen Signaturen kryptografische Verfahren eingesetzt.

Zur Erzeugung einer digitalen Signatur werden die folgenden drei Dinge benötigt:

- Ein Zertifikat, ausgestellt auf den „Inhaber"
- Ein passender privater Schlüssel, welcher nur der „Inhaber" besitzt und geschützt aufbewahren muss
- Das zu unterschreibende Dokument

Mit der Signatursoftware kann der „Inhaber" damit eine digitale Signatur erzeugen. Der Empfänger des Dokuments kann nun die digitale Signatur prüfen. Dazu benötigt er die folgenden drei Dinge:

- Das signierte Dokument
- Das Zertifikat des „Inhabers". Dieses ist in der Regel im Dokument selbst eingebettet.
- Die digitale Signatur. Auch diese ist zusammen mit dem Zertifikat im Dokument eingebettet.

Dieser Vorgang lässt sich durch den Empfänger mit der Signatursoftware leicht ausführen.

Gemäss Gesetz benötigt der „Inhaber" für die Erzeugung qualifizierter Signaturen zusätzlich eine Signaturerstellungseinheit. Technisch gesehen, handelt es sich dabei um ein elektronisches Gerät, welches den privaten Schlüssel sicher verwahrt und von Zugriffen von aussen schützt. Als geeignete Geräte werden in der Praxis Smartcards, USB-Token und HSM (Hardware Security Module) eingesetzt. Diese Geräte enthalten, aus praktischen Gründen, neben dem privaten Schlüssel auch die „Inhaber"-Zertifikate und die Zertifikate des Ausstellers. Die Zertifikate müssen im Gegensatz zum privaten Schlüssel nicht geschützt werden. Sie dürfen publiziert werden, da sie für die Prüfung der digitalen Unterschrift benötigt werden.

Standards für digitale Dokumente und Signaturen

Die wichtigsten Dokumentenstandards für signierte, digitale Dokumente sind:

- ISO-19005 (PDF/A): Die ISO Norm 19005 definiert ein Dateiformat basierend auf PDF, genannt PDF/A. Das Format bietet einen Mechanismus, der elektronische Dokumente auf solche Weise darstellt, dass das visuelle Erscheinungsbild über lange Zeit erhalten bleibt, unabhängig von Werkzeugen und Systemen zur Herstellung, Speicherung und Reproduktion. Deshalb muss das Dokument alles enthalten, was für die einwandfreie Darstellung benötigt wird (Schriften, Farbprofile, etc.) und darf weder direkt noch indirekt auf externe Quellen verweisen.
- XML: Das Format wurde für den Austausch von hierarchisch strukturierten Daten in Textform zwischen Maschinen entwickelt. Die Spezifikation wird vom W3C (World Wide Web Consortium) publiziert.
- EDIFACT: Dies ist ein branchenübergreifender internationaler Standard für den Austausch elektronischer Daten im Geschäftsverkehr. EDIFACT ist einer von mehreren internationalen EDI-Standards. Verantwortlich für den EDIFACT-Standard ist eine UN-Einrichtung.

Das ETSI hat Standards für die Datenstrukturen von digitalen Signaturen entwickelt, die den Anforderungen für fortgeschrittene und qualifizierte elektronische Signaturen genügen. Dies sind die Standards:

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

Digitale Signaturen werden hauptsächlich für die folgenden beiden Anwendungen eingesetzt: Den Dokumentenaustausch und die Archivierung. Für die langfristige Aufbewahrung von Dokumenten muss die digitale Signatur zusätzlichen Anforderungen genügen. Die erste Anforderung betrifft die langfristige Gültigkeitsprüfung des Zertifikats. Sie wird als LTV (Long Term Validation) bezeichnet. Einerseits beschreiben die ETSI Standards Massnahmen gegen Angriffe auf kryptografische Verfahren, welche durch die stetig zunehmende Rechenleistung möglich werden. Andererseits beinhaltet eine digitale Signatur mit LTV-Eigenschaft zusätzlich die folgenden Daten:

- Trust Chain: Das Zertifikat des Herausgebers inkl. aller Zwischenzertifikate, welche zusammen eine Vertrauenskette bilden.
- OCSP-Response: Daten, welche die Gültigkeit des Zertifikats durch den Herausgeber zum Zeitpunkt der Unterschrift bescheinigen.

Für die LTV-Informationen muss zum Zeitpunkt der Erzeugung der Unterschrift der OCSP-Dienst zur Verfügung stehen. Für die spätere Prüfung wird er nicht mehr benötigt. Damit ist gewährleistet, dass diese Signaturen auch langfristig geprüft werden können.
Bei digitalen Signaturen ohne LTV-Eigenschaft verhält es sich umgekehrt. Für deren Erzeugung muss kein Dienst zur Verfügung stehen. Für die Prüfung muss jedoch der OCSP-Dienst zugänglich sein.

Die zweite Anforderung betrifft die Prüfung des Zeitpunkts der Unterschrift. Dafür muss die Signatur zusätzlich die folgenden Daten enthalten:

- TSP-Response: Daten von einem Zeitstempeldienst, welche den Zeitpunkt der Unterschrift bescheinigen.

