PDF STANDARDS AND DIGITAL SIGNATURES

- PDF Advanced Electronic Signatures (PAdES)
  - > ETSI TS 102 778-1: Overview
  - > ETSI TS 102 778-2: CMS (ISO-32000-1)
  - > ETSI TS 102 778-3: CAdES (ISO-32000-2)
  - > ETSI TS 102 778-4: LTV (ISO-32000-2)
  - > ETSI TS 102 778-5: XAdES (XML Forms Architecture)
  - > ETSI TS 102 778-6: Signature appearance
- ISO 32000-2: DIS / CD
  - > Under development
- iText white paper
  - > http://itextpdf.com/book/digitalsignatures
  - > http://www.slideshare.net/blowagie/whats-new-in-pdf-2

ETSI TS 102 778-1 V1.1.1 (2009-07)

Technical Specification

Electronic Signatures and Infrastructures (ESI);
PDF Advanced Electronic Signature Profiles;
Part 1: PAdES Overview - a framework document for PAdES

DRAFT INTERNATIONAL STANDARD ISO/DIS 32000-2

ISO/TC 171/SC 2 Secretariat: **ANSI**

Voting begins on **2012-03-01** Voting terminates on **2012-08-01**

Document management — Portable document format —

Part 2:
PDF 2.0

Digital Signatures for PDF documents

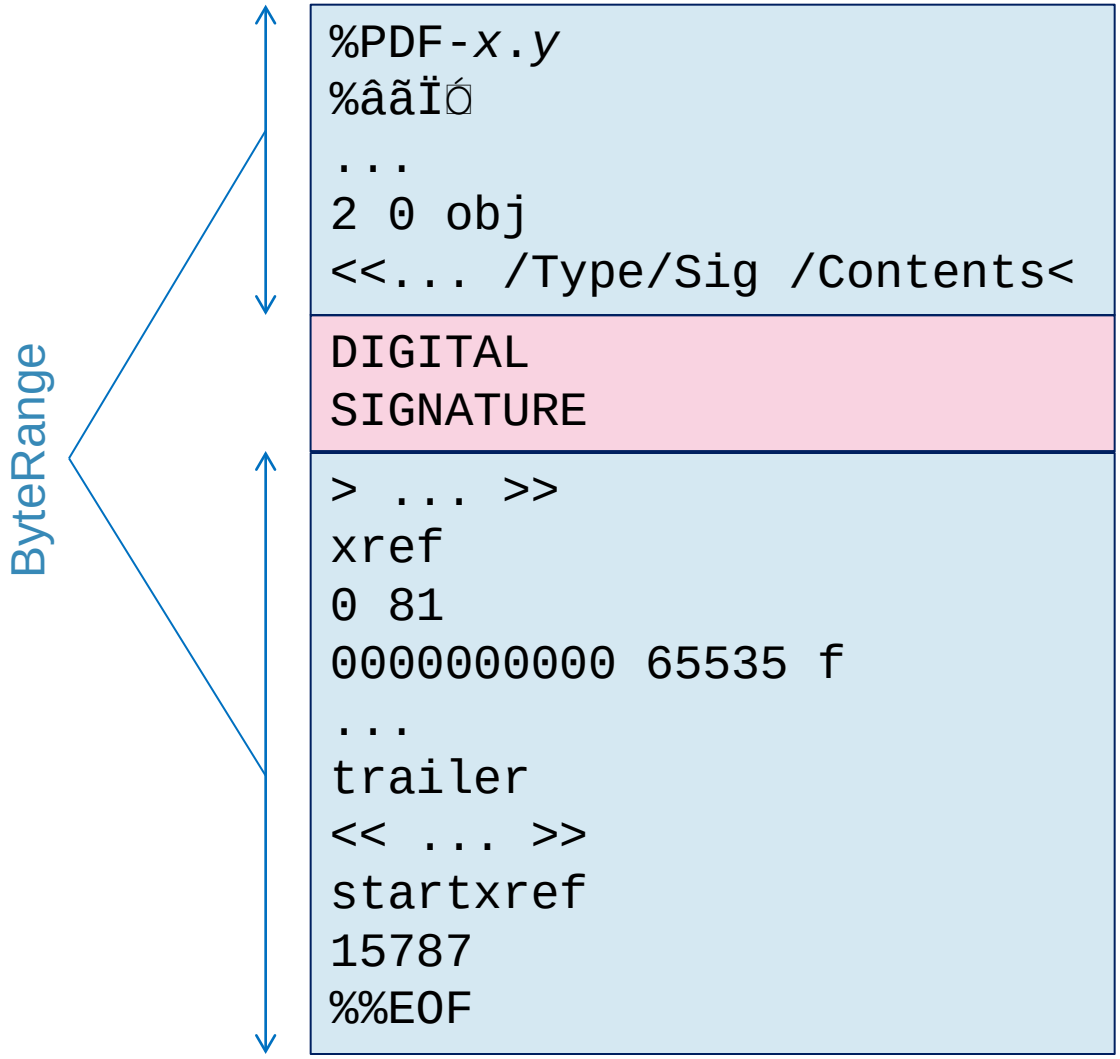
A White Paper by Bruno Lowagie (iText Software)

