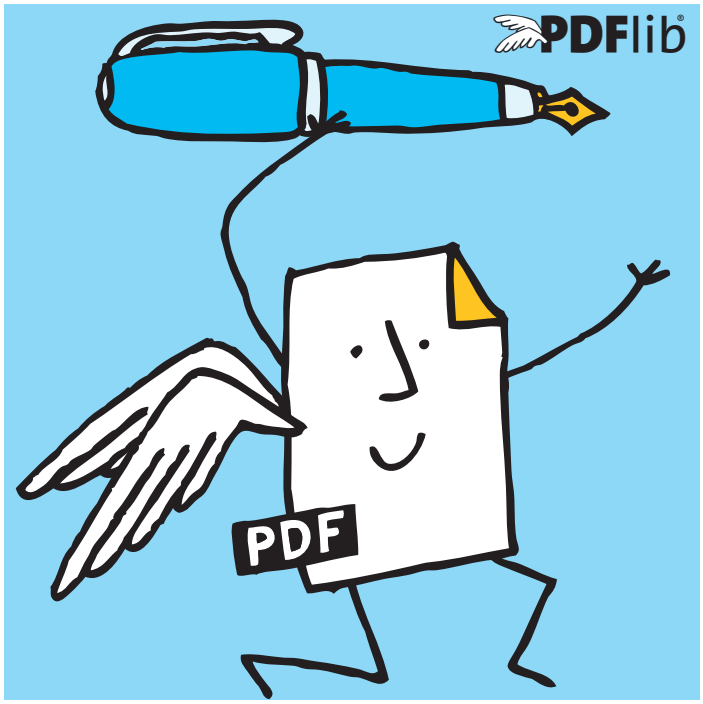


datasheet

PDFlib PLOP DS 5.3

PDF Linearization, Optimization, Protection, Digital Signature

What is PDFlib PLOP DS?

PDFlib PLOP DS is based on PDFlib PLOP, a versatile tool for linearizing, optimizing, repairing, analyzing, encrypting and decrypting PDF documents. PDFlib PLOP DS additionally offers the ability to apply digital signatures to PDF documents. It supports the latest trends and standards in digital signature technology including PDF 2.0 according to ISO 32000-2 and PAdES signatures (ETSI TS 102 778 and ETSI EN 319 142), which in turn are based on CAdES (ETSI TS 101 733).

Digital Signatures with PDFlib PLOP DS

PDFlib PLOP DS applies PDF signatures which can be validated with Adobe Reader, Acrobat, or any other validator which supports PDF signatures. PLOP DS reads the signer's digital ID (i.e. the certificate plus corresponding private key) from memory, a disk file, or a secure hardware token such as a smartcard. The digital ID is used to create a cryptographic signature for the PDF document. Applying a signature can be combined with encryption.

PDF Signature Properties

- Create signatures in existing PDF signature fields or generate new fields which hold the signature. The signatures can be invisible or visible at a particular location on the page.
- Visualize digital signatures by importing a logo, scan of a handwritten signature or other representation as PDF page.
- Create PDF certification (author) signatures which allow document changes such as form-filling without breaking the signature.
- Validation information can be stored directly in the signature according to ISO 32000-1 or in a Document Security Store (DSS) as specified in ISO 32000-2 and PAdES part 4.
- Signatures can be applied in an incremental PDF update section to preserve existing signatures and document structure, or by rewriting the document structure which allows optimization and encryption.

PDF Versions and Standards

PLOP DS supports all relevant PDF versions and standards:

- PLOP DS processes all PDF versions up to Acrobat DC, i.e. PDF 1.7 (ISO 32000-1) up to extension level 8. PLOP DS can also process documents according to PDF 2.0 (ISO 32000-2).
- PLOP DS is aware of the PDF/A-1/2/3 (ISO 19005) archiving standards: if the input document conforms to PDF/A, the output document is guaranteed to conform as well. PLOP DS fully supports XMP extension schemas as required by PDF/A.
- Similarly, PLOP DS is aware of the PDF/X-1a/3/4/5 (ISO 15930) print production standards, PDF/VT-1/2 (ISO 16612-2) for variable and transactional printing and PDF/UA-1 (ISO 14289) for accessible PDF.