Ohne Zeitstempel lässt sich der Zeitpunkt der Unterschrift nachträglich nicht mehr beweisen. Der TSP-Dienst muss immer zum Zeitpunkt der Unterschrift zur Verfügung stehen. Für die Prüfung ist kein TSP-Dienst erforderlich.

Aufgabe und Nutzen des Signaturdienstes aus der Cloud

Was ist die Aufgabe des Dienstes?

Die Hauptaufgabe eines Signaturdienstes ist die Erzeugung von vollständigen Signaturdaten aufgrund einer Signaturanforderung des Signaturclients. Die Signaturanforderung wird aufgrund des zu signierenden Dokuments einerseits und der Authentifizierung des Kunden andererseits erzeugt. Der Dienst sendet die Signaturdaten zurück an den Signaturclient, wo sie dann mit dem Ursprungsdokument zum signierten Dokument verknüpft werden.

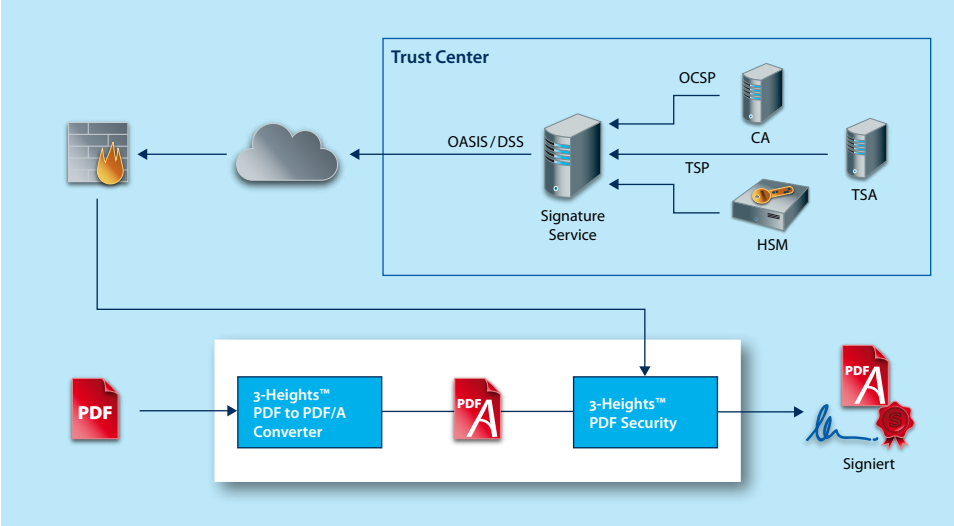


Abbildung 1: Ein zentraler Dienst für die Erzeugung und Prüfung von digitalen Signaturen

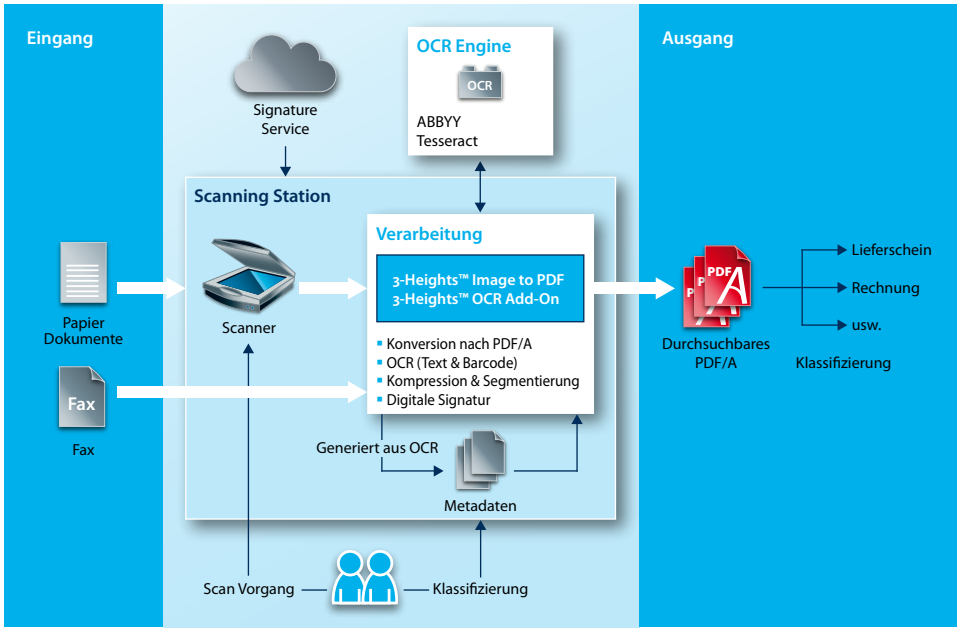
Das Dokument selbst wird nicht an den Dienst übermittelt, sondern ein Hashwert (eine Art Fingerabdruck) davon. Vom Hashwert kann nicht auf den Inhalt des Dokuments geschlossen werden. Damit bleibt die Vertraulichkeit des Dokuments in allen denkbaren Anwendungen wie Patientenakten, Bankdaten, Konstruktionszeichnungen usw. gewährleistet.
Die gegenseitige Authentifizierung des Clients und des Servers und die Transaktion erfolgt über sichere Verbindungen (TLS). Die sichere Verbindung wird durch je ein Client- und Serverzertifikat geschützt. Durch diese Massnahme kann der Dienst die Signaturen eindeutig einem Kunden zuordnen.
Der Dienst bewirtschaftet für jeden Kunden die notwendigen privaten Schlüssel und Zertifikate in einer sicheren und vertrauenswürdigen Umgebung. Damit erzeugt der Dienst die individuellen Signaturen. Unterstützt werden fortgeschrittene Organisationszertifikate nach ZertES und ElDI-V sowie qualifizierte Zertifikate auf der Basis der SuisseID. Die Zertifikate werden vom Dienst automatisch erneuert, wenn ihre Gültigkeitsdauer abläuft.
Der Dienst kann wahlweise auch langfristig gültige Signaturen (LTV) erzeugen sowie einen Zeitstempel integrieren.
Durch den redundanten Aufbau des Dienstes wird eine hohe Verfügbarkeit gewährleistet. Betrieben wird der Dienst von einem akkreditierten Herausgeber von Zertifikaten, welcher die Einhaltung aller notwendigen Regularien garantiert.

