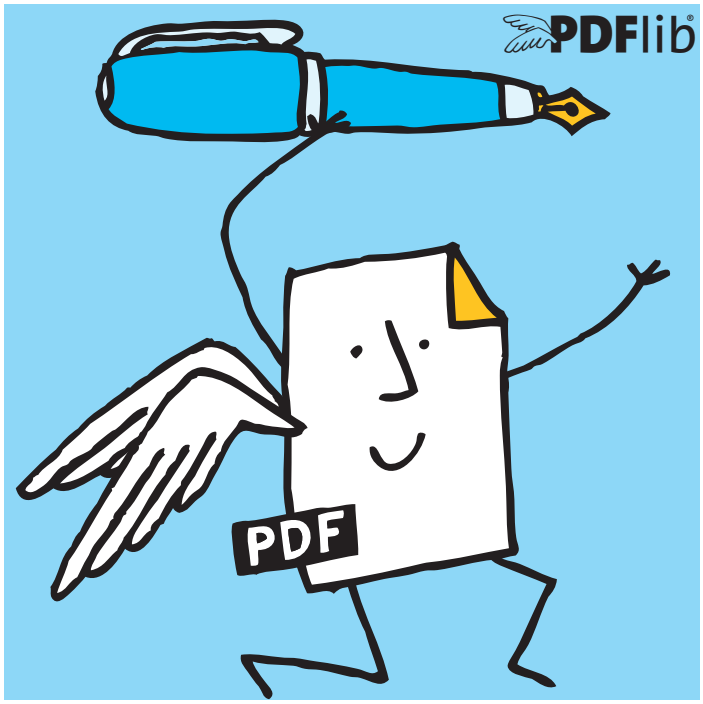


Datenblatt

PDFlib PLOP DS 5.4

Linearisierung, Optimierung, Sicherheit, Digitale Signaturen für PDF

Was ist PDFlib PLOP DS?

PDFlib PLOP DS basiert auf PLOP, einem vielseitigen Tool zur Linearisierung, Optimierung, Reparatur, Analyse sowie Ver- und Entschlüsselung von PDF-Dokumenten. PLOP DS bietet darüber hinaus die Möglichkeit, PDF-Dokumente digital zu signieren. Es unterstützt die neuesten Standards der Signaturtechnik einschließlich PDF 2.0 gemäß ISO 32000-2 und PAdES-Signaturen, die von der europäischen eIDAS-Verordnung gefordert werden..

Digitale Signaturen mit PDFlib PLOP DS

PDFlib PLOP DS erstellt PDF-Signaturen, die sich mit Adobe Reader, Acrobat oder jedem anderen Validierer prüfen lassen, der PDF-Signaturen unterstützt. PLOP DS liest die digitale ID des Unterzeichners (also Zertifikat und den zugehörigen privaten Schlüssel) aus dem Arbeitsspeicher, einer Datei, dem Windows-Zertifkatspeicher oder einem sicheren Hardware-Token. Mit dieser ID erstellt PLOP DS eine kryptografische Signatur für das PDF-Dokument. Die Signatur kann mit Verschlüsselung kombiniert werden.

PDF-Signatureigenschaften

- Erstellung von Signaturen in bestehenden PDF-Signaturfeldern oder Generierung neuer Felder für die Signatur. Die Signaturen können an einer bestimmten Stelle auf der Seite sichtbar oder unsichtbar sein.
- Visualisierung der digitalen Signatur durch Import eines Logos, den Scan einer manuellen Unterschrift oder eine andere Darstellung als PDF-Seite.
- Erstellung zertifizierter PDF-Dokumente (auch Zertifizierungs- oder Autorensignatur genannt), die Dokumentänderungen ermöglichen. So können zum Beispiel Formularfelder ausgefüllt werden, ohne die Signatur ungültig zu machen.
- Validierungsinformationen können gemäß ISO 32000-1 direkt in der Signatur gespeichert werden oder in einem Document Security Store (DSS) gemäß ISO 32000-2 und PAdES Teil 4.
- Signaturen können in einem inkrementellen PDF-Update angewendet werden, um vorhandene Signaturen und Dokumentstruktur zu bewahren, oder durch Neuerstellung der Dokumentstruktur zur Optimierung und Verschlüsselung.

