

3-Heights™ PDF Security

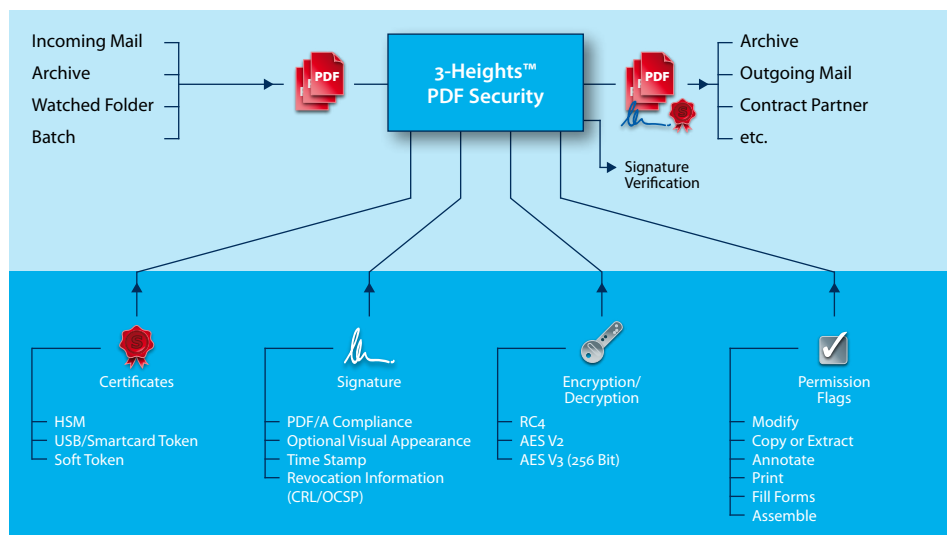
Die 3-Heights™ PDF Security Komponente bietet umfassende Funktionalitäten in zwei unabhängigen, aber kombinierbaren Bereichen an: Elektronische Signatur und Verschlüsselung.

Elektronisches Signieren

Das Aufbringen einer elektronischen Signatur stellt die Authentizität und Integrität eines Dokumentes sicher, welches wichtige Anforderungen im elektronischen Datenaustausch sind. Je nach Land und Ausprägung der Signatur ist eine elektronische Unterschrift gleichwertig zu einer Handunterschrift. Die elektronische Signatur bringt Vorteile bezüglich Geschwindigkeit, Sicherheit und Automatisierbarkeit der Geschäftskorrespondenz. Mit der 3-Heights™ PDF Security Komponente können fortgeschrittene und qualifizierte elektronischen Signaturen aufgebracht werden. Vorzüge der Komponente sind PDF/A Konformität, Einbettung von OCSP und CRL, Zeitstempel und die Anbindung an Hardware-Signaturgeräten (HSM) für Massensignaturanwendungen. Vorhandene Signaturen können mit der Komponente verifiziert werden.

Verschlüsseln

PDF Dokumente im professionellen Einsatz beinhalten wichtige Informationen, die gegen unberechtigten Zugriff und unbeabsichtigte Änderungen geschützt werden müssen. Dazu werden PDF Dokumente verschlüsselt und mit Benutzerrechten versehen.






Eigenschaften und Nutzen

Die Komponente zeichnet sich durch die hohe Performanz und einen umfangreichen Leistungskatalog aus. Dadurch lassen sich auch grosse Bestände an PDF Dokumenten rasch verschlüsseln und signieren.

Durch fortgeschrittene und Qualifizierte Elektronische Signaturen (QES) wird die Integrität und Authentizität von Dokumenten sichergestellt und die Qualität von archivierten Dokumenten sowie die Sicherheit von Geschäftsprozessen erhöht.

Produktvarianten

API	Shell	Service
		



Durch eine Autoren Signatur (MDP) oder das Setzen von Benutzerrechten werden die Berechtigungen von Dokumenten festgesetzt.

Einsatzgebiete

Archivierung

Vor der Archivierung werden Dokumente signiert, was z. B. die Revisionsicherheit erhöht. Bei grossen Mengen kann dazu eine HSM verwendet werden.

Posteingang

Prüfung von signierten PDF Dokumenten beim Posteingang, um sicher zu stellen, dass diese während der Übermittlung nicht geändert wurden und auch von einem authentifizierten Sender übermittelt wurden.