Wo wird der Dienst eingesetzt?

Der Signaturdienst kann in der Unternehmung überall dort eingesetzt werden, wo digitale Signaturen erzeugt werden sollen oder müssen. Einige typische Beispiele sind nachfolgend beschrieben.

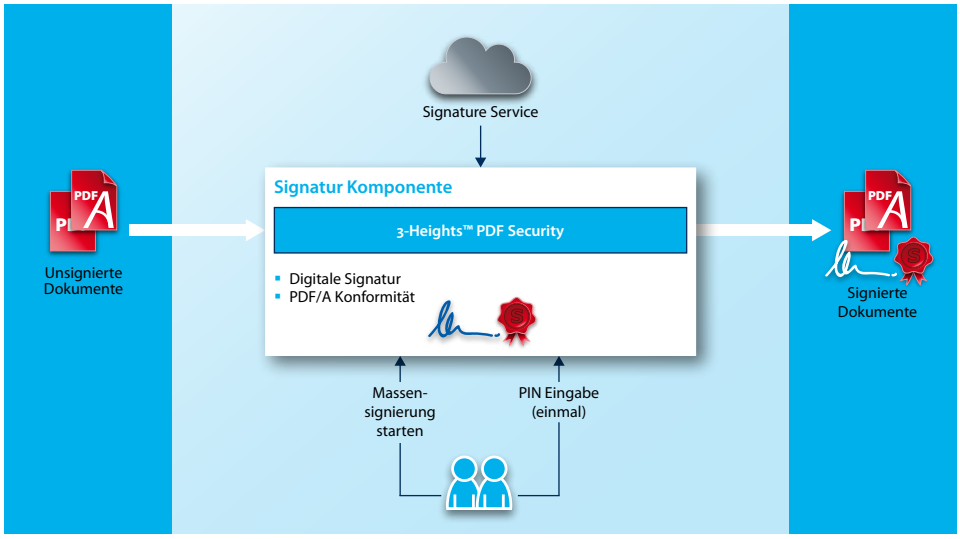
Integritätsschutz im Posteingang

Papierdokumente, welche im Posteingang einer Unternehmung anfallen, können gescannt, nach PDF/A umgewandelt und mit einem Zeitstempel signiert werden. Gleiches gilt für den Empfang des gesamten FAX-Verkehrs zwischen der Unternehmung und seinen Geschäftspartnern. Durch diese Massnahme wird die Integrität der eingegangenen Dokumente in den nachfolgenden Prozessen gewährleistet.



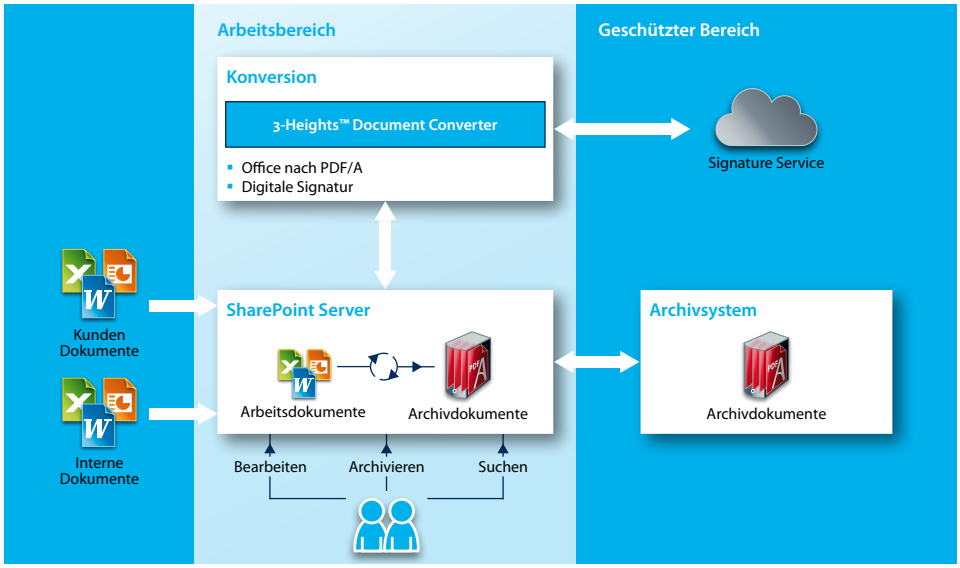
ElDI-V konforme Dokumente im Postausgang