Introduction

The main rationale for PDF used to be viewing and printing documents in a reliable way. The technology was conceived with the goal "to provide a collection of utilities, applications, and system software so that a corporation can effectively capture documents from any application, send electronic versions of these documents anywhere, and view and print these documents on any

PDF SYNTAX

- There are no bytes in the PDF that aren't covered, other than the PDF signature itself.*
- The digital signature isn't part of the ByteRange.
- The concept "to initial a document" doesn't exist; you sign the complete document at once (not on a page per page basis).



* Read "Collisions in PDF Signatures" by Florian Zumbiehl http://pdfsig-collision.florz.de/

INGREDIENTS OF A DIGITAL SIGNATURE

Producer-side

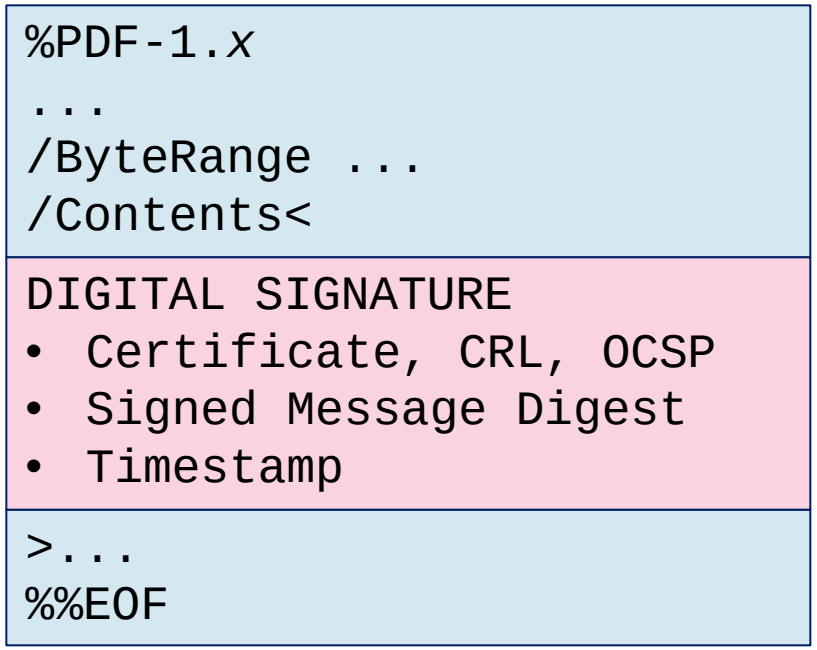
(the signing app)

- Certificate
  - > Public key
  - > Identity info
- Private key
- Original document

ByteRange

Consumer-side

(the signed document)



