Pdf Signing fundamentals

Begriffe

ISO 32000-1 (PDF standard)

- Core PDF Spezifikation: Definiert wie PDF's strukturiert sind (pages, fonts, annotations, signatures)

PDFBox / iText 7

- Pdf engine
- Pdfbox opensource, verwendet von EU DSS (siehe hier)
- itext 7 lizenz einkaufbar
- Nicht notwendig bei verwendung von eu dss

EU DSS

- =Digital Signature Service (DSS): creation, extension and validation of advanced electronic signatures
- =AdES engine d.h.
    - PAdES-B / T / LT / LTA logic
    - OCSP & CRL fetching
    - Timestamping
    - Certificate chain building
    - EUTL trust validation
    - Signature validation reports (ETSI compliant)
- Api: input unsigned pdf, output: signed pdf
- Workflow in java: 1. Load PDF (FileDocument) 2. Load your private key + cert (SignatureTokenConnection) 3. Set PAdES signing parameters (level, digest, optional visible signature, TSA) 4. Call PAdESService.sign (calls OCSP/CRL, ...) 5. Save signed PDF
- EU DSS ist vorallem AdES-Engine d.h. wenig QES Signatur
    - EU DSS erzeugt Advanced Electronic Signatures (AdES).
    - Eine Qualified Electronic Signature (QES) benötigt zusätzlich:

        - Qualifiziertes Zertifikat von einem Qualified Trust Service Provider (QTSP)
        - Signaturerstellung auf einer sicheren Signaturerstellungseinheit (QSCD / HSM / Smartcard)
- DSS kann QES technisch erzeugen, wenn man:
    - einen Zugang zu einem QTSP-HSM hat
    - die private Key-Operation innerhalb der QSCD erfolgt

Bouncycastle

- Java implementation of cryptographic algorithms and cryptographic protocols that make use of the algorithms.
- contains a low-level lightweight API suitable for use in any environment with additional infrastructure built on top of that to construct a provider conforming to the JCA framework.
- Used by eu dss

CA (certificate authority)

- Ausstellung und Verwaltung digitaler Zertifikate + Gewährleistung sicherer Kommunikation + Überprüfung der Benutzer
- Authentizität über Public Key Infrastructure (PKI) X.509-Zertifikat - enthält infos wie
    - Namen Eigentümers + Public Key, Namen der ausstellenden CA, Gültigkeitsdatum des Zertifikats + wofür es verwendet werden kann
- Im idealfall vertreten in AATL + EUTL trust list

CRL (old) / OCSP (new)

- Problem (revocation checking): Years later need to validate: Was signing certificate valid at signing time (i.e. Enables offline validation years later)
    - OCSP responders may be offline
    - CRL URLs may be gone
    - CA may no longer exist
- CRL (Certificate Revocation List): Periodically published list of revoked certificates
- OCSP (Online Certificate Status Protocol): ist protokoll dass Live query ermöglicht: “Is this cert still valid?”
    - New alternative to crl

    - Funktionsweise: 1. OCSP-Anfrage an einen OCSP-Responder (Server der von ausstellenden CA betrieben wird) 2. OCSP-Responder (von CA) prüft Gültigkeit der Anfrage 3. Antwort: Zertifikat ist aktuell/widerrufen/unbekannt
    - Webbrowser (edge, safari) unterstützen OCSP
- PAdES LT/LTA embeds OCSP/CRL responses

TSA (Time Stamping Authority)

- =Trusted third party issuing cryptographic timestamps
- Proves WHEN a document was signed

ADES (Advanced Electronic Signature)

- Definiert rechtlich gültige Signaturen auf Daten jeder Art: Generische Signaturtechnologie (CAdES, XAdES)
- Unterkategorien p**ades**, c**ades**, X**ades**
    - PAdES (PDF Advanced Electronic Signature) = AdES speziell für PDF - Definiert, wie CAdES/AdES-Signaturen im PDF-Format eingebettet werden - Legt Langzeitprofile (B, T, LT, LTA) fest

QES

- Erstellung workflow z.B.
    a. erstellung qualifizierter Signatur (QES)
    b. Erzeugst daraus PAdES-LTA, d.h.: Signatur + OCSP/CRL embedded; Archivierungstimestamps; Langzeitvalidierunggarantiert

Pades (PDF Advanced Electronic Signatures)

- ETSI standard defining how to apply CAdES signatures inside PDFs
- Ensures long-term validation & EU compliance
- Defined in (incl. profiles): ETSI EN 319 142-1
- Profile/Signature levels
    - PAdES_BASELINE_B: basic
    - PAdES_BASELINE_T: includes TSA timestamp
    - PAdES_BASELINE_LT: embeds OCSP/CRL
    - PAdES_BASELINE_LTA: adds archive timestamps d.h. kein zusätzlicher input im vergleich zu lt sondern fügt Archiv-Zeitstempel ein (LTA) d.h. konkret 1

weiterer api call an eine TSA, die Archiv-Zeitstempel ausstellen darf (meist dieselbe TSA wie für LT)

- “signature extension”: Sofern bereich z.B. T vorhanden ist kann ein upgrade auf lt oder lta erfolgen
- Unterschied zu CAdES, XAdES: cades macht signing für binary data, xades für xml data, pades = cades für pdf

