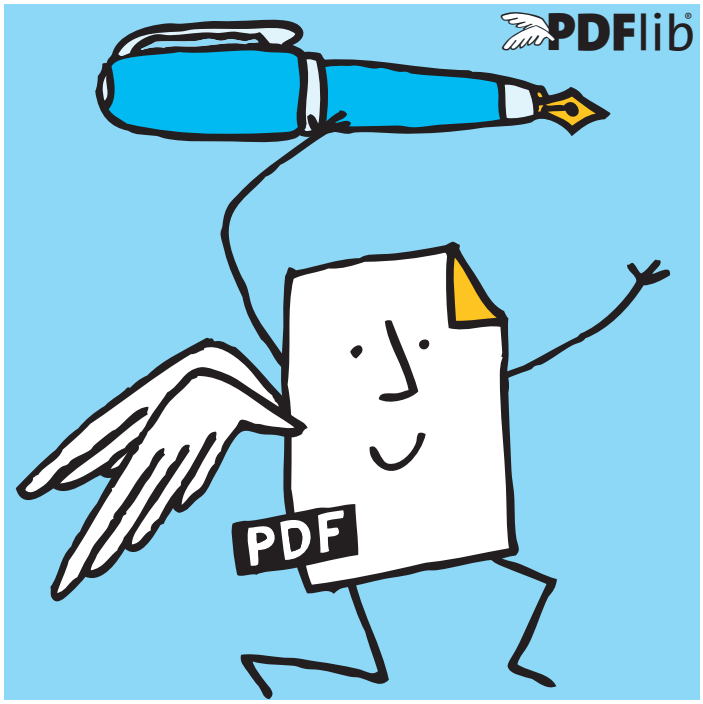


datasheet

PDFlib PLOP DS 5.3

PDF
線形化・
最適化・
保護・
電子署名

PDFlib PLOP DS とは

PDFlib PLOP DS は、PDF 文書を線形化・最適化・修復・分析・暗号化・復号するための堅牢なツールである PDFlib PLOP をベースとしています。PDFlib PLOP DS はこれに加え、PDF 文書に電子署名を行う機能を提供します。ISO 32000-2 に従った PDF 2.0 や、CAdES（ETSI TS 101 733）に基づいた PAdES 署名（ETSI TS 102 778・ETSI EN 319 142）を含む電子署名技術における最新動向・規格群に対応しています。

PDFlib PLOP DS を用いた電子署名

PDFlib PLOP DS は、Adobe Reader・Acrobat のみならず PDF 署名に対応している任意のバリデータを用いて検証できる PDF 署名を行います。PLOP DS は、その署名者のデジタル ID（すなわち証明書とそれに対応する秘密鍵）を、メモリかディスクファイルから、またはスマートカードのようなセキュアなハードウェアトークンから読み取ります。このデジタル ID を用いて、その PDF 文書のための暗号化署名が生成されます。署名を行う際に暗号化を行うことも可能です。

PDF 署名のさまざまな特性

- 既存の PDF 署名フィールド内に署名を作成、もしくは署名を保持する新規のフィールドを生成。この署名は、不可視にすることも、ページ上の特定の位置において可視にすることもできます。
- ロゴや手書き署名のスキャン等の表現を PDF ページとして取り込むことによって電子署名をビジュアル化。
- その署名を破壊することなくフォーム記入等の文書変更ができるよう許可する PDF 認証（作成者）署名を生成。
- 検証情報を、ISO 32000-1 に従ってその署名内に直接格納することもできますし、ISO 32000-2 と PAdES パート 4 で仕様化されているように文書セキュリティストア（DSS）内に格納することもできます。
- 署名を、既存の署名群と文書構造が温存されるよう、増分的な PDF 更新セクション内に行うこともできますし、最適化・暗号化が可能となるよう文書構造を書き換えることによって行うことも可能です。