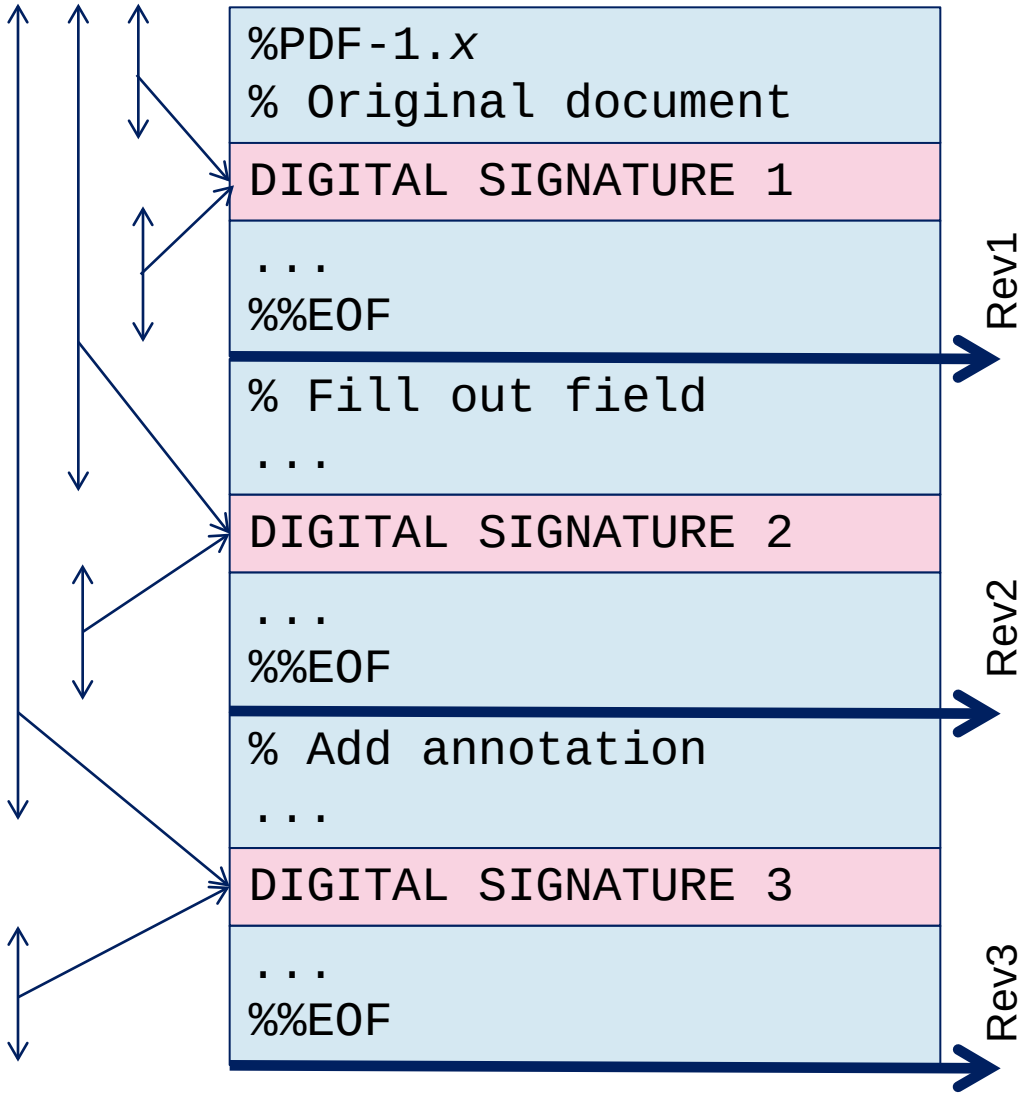
SUBFILTERS

- Stop using:
  - **adbe.x509.rsa_sha1:** uses PKCS#1: forbidden in PAdES
    - Message Digest: SHA-1, SHA256, SHA384, SHA512, RIPEMD160
    - Encryption: RSA
  - **adbe.pkcs7.sha1:** deprecated in ISO-32000-2
    - Message Digest: SHA-1
    - Encryption: RSA, DSA
- Use “detached”:
  - **adbe.pkcs7.detached / ETSI.CAdES.detached**
    - SHA-1, SHA256, SHA384, SHA512, RIPEMD160
    - RSA, DSA, ECDSA
  - **Warning**
    - SHA-1 is being phased out
    - Key length ≥ 2048-bit
    - Some combinations won’t work in old versions

