

3-Heights™ PDF Security

The 3-Heights™ PDF Security component offers comprehensive functionality in two independent yet combinable areas: Electronic signatures and encryption.

Electronic Signatures

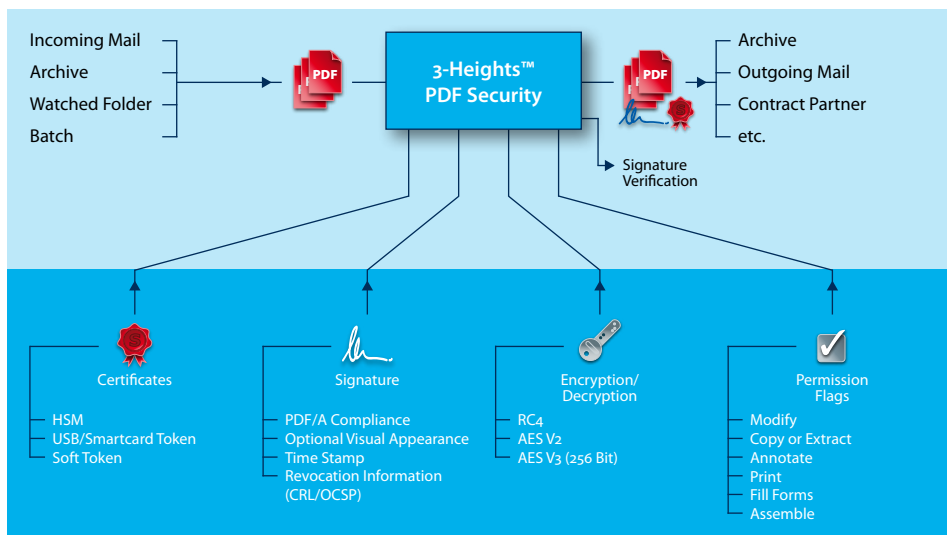
Applying an electronic signature guarantees the authenticity and integrity of documents, both of which are important requirements in electronic data exchange. Depending on the characteristics of the signature and the country it is used in, an electronic signature can be equivalent to signing a document by hand. Electronic signatures offer advantages with regard to the speed, security and automation of business correspondence. The 3-Heights™ PDF Security component is able to apply various types of electronic signature (simple, advanced and qualified). The component's benefits include PDF/A conformity, embedding information on the validity of certificates (OCSP, CRL), time stamps and compatibility with signature hardware (HSM) for mass signature applications. The component can verify existing signatures by checking their integrity.

Encryption

PDF documents used in professional circumstances contain important information that needs to be protected against unauthorized access and unintentional alteration. This is achieved by protecting PDF documents through encryption and user permission flags.

Product Variants

API	Shell	Service



Properties and Benefits

This component is characterized by its high performance and a comprehensive range of services. It efficiently encrypts and signs even large numbers of PDF documents. Advanced and qualified electronic signatures (QES) guarantee the authenticity and

integrity of documents whilst improving the quality of archived documents and increasing the security of business processes.

Document authorization can be defined by applying an author's signature (MDP) or setting permission flags.

Areas of Use

Archiving

Documents are signed prior to archiving to increase compliance with audit requirements. A hardware security module can be used to handle large numbers of documents.

Incoming Mail

Verification of incoming signed PDF documents to ensure they have not been modified during transmission and were transmitted by an authenticated sender.

Outgoing Mail

The component can encrypt and apply an electronic signature to PDF documents thus enabling the recipient to verify authenticity and integrity.

Software Manufacturers/OEM

The 3-Heights™ PDF Security component is quickly integrated in solutions without any need for extensive learning and programming.

Other Areas of Use

- Add encryption and/or digital signatures for PDF files to applications (client, server, web)
- Centralized signature service with HSM for mass signatures in input/output management
- Workflow support systems (author, review, release, etc.)
- Client solutions (signature application software)
- Ebooks

Technical details

Input Formats

- PDF
- PDF/A

Output Formats

- PDF
- PDF/A (if input format is already PDF/A)

Compliance

- Standards: ISO 19005-1 (PDF/A-1), ISO 19005-2 (PDF/A-2), ISO 32000 (PDF 1.7)
- PAdES

Operating Systems

- Windows 2000, XP, Vista, 7
- Windows Server 2003, 2008, 2008 R2 – 32 and 64 Bit
- HP-UX – 32 Bit and Itanium
- IBM AIX – 32 and 64 Bit
- Linux (SuSE and Red Hat on Intel)
- Mac OS X
- Sun Solaris

Interfaces

- API: C, Java, .NET, COM

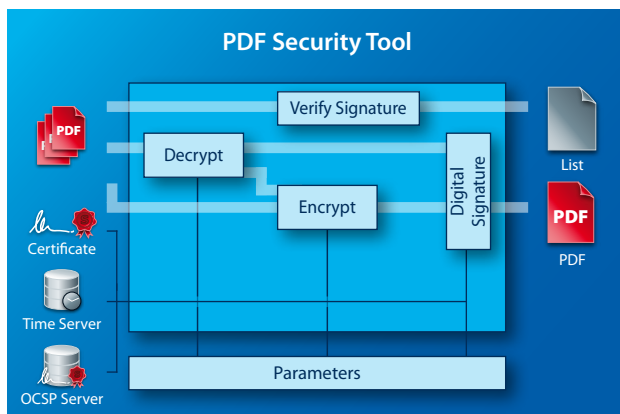
Programming Languages

All program libraries are written in efficient and thread-safe C++. API offers a selection of the following connections to programming languages:

- C#, VB .NET, J# via .NET
- Java via JNI
- MS Visual Basic, Borland Delphi, MS Office products such as Access and C++ via COM
- C and C++ via native C

Product Variants

- Shell tool (command line for batch processing)
- API (programming interface)
- Windows service (monitored directories)



Performance Characteristics

- PDF/A compliant signature
- Embedding of cryptographic time stamps (TSP)
- Embedding of Online Certificate Status Protocols (OCSP)
- Embedding of Certificate Revocation Lists (CRL)
- Cryptographic Service Provider (CSP) interface
- Supports Windows Certificate Store
- PKCS#11 interface for connecting a hardware security module (HSM)
- Hardware Token Session Support -> unique PIN input for batch signing
- Programmatic PIN transfer for advanced signatures, e.g. corporate certificates
- Revocation information caching for efficiently signing large numbers of documents
- Platform independent

Functions

Electronic Signatures

- Application of compliant signatures to PDF/A documents
- Verification of signatures in a PDF document
- Simple, advanced and qualified electronic signatures
- Long-term signatures with embedded trust chain, time stamp and verification information on certificate validity
- Support for mass signature devices (HSM) via PKCS#11
- Author's signature (MDP)
- Listing and restoring revisions
- Invisible and visible signatures and design functions for visible signatures

Encryption

- Protect PDF files against unauthorized access
- Encrypt and decrypt PDF documents with owner and user passwords
- Set document permission flags
 - Read
 - Print
 - Extract
 - Annotate, sign
 - Change
 - etc.
- Set encryption filters (none, RC4, AES)
- Set encryption key length (40... 128)