PDF のさまざまなバージョンと規格

PLOP DS は、あらゆる標準的な PDF のバージョンと規格に対応しています：

- PLOP DS は、Acrobat DC すなわち PDF1.7（ISO 32000-1）拡張レベル 8 までのすべての PDF バージョンに対応しています。PLOP DS は、PDF 2.0（ISO 32000-2）に準拠した文書を処理することもできます。
- PLOP DS は、PDF/A-1/2/3（ISO 19005）アーカイビング規格群に対応しています：入力文書が PDF/A に準拠していれば出力文書も準拠が保証されます。PLOP DS は、PDF/A に要求される XMP 拡張スキーマに完全対応しています。
- 同様に PLOP DS は、PDF/X-1a/3/4/5（ISO 15930）印刷業務規格群と、バリアブル印刷・トランザクション印刷のための PDF/VT-1/2（ISO 16612-2）と、アクセシブル PDF のための PDF/UA-1（ISO 14289）に対応しています。

その他の PDF 処理機能

電子署名に加え、PDFlib PLOP DS は、基礎製品 PDFlib PLOP のすべての機能を有しています：

- PDF 線形化：高速な Web 配信（バイトサービング）を実現。
- 最適化：PDF 文書の品質に影響を与えることなくファイルサイズを削減。
- パスワードセキュリティ：PDF 文書の暗号化・復号や、印刷禁止・内容抽出禁止等の制限の追加・除去。
- 証明書セキュリティ：PDF 文書を、デジタル署名によって識別される限られた受領者のために暗号化。
- 修復モード：破損した PDF 文書を自動的に検出し、可能であれば問題を修復。
- PDF 分析：PDF 文書の任意のプロパティを pCOS インタフェースを通じてクエリ。
- 文書情報項目：文書情報項目をクエリ・追加・変更。
- XMP メタデータ：XMP を追加、文書情報を同期。

PLOP 基礎製品について詳しくは別紙 PLOP データシートをご覧ください。

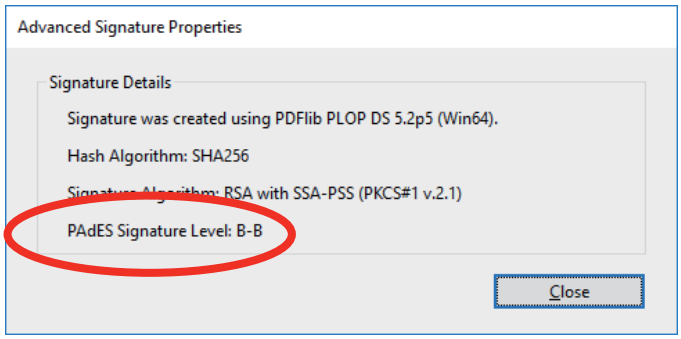
署名の特性

さまざまな署名規格

- PDF 1.7（ISO 32000-1）に従った CMS ベースの PDF 署名
- PDF 2.0（ISO 32000-2）に従った長期検証（LTV）のための署名
- 適格eIDAS署名のためのPAdES（ETSI TS 102 778パート2・3・4、ETSI EN 319 142）、CAdES（ETSI TS 101 733）