PDF-Versionen und -Standards

PLOP DS unterstützt alle relevanten PDF-Versionen und -Standards:

- PLOP verarbeitet alle PDF-Versionen bis PDF 1.7 (ISO 32000-1) einschließlich Extension Level 8 und PDF 2.0 (ISO 32000-2).
- PLOP DS berücksichtigt die Archivierungsstandards PDF/A-1/2/3 (ISO 19005): ist das Eingabedokument PDF/A-konform, so ist dies auch für die Ausgabe gewährleistet. Auch XMP Extension Schemas gemäß PDF/A werden von PLOP DS vollständig unterstützt.
- Entsprechend unterstützt PLOP DS die Standardreihe PDF/X-3/4/5 (ISO 15930) für die Druckproduktion, den Standard für variablen und Transaktionsdruck PDF/VT-1 (ISO 16612-2) sowie PDF/UA-1 (ISO 14289) für barrierefreie PDF-Dokumente.

Weitere PDF-Verarbeitungsfunktionen

Zusätzlich zu digitalen Signaturen enthält PDFlib PLOP DS auch die Funktionen des Basisprodukts PDFlib PLOP:

- Optimierung: Die Dateigröße eines PDF-Dokuments ohne Qualitätsverlust verringern.
- Kennwortschutz: PDF-Dokumente verschlüsseln und entschlüsseln sowie Beschränkungen wie »Drucken nicht zulässig« oder »Textextraktion nicht zulässig« hinzufügen oder entfernen.
- Zertifikatsicherheit: Verschlüsseln von PDF-Dokumenten für eine geschlossene Gruppe von Empfängern, die durch ihre digitalen Zertifikate identifiziert werden.
- Reparaturmodus: Beschädigte PDF-Dokumente erkennen und die Probleme nach Möglichkeit automatisch beheben.
- PDF-Analyse: Beliebige Eigenschaften von PDFs mit der pCOS-Schnittstelle abfragen.
- Dokument-Infofelder: Abfragen, Hinzufügen oder Ersetzen von Infofeldern.
- XMP-Metadaten: XMP hinzufügen und mit den Dokument-Infofeldern synchronisieren.

Weitere Informationen zum Basisprodukt PLOP finden Sie im separaten Datenblatt für PLOP.

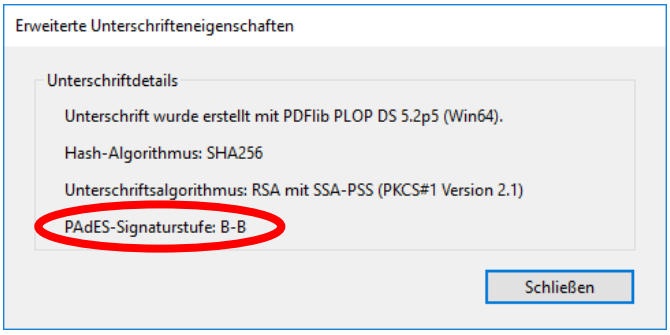
Signaturfunktionen

Signaturstandards

- CMS-basierte Signaturen gemäß PDF 1.7 (ISO 32000-1)
- Signaturen für Langzeitvalidierung (Long-Term Validation, LTV) gemäß PDF 2.0 (ISO 32000-2)
- PAdES (ETSI TS 102 778 Teil 2, 3 und 4, ETSI EN 319 142) und CAdES (ETSI TS 101 733) zur Erstellung qualifizierter Signaturen gemäß eIDAS-Verordnung