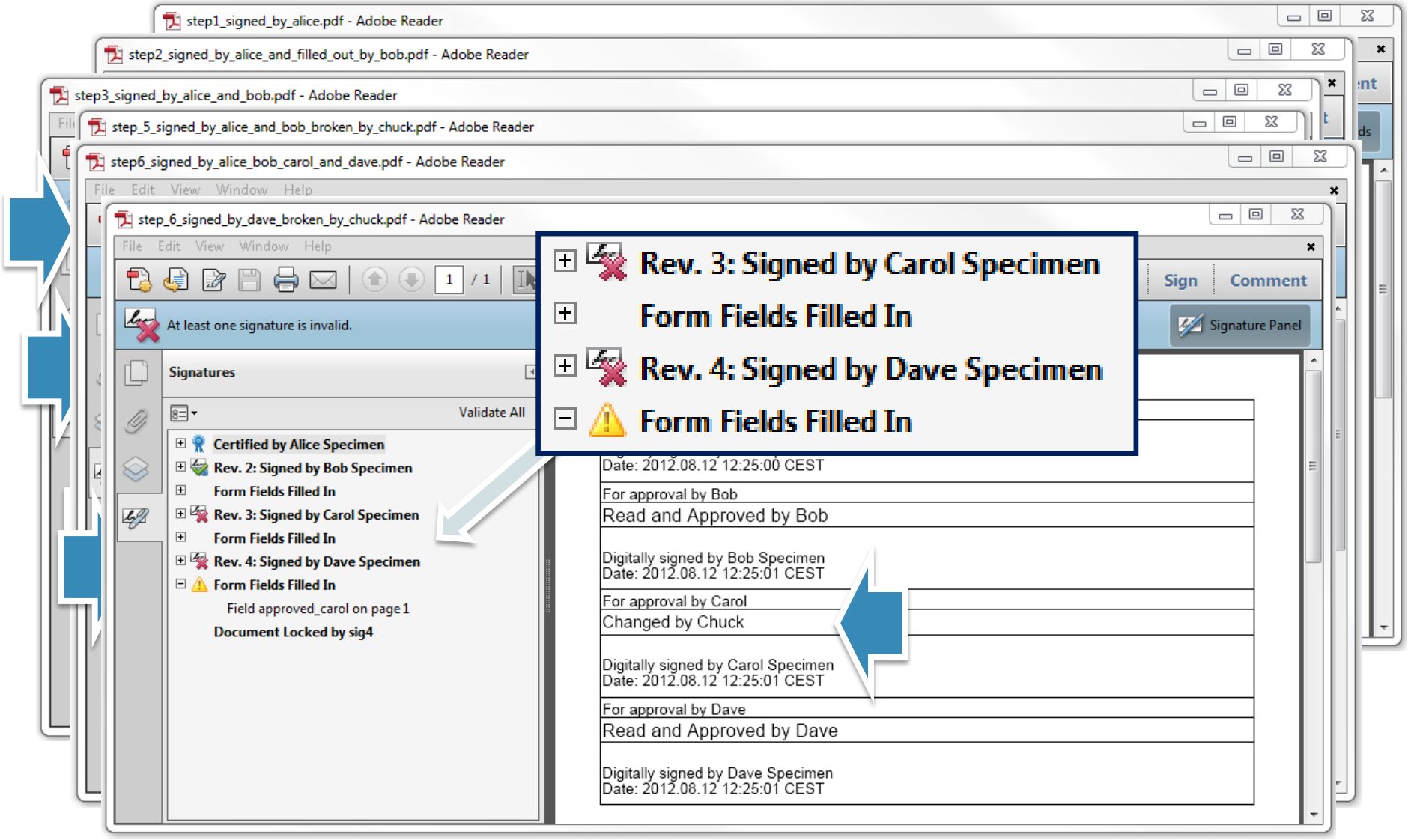
SERIAL SIGNATURES

- A document can be signed more than once.
- Parallel signatures aren't supported
- Additional signatures sign all previous signatures