AATL (Adobe Approved Trust List) & EUTL (EU Trusted List)

- = trust lists of CA's
- AATL = Adobe’s global list of trusted CAs i.e. Determines if Adobe Reader shows: Signature valid
- EUTL = Official EU list of Qualified Trust Service Providers (QTSPs)
- Unterschied: AATL → Adobe UI trust, EUTL → Legal trust under eIDAS
- Qualified signatures (QES) require EUTL trust
- Ideally CA is in both AATL + EUTL

eIDAS (EU regulation)

- =EU regulation governing electronic signatures
- Signature levels under eIDAS
    - Electronic signature: Any data indicating intent z.B. einfache Unterschrift via adobe
    - Advanced (AdES): Identifies signer, tamper-proof z.B. fingerprint (hash)
    - Qualified (QES): Advanced + qualified cert + QSCD
- Jede digitale Signatur = elektronische Signatur aber nicht jede elektronische signatur ist eine digitale signatur
- TR-03138 implementiert eIDAS-konforme Signaturen nach deutschen Regeln
- Wann wird was benötigt (ades vs qes)
    - Regel: QES wird dann notwendig, wenn Gesetz oder Vertrag explizit qualifizierte Signatur verlangt, oft geht es richtung: Rechnungen / Invoices: AdES-B/T/LT reicht oft (gesetzlich gültig, z.B. GoBD), Verträge / Notarielle Dokumente / Verträge mit hoher rechtlicher Wirkung: QES

BSI TR-03138 – RESISCAN (Germany)

- =German BSI technical guideline
- Defines legally compliant scanning & archiving
- TR-03138 implementiert eIDAS-konforme Signaturen nach deutschen Regeln
- beziehung zu pdf signing: es wird gefordert: PAdES-LTA, Long-term proof, Audit-safe archiving, Evidence preservation

ETSI (European Telecommunications Standards Institute)

- ISO defines *where* signatures live in PDF
- ETSI defines *how* to do them legally & interoperably
- Example Standards

Topic	**Standard**
PDF base	**ISO 32000-1**
PAdES	**ETSI EN 319 142**
AdES framework	**ETSI EN 319 102-1**
CAdES	**ETSI EN 319 122**
XAdES	**ETSI EN 319 132**

How everything fits together (end-to-end)

1. PDF structure → ISO 32000-1
2. Signature container → CAdES
3. PDF-specific rules → PAdES
4. Signing key → Keystore / HSM
5. Timestamp → TSA^
6. Revocation proof → OCSP / CRL
7. Trust anchor → EUTL (+ AATL for Adobe)
8. Legal framework → eIDAS
9. Archiving compliance → PAdES-LTA + BSI TR-03138

Fragen: Bereits im Kontext beantwortet

- EIDAS muss angewendet werden: ja da EU-based corporation
- Welche dokumente sollten gesigned werden (sofern notwendig)
- Zu welchem Prozessschritt soll die pdf gesigned werden

Fragen: Noch offen

1. Müssen pdf's gesigned werden
2. Retention requirements: 6 / 10 / 30 years archival rules (implies PAdES-LT or LTA)
3. Visible signature required?
4. Single vs. Multiple Signatures
5. Benötigt Dokument mehrere Unterschriften z.B.: Beteiligung mit mehreren Parteien: Genehmigungskette (z. B. Einkauf → Abteilung → CFO)
6. Regulatorische signing frameworks
    a. eIDAS
    b. Internal audit requirements
    c. Possibly BSI TR-03138 (RESISCAN) for Germany
7. Welcher Signature type (siehe eIDAS: Electronic / Advanced / Qualified signatures) muss genommen werden für den usecase: Is QES required or Is AdES enough?
8. Falls ades: Welches pades profil ist zu benutzen
    a. Is timestamp mandatory? (TSA integration)
    b. Is long-term validation required? (PAdES-LT vs LTA)
    c. If no one answers this explicitly → assume PAdES-LT minimum
9. wo passiert das signing?
    a. Central signing service
        i. wie viele Documents per hour?
        ii. Batch vs real-time?
        iii. SLA?
    b. Embedded in business service (viele der folgefragen beziehen sich auf diese option)
    c. External signing gateway
10. Welche PKI/CA ist zu nehmen: unternehmens-intern oder External QTSP (e.g. D-Trust, T-Systems, Swisscom, GlobalSign)
11. welcher TSA ist zu benutzen

12. welcher ocsp service ist zu benutzen
13. Revocation strategy: OCSP preferred, CRLs as fallback?
14. Wer owned private key, Wo liegt der private key (must not leave secure storage) zum signen und wie bekomme ich zugriff auf diesen bzw. Wie frage ich diesen ab (PKCS#12, REST, ...) (inkl. Wie passiert auth)
    a. HSM
    b. Smartcard
    c. Cloud signing service
    d. Rest service bei der bahn
15. Which library stack is allowed?
    a. Apache PDFBox (PDF)
    b. EU DSS (Digital Signature Services): Is EU DSS allowed?
    c. iText: Is iText licensed?
    d. Welche crypto lib ist approved: z.B. BouncyCastle?