Im Postausgang werden unsignierte Dokumente, wie beispielsweise Rechnungen in PDF/A umgewandelt und mit einer fortgeschrittenen und ElDI-V konformen Signatur versehen.



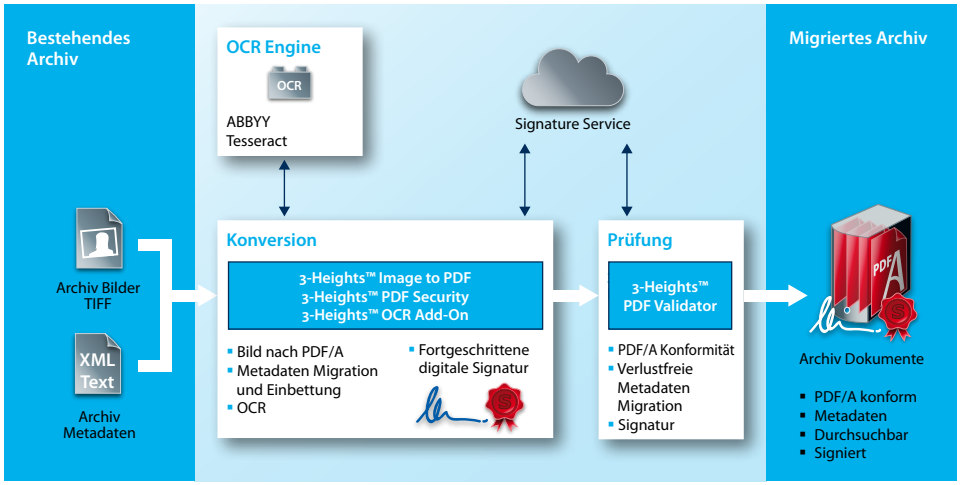
Archivierung von finalen Arbeitsdokumenten

Arbeitsdokumente, welche in ihrem Lebenszyklus den finalen Zustand erreicht haben und archiviert werden sollen, werden in PDF/A konvertiert und gleichzeitig digital signiert. Der Bearbeitungsprozess der Dokumente wird oft mit einem SharePoint Server unterstützt. Mittels einer Erweiterung kann die Konversion in PDF/A und das Aufbringen einer digitalen Signatur aus der Cloud automatisiert werden.



Archivmigration mit Nachvollziehbarkeit

Ein bestehendes Archiv mit TIFF, JPEG und anderen Bildern sowie getrennten Indexdaten werden in PDF/A umgewandelt und gleichzeitig mit einer Signatur aus der Cloud versehen. Durch die Signatur wird die Nachvollziehbarkeit der Migration gewährleistet.



Was sind die Vorteile eines Signaturdienstes?

Der Signaturdienst bietet gegenüber eigenständigen Lösungen deutliche wirtschaftliche und technische Vorteile. Hier sind die wichtigsten zusammengefasst.