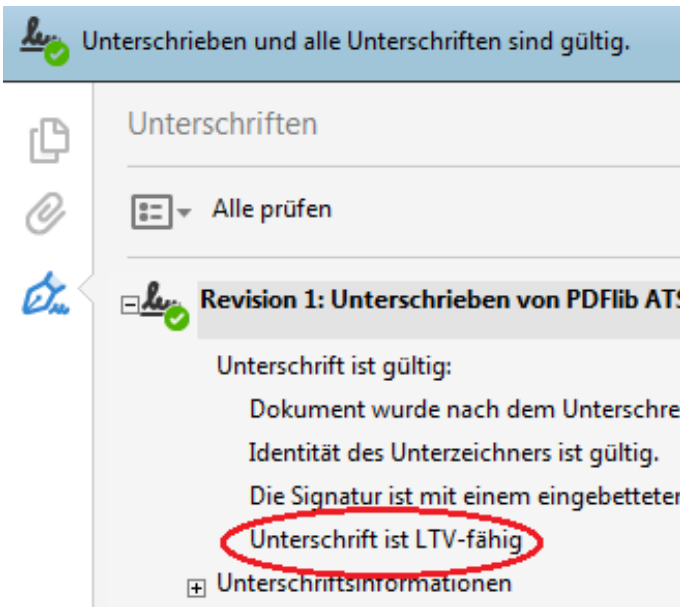
PAdES-Signaturstufen

- Einfache Signatur (Stufe B-B)
- Signatur mit Zeit (Stufe B-T)
- Signatur mit Material für die Langzeitvalidierung (Stufe B-LT)
- Signatur mit Langzeitverfügbarkeit und Integrität von Validierungsmaterial (Stufe B-LTA): Voraussetzung für eIDAS
- Einfache elektronische Signatur (BES) und explizit Richtlinien-basierte elektronische Signatur (EPES) gemäß PAdES Teil 3



Zeitstempel

- Anfordern eines Zeitstempels von einer vertrauenswürdigen Zeitquelle (Timestamp Authority, TSA) gemäß RFC 3161, RFC 5816 und ETSI EN 319 422 sowie Einbetten in die Signatur. Die Daten der TSA können aus dem Zertifikat entnommen werden, um Zeitstempel ohne weitere Konfiguration zu erstellen.
- Erstellen von Zeitstempeln auf Dokumentebene gemäß ISO 32000-2 und PAdES Teil 4. Ein Zeitstempel auf Dokumentebene garantiert den Zustand des Dokuments auch ohne personenbasierte Signatur.



Kryptografische Details der Signatur

- Signaturen gemäß den RSA- und DSA-Verfahren sowie Elliptic Curve Digital Signature Algorithm (ECDSA). Für RSA werden die Encoding-Methoden PKCS#1 v1.5 und PKCS#1 v2.1 (PSS) unterstützt.
- Starke Signatur- und Hashfunktionen.
- Einbindung der vollständigen Zertifikatskette in die erzeugten Signaturen. Das bedeutet, dass Signaturen mit Zertifikaten einer CA (Certificate Authority) auf der Adobe Approved Trust List (AATL) oder European Union Trust List (EUTL) in Acrobat und Adobe Reader ohne weitere Konfiguration auf Client-Seite validiert werden können.
- Einbindung von OCSP-Antworten (Online Certificate Status Protocol gemäß RFC 2560 und RFC 6960) und Zertifikatsperrlisten (Certificate Revocation Lists, CRL gemäß RFC 3280) als Sperrinformationen für die Langzeitvalidierung (Long-Term Validation, LTV).

Signatur-Engines

PLOP DS unterstützt verschiedene kryptografische Engines, also Komponenten zur Generierung der digitalen Signaturen:

- Die integrierte Engine implementiert die erforderlichen kryptografischen Funktionen direkt in PLOP DS ohne externe Abhängigkeiten. Die integrierte Engine unterstützt Software-basierte digitale IDs in den Zertifikatformaten PKCS#12 und PFX.

- PLOP DS kann kryptografische Tokens über die PKCS#11-Schnittstelle anbinden. Zur Signaturerstellung können damit digitale IDs auf Smartcards, USB-Sticks und anderen sicheren Geräten genutzt werden, einschließlich Geräten mit integrierter Tastatur zur sicheren PIN-Eingabe.

- Die PKCS#11-Schnittstelle kann auch zum Signieren mit einem Hardware-Security-Modul (HSM) verwendet werden. HSMs bieten sichere Schlüsselspeicher und genügend Leistung für hochvolumige Signaturanwendungen. PLOP DS verwendet PKCS#11-Sessions, um die Leistung bei Massensignaturen mit HSMs zu maximieren. PLOP DS kann auch mit HSMs in der Cloud genutzt werden, z.B. AWS CloudHSM.

- Unter Windows kann PLOP DS die kryptografische Infrastruktur des Betriebssystems (MSCAPI) nutzen. Digitale IDs aus dem Zertifikatspeicher von Windows können zur Signaturerstellung genutzt werden. Dabei lassen sich sowohl Software-basierte digitale IDs als auch sichere Hardware-Tokens einsetzen. Beachten Sie, dass für die MSCAPI-Engine nicht alle Signaturfunktionen, wie zum Beispiel LTV, verfügbar sind.

- Alternativ kann eine vom Benutzer bereitgestellte Krypto-Engine verwendet werden, um sicherzustellen, dass alle kryptographischen Operation (Hashing und Signieren) in einer speziellen Krypto-Bibliothek durchgeführt werden.