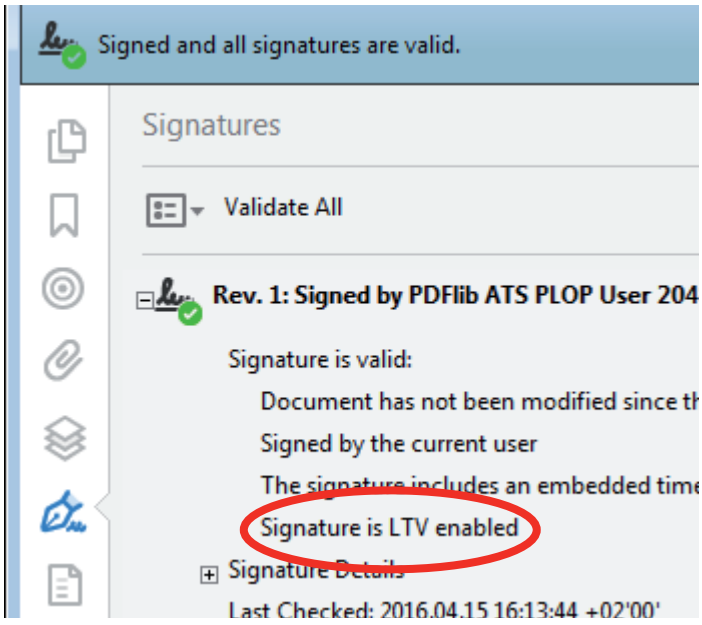
さまざまな PAdES 署名レベル

- 基本署名（レベル B-B）
- 時刻付き署名（レベル B-T）
- 長期検証資料付き署名（レベル B-LT）
- 検証資料の長期可用性・保全性を提供する署名（レベル B-LTA）
- PAdES パート 3 に従った基本電子署名（BES）・明示的ポリシーベース電子署名（EPES）



タイムスタンピング

- RFC 3161・RFC 5816・ETSI EN 319 422 に従って信頼済みタイムスタンプ局（TSA）からタイムスタンプを取得し、生成する署名の中へそれを埋め込み。TSA の詳細を、何ら構成なく、AATL 証明書から読み取ってタイムスタンプを生成できます。
- ISO 32000-2・PAdES パート 4 に従って文書レベルのタイムスタンプ署名を生成。文書レベルのタイムスタンプは、個人署名を行うことなく文書の状態を保証します。



暗号署名の詳細

- RSA・DSA アルゴリズムに従った署名のみならず、楕円曲線電子署名アルゴリズム（ECDSA）に従った署名。RSA については、PKCS#1 v1.5・PCKS#1 v2.1（PSS）に対応しています。
- 強固な署名・ハッシュ関数。
- 生成する署名内に完全な証明書チェーンを埋め込み。これによって、Adobe 認定信頼リスト（AATL）か欧州連合信頼リスト（EUTL）に載っている CA（認証局）からの証明書を持った署名を、クライアント側で何ら構成を必要とせず、Acrobat・Adobe Reader 内で検証できます。
- オンライン証明書状態プロトコル（OCSP。RFC 2560・RFC 6960 に拠る）応答と証明書失効リスト（CRL。RFC 3280 に拠る）を、長期検証（LTV）のための失効情報として埋め込み。

さまざまな署名エンジン

PLOP DS は、複数の暗号化エンジンに対応しています。暗号化エンジンとは、電子署名を生成するためのコンポーネントです：

- その内蔵のエンジンは , 必要な暗号化機能を直接 PLOP DS 内に、一切の外部依存なく実装しています。この内蔵エンジンは、PKCS#12・PFX 形式のソフトウェアベースのデジタル ID に対応しています。

- PLOP DS は暗号化トークンを、標準の PKCS#11 インタフェースを通じて紐付けることができます。この方法で、スマートカード・USB スティック等セキュアデバイス上のデジタル ID を用いて署名を行うことが可能です。これは、セキュアな PIN 入力のためのキーボードが付いた機器でも同様です。

- また、この PKCS#11 インタフェースを使用して、ハードウェアセキュリティモジュール（HSM）を用いて署名することも可能です。HSM は、セキュアなキーストレージを提供するとともに、大量署名の用途に充分なパフォーマンスを提供します。PLOP DS は、PKCS#11 セッションを使用することによって、HSM を用いたバルク署名のパフォーマンスを最大化します。PLOP DS は、AWS CloudHSM 等クラウドの HSM を用いて使用することも可能です。

- Windows では PLOP DS は、このオペレーティングシステムが提供している暗号化インフラストラクチャ（MSCAPI）を活用できます。ソフトウェアベースのデジタル ID やセキュアハードウェアトークンも含め、Windows 証明書ストアからのデジタル ID を用いて署名を行うことが可能です。ただし LTV 等、MSCAPI エンジンでは利用できない署名機能もあります。
- あるいは、専用の暗号化ライブラリ内ですべての暗号化操作（ハッシュ化および署名）が実行されるようにするために、ユーザーが与える暗号化エンジンを使用することも可能です。