Schnelle Einführungszeit	Der Aufbau einer Signaturinfrastruktur mit Server und Clients in einer Unternehmung braucht Know-how, Schulung des Personals und Zeit. Die Nutzung des Signaturdienstes reduziert diese Zeit erheblich, da der Aufbau einer Serverinfrastruktur entfällt und nur noch die wesentlich einfacheren Signaturclients eingeführt werden müssen.
Reduktion der Investitions- und Betriebskosten	Anschaffungen wie HSMs, Zertifikate und Tokens für jeden Mitarbeiter entfallen. Auch die Kosten für den Betrieb von Servern und die Erneuerung von Zertifikaten entfallen. Abgelaufene Zertifikate können teuer werden, wenn sie zum Betriebsstillstand führen.
Allgegenwärtigkeit, Ortsunabhängigkeit, keine Tokens	Mit dem Signaturdienst können Dokumente und Daten überall unterschrieben werden, ohne dass Tokens und Kartenleser zur Verfügung stehen müssen. Mit der zunehmenden Verbreitung von mobilen Geräten ist dies oft die einzige Möglichkeit, um elektronische Unterschriften leisten zu können. Die Unterschriften können über das Netzwerk, beispielsweise von Heimarbeitsplätzen, geleistet werden.
Compliance / Regularien	Der Dienst wird von einem akkreditierten Herausgeber von Zertifikaten betrieben, welcher die Einhaltung aller notwendigen Regularien (ZertES) garantiert. Der Dienst erzeugt sowohl fortgeschrittene Signaturen nach EIDI-V als auch qualifizierte Signaturen entsprechend der SuisseID.
Hohe Verfügbarkeit	Der Betreiber des Dienstes garantiert durch die redundante Auslegung der Hardware eine hohe Verfügbarkeit des Dienstes.
Hohe Qualität, Konformität mit Standards	Der Anbieter des Dienstes gewährleistet die laufende Weiterentwicklung und Anpassung der digitalen Signaturen an die neusten technischen Industriestandards (ISO, ETSI).
Sicherheit	Der Dienst bewirtschaftet private Schlüssel und Zertifikate in einer sicheren und vertrauenswürdigen Umgebung. Die Zertifikate werden vom Dienst automatisch erneuert, wenn ihre Gültigkeitsdauer abläuft.
Vertraulichkeit	Mit dem Signaturdienst können Daten und Dokumente der höchsten Vertraulichkeitsstufe signiert werden, da die Daten die Unternehmung für den Signaturvorgang niemals verlassen.
Geringere Angreifbarkeit	Die Verwendung des Dienstes erhöht die Robustheit von Firewall-Angriffen, da für den Dienst nur ein einziges, XML-basiertes Protokoll eingesetzt wird. Eigenständige Lösungen benötigen Zugriff auf mehrere, sicherheitstechnisch aufwändigere OCSP- und TSP-Protokolle. Zudem ist die Verbindung zwischen dem Signaturclient und dem Signaturdienst durch gegenseitige TLS-Authentifizierung geschützt.
Skalierbarkeit	Der Dienst kann einzelne bis zu mehreren Millionen Signaturanforderungen pro Tag bewältigen.

Tabelle 2: Die Vorteile eines Signaturdienstes aus der Cloud

Software für die Nutzung des Signaturdienstes aus der Cloud

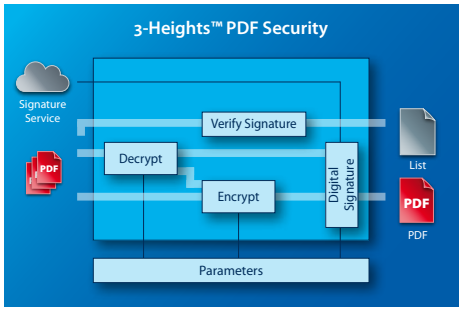
Aufgabe des Signaturclients

Der Signaturclient ist eine Softwarekomponente, welche Daten und Dokumente mithilfe des Signaturdienstes aus der Cloud signieren kann. Der Signaturclient kommuniziert über das OASIS/DSS Protokoll mit dem Dienst. Er erstellt korrekte Signaturanforderungen, überprüft die Antwort und bettet das Resultat in die zu signierenden Daten oder das zu signierende Dokument ein.

Der Signaturclient ist Bestandteil der im Folgenden beschriebenen Produkte:

3-Heights™ PDF Security

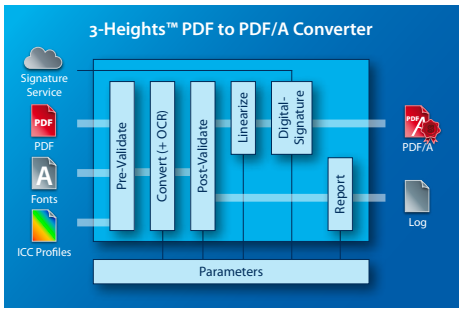
Die 3-Heights™ PDF Security Komponente bietet zwei Hauptfunktionen an: Die Verschlüsselung und die digitale Signatur für PDF-Dokumente. Der Funktionsteil „digitale Signatur" beinhaltet:



- PDF und PDF/A konform signieren (PAdES Part 2)
- Signaturen in einem PDF-Dokument auf Gültigkeit überprüfen
- Benutzersignaturen, Autorensignaturen (MDP) und Zeitstempelsignaturen
- Einfache, fortgeschrittene oder qualifizierte elektronische Signatur
- Langzeit Signatur (LTV) mit eingebetteter Vertrauenskette, Zeitstempel und Prüfinformation zur Zertifikatsgültigkeit
- Unterstützung von Signaturdiensten aus der Cloud via OASIS/DSS und Massensignaturgeräten (HSM) via PKCS#11
- Revisionen auflisten und wiederherstellen
- Unsichtbare und sichtbare Signaturen
- Gestaltung der sichtbaren Signatur

3-Heights™ PDF to PDF/A Converter

Der 3-Heights™ PDF to PDF/A Converter baut auf der 3-Heights™ PDF Security Komponente auf und bietet zusätzlich die folgenden Funktionen an:



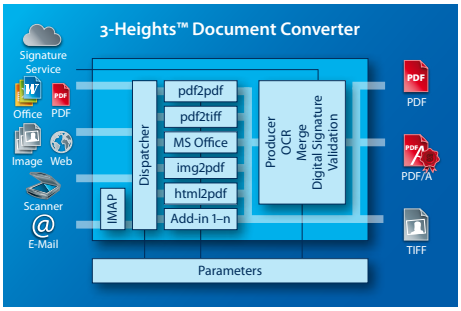
- PDF Dokumente nach PDF/A-1, PDF/A-2 oder PDF/A-3 konvertieren
- Eingehende Dokumente validieren
- Ausgehende Dokumente validieren
- Automatisches und konfigurierbares Einbetten von Farbprofilen bei Verwendung von geräteabhängigen Farbräumen