Additional PDF Processing Features

In addition to digital signatures PDFlib PLOP DS includes all features of the base product PDFlib PLOP:

- PDF linearization for fast Web delivery (byteserving).
- Optimization: reduce the file size of PDF documents without affecting quality.
- Password security: encrypt or decrypt PDF documents and apply or remove restrictions such as »printing not allowed« or »content extraction not allowed«.
- Certificate security: encrypt PDF documents for a closed set of recipients which are identified by their digital certificates.
- Repair mode: automatically detect damaged PDF documents and fix the problems if possible.
- PDF analysis: query arbitrary properties of a PDF document via the pCOS interface.
- Document info entries: query, add, or replace document info entries.
- XMP metadata: add XMP and synchronize document info.

For more information about the PLOP base product please refer to the separate PLOP datasheet.

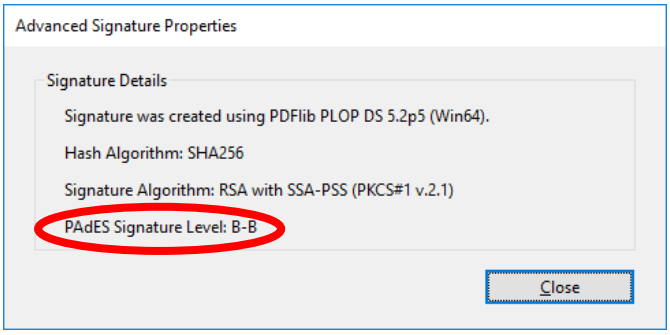
Signature Characteristics

Signature Standards

- CMS-based signatures according to PDF 1.7 (ISO 32000-1)
- Signatures for Long-Term Validation (LTV) according to PDF 2.0 (ISO 32000-2)
- PAdES (ETSI TS 102 778 part 2, 3 and 4, ETSI EN 319 142), CAdES (ETSI TS 101 733) for qualified eIDAS signatures

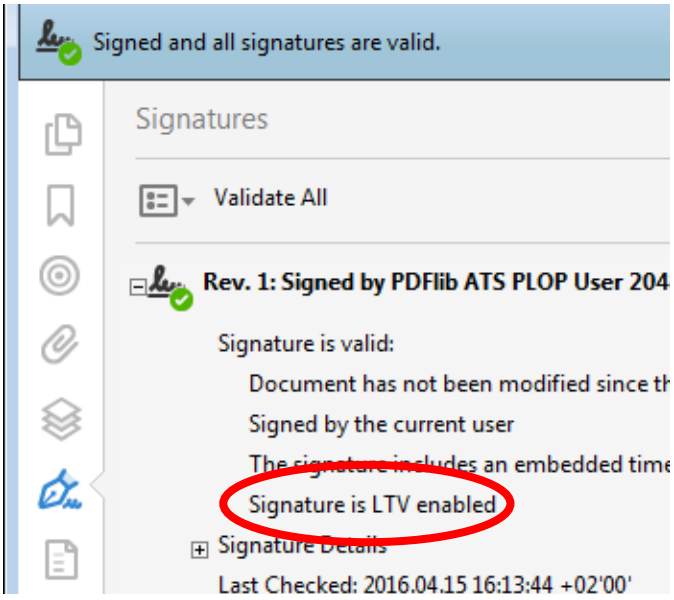
PAdES Signature Levels

- Basic Signature (Level B-B)
- Signature with Time (Level B-T)
- Signature with Long-Term Validation Material (Level B-LT)
- Signature providing Long Term Availability and Integrity of Validation Material (Level B-LTA): required for eIDAS conformance
- Basic Electronic Signature (BES) and Explicit Policy-based Electronic Signature (EPES) according to PAdES part 3



Timestamping

- Retrieve a timestamp from a trusted Timestamp Authority (TSA) according to RFC 3161, RFC 5816 and ETSI EN 319 422, and embed it in the generated signature. TSA details can be read from AATL certificates to create timestamps without any configuration.
- Create document-level timestamp signatures according to ISO 32000-2 and PAdES part 4. A document-level timestamp assures the state of a document without applying a personal signature.



Cryptographic Signature Details

- Signatures according to the RSA and DSA algorithms as well as the Elliptic Curve Digital Signature Algorithm (ECDSA). PKCS#1 v1.5 and PKCS#1 v2.1 (PSS) encoding for RSA are supported.
- Strong signature and hash functions.
- Embed the full certificate chain in the generated signatures, which means that signatures with certificates from a CA (Certification Authority) on the Adobe Approved Trust List (AATL) or European Union Trust List (EUTL) can be validated in Acrobat and Adobe Reader without any configuration on the client side.
- Embed Online Certificate Status Protocol responses (OCSP according to RFC 2560 and RFC 6960) and Certificate Revocation Lists (CRL according to RFC 3280) as revocation information for Long-Term Validation (LTV).