Postausgang

PDF Dokumente lassen sich mit der Komponente verschlüsseln und mit digitaler Signaturen versehen, damit der Empfänger die Echtheit und Unversehrtheit prüfen kann.

Softwarehersteller/OEM

3-Heights™ PDF Security kann ohne grossen Lern- und Programmieraufwand in kurzer Zeit in Lösungen eingebaut werden.

Weitere Einsatzgebiete

- Applikation (Client, Server, Web) mit Verschlüsselung und/oder digitaler Signatur für PDF Dateien erweitern
- Zentraler Signatur-Dienst mit HSM für Massensignaturen im Input- und Output-Management
- Workflow Support Systeme (Autor, Review, Freigabe usw.)
- Clientlösungen (Signatur Anwendungssoftware)
- E-Books

Technische Daten

Eingangsformate

- PDF
- PDF/A

Ausgangsformate

- PDF
- PDF/A (falls Eingangsformat schon PDF/A ist)

Compliance

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

Betriebssysteme

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

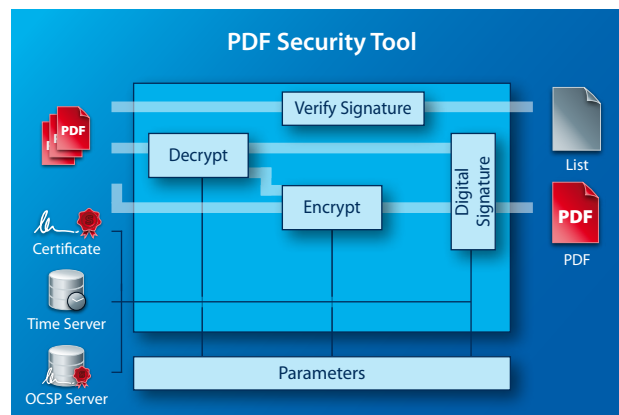
Schnittstellen

- API: C, Java, .NET, COM

Programmiersprachen

Alle Programmibibliotheken sind in effizientem und Thread sicherem C++ geschrieben. In der API wird eine Auswahl der folgenden Anbindungen an Programmiersprachen angeboten:

- C#, VB .NET, J# via .NET
- Java via JNI
- MS Visual Basic, Borland Delphi, MS Office Produkte wie Access und C++ via COM
- C und C++ via native C



Produktvarianten

- Shell Tool (Befehlszeile für Stapelerarbeitung)
- API (Programmierschnittstelle)
- Windows Service (Überwachte Verzeichnisse)

Leistungsmerkmale

- PDF/A konforme Signatur
- Einbettung von kryptografischen Zeitstempeln (TSP)
- Einbettung von Online Certificate Status Meldungen (OCSP)
- Einbettung von Certificate Revocation Lists (CRL)
- Schnittstelle zu Cryptographic Service Provider (CSP)
- Unterstützung Windows Certificate Store
- PKCS#11 Schnittstelle zur Anbindung an ein Hardware Security Modul (HSM)
- Hardware Token Session Support -> einmalige PIN Eingabe für Batch Signierung
- Programmatische PIN Übergabe für fortgeschrittene Signaturen, z. B. Firmenzertifikate
- Revocation Information Caching zum raschen Signieren vieler Dokumente
- Plattform unabhängig

Funktionen

Elektronische Signatur

- PDF/A konform signieren
- Signaturen in einer PDF Datei auf Gültigkeit überprüfen
- Einfache, fortgeschrittene oder Qualifizierte Elektronische Signatur
- Langzeit Signatur mit eingebetteter Vertrauenskette, Zeitstempel und Prüfinformation zur Zertifikatsgültigkeit
- Unterstützung von Massensignaturgeräten (HSM) via PKCS#11
- Autoren Signatur (MDP)
- Revisionen auflisten und wiederherstellen
- Unsichtbare und sichtbare Signaturen und Gestaltung der sichtbaren Signatur

Verschlüsselung

- Schützen von PDF Dateien vor unberechtigtem Zugriff
- Verschlüsseln und entschlüsseln von PDF Dokumenten mit Besitzer und Benutzer Passwörtern
- Setzen von Dokument Zugriffsrechten
 - Lesen
 - Drucken
 - Extrahieren
 - Annotieren, Signieren
 - Ändern
 - usw.
- Setzen von Verschlüsselungsfilter (kein, RC4, AES)
- Setzen der Schlüssellänge (40... 128 Bit)
- Entschlüsselung inkl. AES V3 (256 Bit)