- Automatisches und konfigurierbares Einbetten von Schriften: Als Untergruppe einbetten, um die Dateigrösse klein zu halten oder gesamte Schrift einbetten, um ein späteres Editieren der Datei zu ermöglichen
- Automatische Erzeugung von Metadaten oder deren Einbettung aus externen Quellen
- Anbindung einer OCR Engine (Abbyy oder Tesseract) für Texterkennung; den erkannten Text optional als Textdatei speichern

3-Heights™ Document Converter

Der 3-Heights™ Document Converter ist eine unternehmensweit einsetzbare Lösung für die Konvertierung aller gängigen Dateiformate nach PDF/A, PDF und TIFF. Die häufigste Anwendung ist die Umwandlung von Microsoft Office Dokumenten zu PDF oder PDF/A für die Archivierung mit dem optionalen Aufbringen einer Signatur aus der Cloud.
Es werden damit verschiedenste Anforderungen im Bereich Konvertierung adressiert, insbesondere:

- MS Office Dokumente in PDF/A archivieren
- Bilder wie TIFF, JPEG und andere Bildformate archivieren
- Webseiten archivieren
- E-Mails archivieren
- Die firmenweite Formatvielfalt vereinheitlichen



Schnittstellen zur Applikationsintegration

Für die Integration von Arbeitsstationen und Server Computern, die Applikationen betreiben, welche die 3-Heights™ Produkte nutzen wollen, gibt es eine Reihe von Schnittstellen. Die Wichtigsten sind:

- **Webservice:** Der Webdienst erlaubt das Signieren von Dokumenten aus dem Intranet, einer Applikation oder von einem mobilen Gerät.
- **Programmierschnittstelle (API):** Diese Komponente ermöglicht die programmatische Integration des Dienstes in Applikationen. Sie bietet Schnittstellen für Java, C, COM und .NET Technologien an. Die Komponente ist auch für andere Plattformen wie Linux, Sun OS, AIX, HP-UX, Mac OS/X etc. verfügbar.
- **Command Line Tool:** Dieses Werkzeug ist ein eigenständiges Programm, welches ohne weitere Voraussetzungen direkt auf der Befehlszeile ausgeführt werden kann. Damit lassen sich Abläufe mithilfe der Befehlssprache (Shell Command) automatisieren, ohne dass eine Entwicklungsumgebung benötigt wird. Das Befehlszeilenprogramm ist auch für andere Plattformen wie Linux, Sun OS, AIX, HP-UX, Mac OS/X etc. verfügbar.

Glossar

Begriffe

Hash	Ein Hashwert (kurz: Hash) ist eine Zahl, welche aus einer beliebig grossen Menge von Daten wie Dokumente, Zertifikate, Nachrichten, usw. berechnet wird. Diese Zahl ist oft viel kürzer als die ursprünglichen Daten (ca. 20 Byte). Der Hashwert hat die Eigenschaft, dass er für gleiche Daten gleich ist und für unterschiedliche Daten mit grosser Wahrscheinlichkeit eindeutig ist. Zudem lässt sich vom Hashwert nicht mehr auf die ursprünglichen Daten zurückschliessen. Für die Berechnung werden Hash-Algorithmen verwendet wie SHA-1 oder SHA-2.
Schlüssel	Das Zertifikat enthält einen öffentlichen Schlüssel (Public Key), der zur Prüfung der Signatur verwendet wird. Der öffentliche Schlüssel muss zu einem privaten Schlüssel (Private Key) passen, der zur Erzeugung der Signatur verwendet wird und an einem sicheren Ort aufbewahrt werden muss.
Signatur, Signieren	Daten, mit welchen die Integrität und Authentizität eines Dokuments sichergestellt werden kann. Die Signatur wird im Wesentlichen so hergestellt: Von den zu signierenden Daten wird der Hashwert gebildet und dieser mit dem privaten Schlüssel verschlüsselt. Die Signatur wird zusammen mit Zertifikaten und Prüfinformationen in eine CMS-Nachricht gepackt und wahlweise in das signierte Dokument eingebettet.
Token	Ein „Behälter" (Teil der HSM, USB-Stick, Smartcard usw.), der private Schlüssel enthält und vor unberechtigtem Zugriff schützt. Oft enthält das Token aus praktischen Gründen auch passende Zertifikate und öffentliche Schlüssel, welche nicht geschützt werden müssen.
Verifikation, Verifizieren	Eine Signatur wird wie folgt überprüft: Die Signatur wird aus dem Dokument extrahiert und mit dem öffentlichen Schlüssel entschlüsselt. Daraus erhält man den Hashwert der Daten zum Zeitpunkt der Unterschrift. Danach wird der Hashwert der signierten Daten neu gebildet und mit dem Hashwert aus der Signatur verglichen. Stimmen die beiden Werte überein, so sind die Daten nicht verändert worden und vertrauenswürdig (Integritätsprüfung). Aus der Signaturnachricht kann auch das Zertifikat extrahiert und damit der Unterzeichnete identifiziert werden (Identitätsprüfung). Weitere Prüfungen in Bezug auf Zertifikatsgültigkeit und Zeitstempel sind je nach Art der Signatur möglich.