運用

PLOP DS ライブラリかコマンドラインツールか

PLOP DS は、さまざまな開発環境用のプログラミングライブラリ（コンポーネント）としても、バッチ処理のためのコマンドラインツールとしても利用できます。ライブラリとコマンドラインツールは提供する機能は同様ですが適した運用タスクが異なっています。

PLOP DS プログラミングライブラリの用途は…

デスクトップ／サーバアプリケーションへの組み込みです。このライブラリのすべての対応言語バインディングでの使用例が PLOP DS パッケージに同梱されています。PLOP DS ライブラリは、PDF 入力文書をディスクファイルからもメモリ内で直接にも受け入れますので、他の製品と容易に組み合わせが可能です。たとえば PDFlib と PLOP DS の組み合わせを活用すれば、PDF インボイスを作成してそれを顧客へ送る前にそれに署名することができます。

PLOP DS コマンドラインツールの得意分野は…

PDF 文書のバッチ処理です。プログラミングを一切必要とせずに強力なコマンドラインオプション群を提供して複雑なワークフローへの統合を可能にします。PLOP DS コマンドラインツールは、PLOP DS ライブラリの使用に対応していない環境からも呼び出せます。

対応開発環境

PDFlib PLOP DS はどこにでも——事実上すべてのコンピューティングプラットフォームで動作します。広く利用されているすべての種類の Windows・macOS・Linux・Unix および IBM zSeries メインフレームシステム用の 32 ビット／64 ビットパッケージを提供しています。iOS・Android 用のバージョンもあります。

PLOP DS のコアは、パフォーマンスの最大化を図りオーバーヘッドを小さくするために高度に最適化された C・C++ で書かれています。シンプルな API（アプリケーションプログラミングインタフェース）を通じて PLOP DS の機能をさまざまな開発環境から利用可能です：

- COM（VB・ASP 等での使用）
- C・C++
- Java
- .NET（C#・VB.NET・ASP.NET 等での使用）
- Objective-C
- Perl
- PHP
- Python
- Ruby

PDFlib ソフトウェア利用の利点

磐石の製品群

世界中の数万人のプログラマーが当社のソフトウェアを使用して成功しています。PDFlib 製品群はサーバ運用のためのあらゆる品質・パフォーマンス要求を満たします。製品はすべて、堅牢な無休サーバ運用と無人バッチ処理に適しています。

速くてシンプル

PDFlib 製品群は非常に高速です——秒速数千ページを実現します。そのプログラミングインタフェースは簡明で学習が容易です。

世界中に PDFlib 製品

当社製品群は世界のあらゆる言語と Unicode に対応しています。世界のあらゆる場所のお客様にご利用いただいています。

プロフェッショナルサポート

問題があるとき、当社は支援に努めます。ビジネスクリティカルなさまざまな応用の要求を満たす商用サポートを提供しています。サポートを追加すると、最新バージョンへのアクセスと、万一の問題発生時の回答時間保証をご利用いただけます。

ライセンシング

サーバライセンス・統合／サイトライセンス・ソースコードライセンスのためのさまざまなライセンシングオプションを提供しています。短時間回答と無償アップデートを伴う幅広い技術サポートのためのサポート契約もご利用いただけます。

PDFlib GmbH について

PDFlib GmbH は PDF 技術に完全特化しています。世界中のお客様が PDFlib 製品群を 1997 年から利用しています。PDF 関連 ISO 規格群等の技術・市場動向に密に追随しています。PDFlib GmbH 製品群は世界中へ出荷されており、主要市場は北米・欧州・日本となっています。

お問い合わせ

完全に機能する評価版が、説明書とサンプルとともに当社 Web サイトにあります。詳しくはお問い合わせください：

PDFlib GmbH
Franziska-Bilek-Weg 9, 80339 München, Germany
電話 +49・89・452 33 84-0、FAX +49・89・452 33 84-99
sales@pdflib.com
www.pdflib.com