Signature Engines

PLOP DS supports multiple cryptographic engines, i.e. components for generating digital signatures:

- The built-in engine implements the required cryptographic functions directly in PLOP DS without any external dependencies. The built-in engine supports software-based digital IDs in the PKCS#12 and PFX formats.

- PLOP DS can attach cryptographic tokens via the standard PKCS#11 interface. This way digital IDs on smartcards, USB sticks, and other secure devices can be used for signing. This includes devices with an integrated keyboard for secure PIN input.

- The PKCS#11 engine can also be used to sign with a Hardware Security Module (HSM). HSMs offer secure key storage and ample performance for high-volume signing applications. PLOP DS uses PKCS#11 sessions to maximize performance of bulk signatures with HSMs. PLOP DS can also be used with HSMs in the cloud such as AWS CloudHSM..

- On Windows PLOP DS can leverage the cryptographic infrastructure provided by the operating system (MSCAPI). Digital IDs from the Windows certificate store can be used for signing, including software-based digital IDs and secure hardware tokens. Note that not all signature features are available with the MSCAPI engine, e.g. LTV.

- Alternatively a user-supplied cryptographic engine can be used to ensure that all cryptographic operations (hashing and signing) are performed in a dedicated cryptographic library.

Deployment

PLOP DS Library or Command-Line Tool?

PLOP DS is available as a programming library (component) for various development environments, and as a command-line tool for batch operations. Library and command-line tool offer similar features, but are suitable for different deployment tasks.

The PLOP DS programming library is used...

...for integration into desktop or server applications. Examples for using the library with all supported language bindings are included in the PLOP DS package. Since the PLOP DS library accepts PDF input documents from a disk file or directly in memory, it can easily be combined with other products. For example, using the combination of PDFlib and PLOP DS you can create PDF invoices and sign them before sending them to the customer.

The PLOP DS command-line tool is suited...

...for batch processing PDF documents. It doesn't require any programming, but offers powerful command-line options which can be used to integrate it into complex workflows. The PLOP DS command-line tool can also be called from environments which do not support the use of the PLOP DS library.

Supported Development Environments

PDFlib PLOP DS is everywhere – it runs on practically all computing platforms. We offer 32-bit and 64-bit packages for all common flavors of Windows, macOS, Linux and Unix, as well as for IBM zSeries mainframe systems. Versions for iOS and Android are also available.

The PLOP DS core is written in highly optimized C and C++ for maximum performance and small overhead. Via a simple API (Application Programming Interface) the PLOP DS functionality is accessible from a variety of development environments:

- COM for use with VB, ASP, etc.
- C and C++
- Java
- .NET for use with C#, VB.NET, ASP.NET, etc.
- Objective-C
- Perl
- PHP
- Python
- Ruby

Benefits of using PDFlib Software

Rock-solid Products

Tens of thousands of programmers worldwide successfully use our software. PDFlib products meet all quality and performance requirements for server deployment. All products are suitable for robust 24x7 server deployment and unattended batch processing.

Speed and Simplicity

PDFlib products are incredibly fast – up to thousands of pages per second. The programming interface is straightforward and easy to learn.

PDFlib Products all over the World

Our products support all international languages as well as Unicode. They are used by customers in all parts of the world.

Professional Support

If there's a problem, we will try to help. We offer commercial support to meet the requirements of your business-critical applications. By adding support you will have access to the latest versions, and have guaranteed response times should any problems arise.

Licensing

We offer various licensing options for server licenses, integration and site licenses, and source code licenses. Support contracts for extended technical support with short response times and free updates are also available.

About PDFlib GmbH

PDFlib GmbH is completely focused on PDF technology. Customers worldwide use PDFlib products since 1997. The company closely follows development and market trends, such as ISO standards for PDF. PDFlib GmbH products are distributed all over the world with major markets in North America, Europe, and Japan.

Contact

Fully functional evaluation versions including documentation and samples are available on our Web site. For more information please contact:

PDFlib GmbH
Franziska-Bilek-Weg 9, 80339 München, Germany
phone +49 • 89 • 452 33 84-0, fax +49 • 89 • 452 33 84-99
sales@pdflib.com
www.pdflib.com