Verschlüsselung	Daten werden verschlüsselt, damit aussenstehende Personen ihre Bedeutung nicht erschliessen können. Für die Kommunikation zwischen Absender und Empfänger wird vom Empfänger ein Schlüsselpaar, bestehend aus einem privaten und öffentlichen Schlüssel, erzeugt. Wenn der Absender nun die Daten mit dem öffentlichen Schlüssel verschlüsselt, kann nur der Empfänger die Daten entschlüsseln, da er der alleinige Besitzer des privaten Schlüssels bleibt. Für die Verschlüsselung werden Algorithmen wie RSA mit Schlüssellängen von aktuell 2048 Bit verwendet. Auf dieser Technik basieren die gebräuchlichen Verfahren für digitale Signaturen.
Zertifikat	Ein Zertifikat ist eine elektronische Bescheinigung der Identität einer natürlichen oder juristischen Person. Das Zertifikat enthält zudem einen öffentlichen Schlüssel zu dem die Person einen passenden privaten Schlüssel besitzt. Mit diesem privaten Schlüssel kann die Person digitale Signaturen erzeugen. Jede beliebige Person kann diese Signatur mithilfe des Zertifikats überprüfen.

Abkürzungen

ASN.1	**Abstract Syntax Notation #1:** Beschreibungssprache für die Syntax von digitalen Nachrichten. Für die binäre Kodierung der Nachrichten werden dafür geeignete Standards eingesetzt (z. B. X.690).
BER	**Basic Encoding Rules:** Einfach zu handhabende Regeln zur binären Kodierung von digitalen Nachrichten.
CA	**Certification Authority:** Akkreditierter Herausgeber von Zertifikaten.
CAdES	**CMS Advanced Electronic Signatures:** Ein ETSI Standard für die Normung von CMS basierten digitalen Signaturen.
CMS	**Cryptographic Message Syntax:** Nachrichtenformat für digitale Signaturen basierend auf der ASN.1 Syntax (auch oft als PKCS#7 bezeichnet).
CRL	**Certificate Revocation List:** Vom Aussteller publizierte Liste von zurückgezogenen Zertifikaten.
DER	**Distinguished Encoding Rules:** Regeln zur binären und eindeutigen Kodierung von digitalen Nachrichten basierend auf BER.

EDIFACT	**Electronic Data Interchange For Administration, Commerce and Transport:** Ein branchenübergreifender internationaler Standard für den Austausch elektronischer Daten im Geschäftsverkehr.
EFD	**Eidgenössisches Finanzdepartement:** Die Schweizer Behörde informiert über Struktur, Aufgaben und über aktuelle Themen der Finanzverwaltung.
ETSI	**European Telecommunications Standards Institute:** Europäische Organisation für die Normung u.a. von digitalen Signaturen.
HSM	**Hardware Security Module:** Gerät zur sicheren Speicherung von privaten Schlüsseln sowie zur Verschlüsselung und Entschlüsselung.
ISO	**International Standards Organisation:** Internationale Organisation für die Normung u.a. von PDF und PDF/A. Die Schweiz ist in der ISO durch die Schweizerische Normenvereinigung (SNV) vertreten.
LTV	**Long Term Validation:** Die Anreicherung von digitalen Signaturen durch zusätzliche Daten, damit die langfristige Überprüfbarkeit ohne online Dienste möglich wird. Die zusätzlichen Daten bestehen aus der Vertrauenskette der Zertifikate vom Inhaberzertifikat bis zum Wurzelzertifikat des Herausgebers sowie Informationen, welche die Gültigkeit der Zertifikate zum Zeitpunkt der Unterschrift bescheinigen.
OASIS/DSS	**Organization for the Advancement of Structured Information Standards / Digital Signing Services:** Ein Standard der OASIS-Organisation für Signaturdienste basierend auf der XML Syntax.
OCSP	**Online Certificate Status Protocol:** Protokoll zur Online-Abfrage des Gültigkeitsstatus eines bestimmten Zertifikats basierend auf der ASN.1 Syntax.
PAdES	**PDF Advanced Electronic Signature Profiles:** Ein ETSI Standard für den Aufbau von CMS Signaturen und deren Einbettung in PDF Dokumenten.
PDF	**Portable Document Format:** Ein von ISO standardisiertes Dateiformat (ISO-32000) für den Dokumentenaustausch. Für häufige Anwendungen von PDF existieren spezielle Unterstandards, wie PDF/A (ISO-19005) für die Archivierung von digitalen Dokumenten.
PIN	**Personal Identification Number:** Geheime Kennzahl, die für den Zugriff auf ein Token benötigt wird.