Betrieb

PLOP DS als Bibliothek oder Kommandozeilen-Tool?

PLOP DS wird als Software-Bibliothek (Komponente) für verschiedene Entwicklungsumgebungen sowie als Kommandozeilen-Tool für Batch-Prozesse ausgeliefert. Die Bibliothek und das Kommandozeilen-Tool bieten den gleichen Funktionsumfang, eignen sich aber für unterschiedliche Einsatzbereiche.

Die PLOP DS-Software-Bibliothek eignet sich...

...zur Integration in Desktop- oder Server-Anwendungen. Programmierbeispiele für alle unterstützten Sprachbindungen sind im PLOP DS-Paket enthalten. Da PLOP DS PDF-Dokumente von Datei oder direkt aus dem Speicher einlesen kann, ist die Kombination mit anderen Produkten einfach realisierbar. So können Sie mit PDFlib und PLOP DS zum Beispiel PDF-Rechnungen erstellen und signieren, bevor sie an die Kunden gesendet werden.

Das PLOP DS-Kommandozeilen-Tool eignet sich...

...zur Batch-Verarbeitung von PDF-Dokumenten. Es erfordert keine Programmierung, sondern kann über leistungsfähige Kommandozeilen-Optionen gesteuert und damit in komplexe Arbeitsabläufe integriert werden.

Unterstützte Entwicklungsumgebungen

PDFlib PLOP DS läuft überall – auf praktisch allen Computersystemen. Wir bieten 32- und 64-Bit-Pakete an und unterstützen alle gängigen Varianten von Windows, macOS, Linux und Unix sowie IBM zSeries Mainframes. Varianten für iOS und Android sind ebenfalls erhältlich.

Der Kern von PLOP DS ist in C und C++ programmiert und auf Schnelligkeit und geringen Overhead optimiert. Über ein einfaches API (Application Programming Interface) lässt sich die PLOP DS-Funktionalität in zahlreichen Programmiersprachen nutzen:

- C und C++
- Java
- .NET und .NET Core
- Objective-C (macOS und iOS) und Swift
- Perl
- PHP
- Python
- Ruby

Vorteile von PDFlib-Software

Zuverlässig

Weltweit arbeiten viele Tausend Programmierer erfolgreich mit unserer Software. PDFlib-Produkte erfüllen alle Qualitäts- und Geschwindigkeitskriterien für den Einsatz auf großen Servern. Alle Produkte sind für den zuverlässigen, unbeaufsichtigten 24-Stunden-Betrieb ausgelegt.

Schnell und einfach

PDFlib-Produkte sind schnell – bis zu Tausenden von Seiten pro Sekunde. Die Programmierschnittstelle ist übersichtlich und einfach zu erlernen.

PDFlib-Produkte sind überall

Unsere Produkte unterstützen alle internationalen Sprachen sowie Unicode. Sie werden von Kunden in der ganzen Welt eingesetzt.

Professioneller Support

Bei Problemen bietet Ihnen unser Support-Team professionelle Unterstützung. Um den reibungslosen Ablauf unternehmenskritischer Anwendungen zu gewährleisten, können Sie Ihre Software-Lizenz durch einen Supportvertrag ergänzen. Ein Supportvertrag garantiert Ihnen kurze Antwortzeiten und Zugang zu den jeweils neuesten Versionen.

Lizenzierung

Bei der Lizenzierung können Sie zwischen verschiedenen Modellen für Server-, Integrations-, Firmen- sowie Quellcodelizenzen wählen.

Über PDFlib GmbH

PDFlib GmbH ist auf die Entwicklung von PDF-Technologie spezialisiert. Unsere Produkte sind seit 1997 im Einsatz. 2006 waren wir eines der Gründungsmitglieder der PDF Association (damals noch PDF/A Competence Center). Das Unternehmen berücksichtigt wichtige technologische Trends, etwa ISO-Standards für PDF. PDFlib GmbH vertreibt alle Produkte weltweit, wobei Europa, Nordamerika und Japan die wichtigsten Märkte darstellen.

Kontakt

Evaluierungsversionen mit vollem Funktionsumfang sind auf unserer Webseite verfügbar. Weitere Informationen erhalten Sie unter:

PDFlib®

PDFlib GmbH
Franziska-Bilek-Weg 9, D–80339 München
Tel. +49 • 89 • 452 33 84-0
sales@pdflib.com www.pdflib.com