PKCS	**Public Key Cryptography Standards:** Eine Reihe von proprietären Standards der RSA Security Incorporated. Die gebräuchlichsten Normen sind: Verschlüsselung von Signaturen (PKCS#1), Nachrichtenformat für Signaturen (PKCS#7), Schnittstelle zu Token (PKCS#11) und Dateiformat für Schlüssel und Zertifikate (PKCS#12).
QES	**Qualified Electronic Signature:** Qualifizierte elektronische Signatur.
TLS	**Transport Layer Security:** Weiterentwicklung von Secure Sockets Layer (SSL), einem hybriden Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
TSA	**Time Stamp Authority:** Akkreditierter Anbieter von Zeitstempeldiensten.
TSP	**Time Stamp Protocol:** Protokoll für die Online-Abfrage von kryptographischen Zeitstempeln basierend auf der ASN.1 Syntax.
XAdES	**XML Advanced Electronic Signatures:** Ein ETSI Standard für die Erzeugung von Signaturen und deren Einbettung in XML-Daten.
XML	**Extensible Markup Language:** Format für den Austausch von hierarchisch strukturierten Daten in Textform zwischen Maschinen.
X.509	ITU-T Standard für eine Public Key Infrastruktur zum Erstellen digitaler Zertifikate basierend auf der ASN.1 Syntax.
X.690	ITU-T Standard für die Kodierung von digitalen Nachrichten basierend auf der ASN.1 Syntax: Basic Encoding Rules (BER), Canonical Encoding Rules (CER) und Distinguished Encoding Rules (DER).

Über PDF Tools AG

Die PDF Tools AG zählt weit über 4000 Unternehmen und Organisationen in 60 Ländern zu ihren Kunden und ist damit ein weltweit führender Hersteller von Softwarelösungen und Programmierkomponenten für PDF und PDF/A Produkte. Zusätzlich werden die Komponenten und Werkzeuge des Softwareherstellers über ein internationales OEM-Partnernetzwerk von Tausenden Benutzern auf der Welt täglich angewendet.

Vor mehr als 15 Jahren hat Dr. Hans Bärfuss, der Gründer und CEO der PDF Tools AG, PDF Technologie in Kundenprojekten eingesetzt. Das PDF und PDF/A Format haben sich seither zu einem mächtigen, weit verbreiteten Format und ISO Standard mit nahezu unbeschränkten Anwendungsmöglichkeiten entwickelt. Auch die PDF Tools AG wurde in dieser Zeit zu einem der wichtigsten Unternehmen im Markt für PDF Technologie und hat den PDF/A ISO Standard für die elektronische Langzeitarchivierung massgeblich mitgeprägt.
Mit den Produkten der PDF Tools AG lassen sich PDF-Dokumente anzeigen, drucken, in Bildformate konvertieren (oder umgekehrt), analysieren, reparieren, optimieren, validieren, zusammensetzen, zerlegen, schützen, stempeln, digital signieren oder auch erweitern.
Als Schweizer Vertreter im ISO-Komitee für PDF/A und PDF, lässt das Unternehmen sein Wissen direkt in die Produkteentwicklung einfliessen. Es entstehen damit qualitativ hochwertige Produkte mit einer effizienten Leistungsfähigkeit - ganz nach dem 3-Heights™ Motto des Entwicklungsteams, welches sich aus qualifizierten Ingenieuren zusammensetzt.
Das Portfolio von PDF Tools AG erstreckt sich von Komponenten, Services bis hin zu Lösungen. Die Produkte unterstützen den gesamten Dokumentenfluss vom Rohmaterial, über Scanningprozesse bis hin zur Signierung und der Archivierung in einem rechtlich konformen Langzeitarchiv. Ein Vorteil der Komponenten und Lösungen ist die breite Palette von Schnittstellen, welche eine reibungslose und einfache Integration in bestehende Umgebungen gewährleistet.
Laufend werden die Produkte aufgrund der wachsenden Anforderungen des Marktes weiterentwickelt. Da der Support von den Entwicklern selbst übernommen wird, erkennen diese Trends und Bedürfnisse der Kunden rasch und setzen das Wissen bei der Planung für Erweiterungen und Komponenten ein.
Sämtliche Entwicklungen erfolgen innerhalb der PDF Tools AG in der Schweiz. Das Unternehmen lagert bewusst keine Programmierung aus, um den gesamten Entwicklungsprozess zentral an einem Standort zu haben. Dies um den eigenen Ansprüchen zu der 3-Heights™-Technologie und der Erfüllung des Firmen-Credos gerecht zu werden. Der Erfolg der Produkte im Markt bestätigt PDF Tools AG diesen Ansatz.
Zu den Kunden des Unternehmens zählen namhafte, weltweit tätige Unternehmen aus sämtlichen Branchen. Das ist das schönste Kompliment und die beste Motivation für das Team, einen wichtigen Beitrag in der PDF und PDF/A Welt zu leisten.

PDF Tools AG | Kasernenstrasse 1 | 8184 Bachenbülach | Switzerland
Tel.: +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

Whitepaper-Signature_Service-DE-20140520