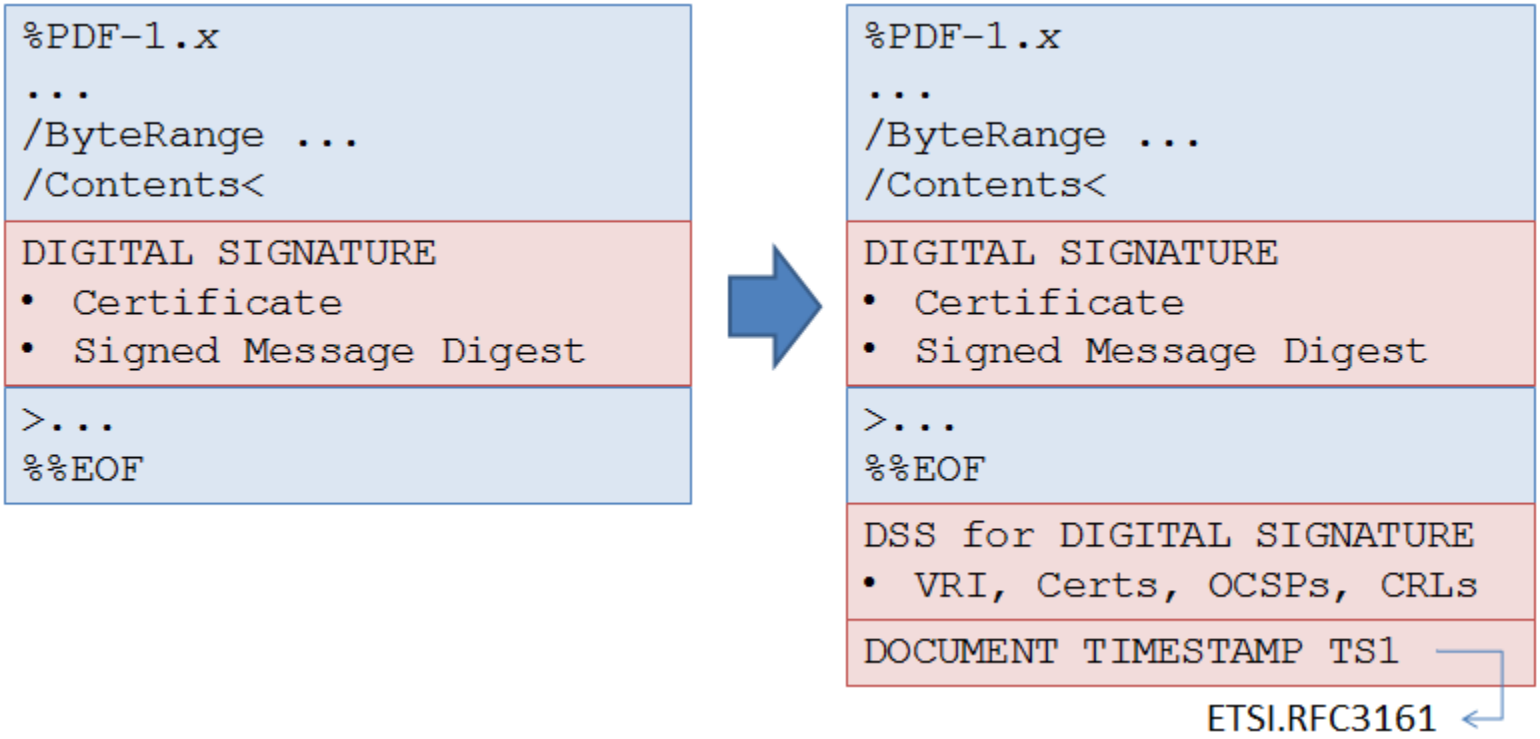
- At most one Certification (aka author) signature; modification detection and prevention (MDP)
- Multiple Approval (aka recipient) signatures
- At most two Usage Rights signatures



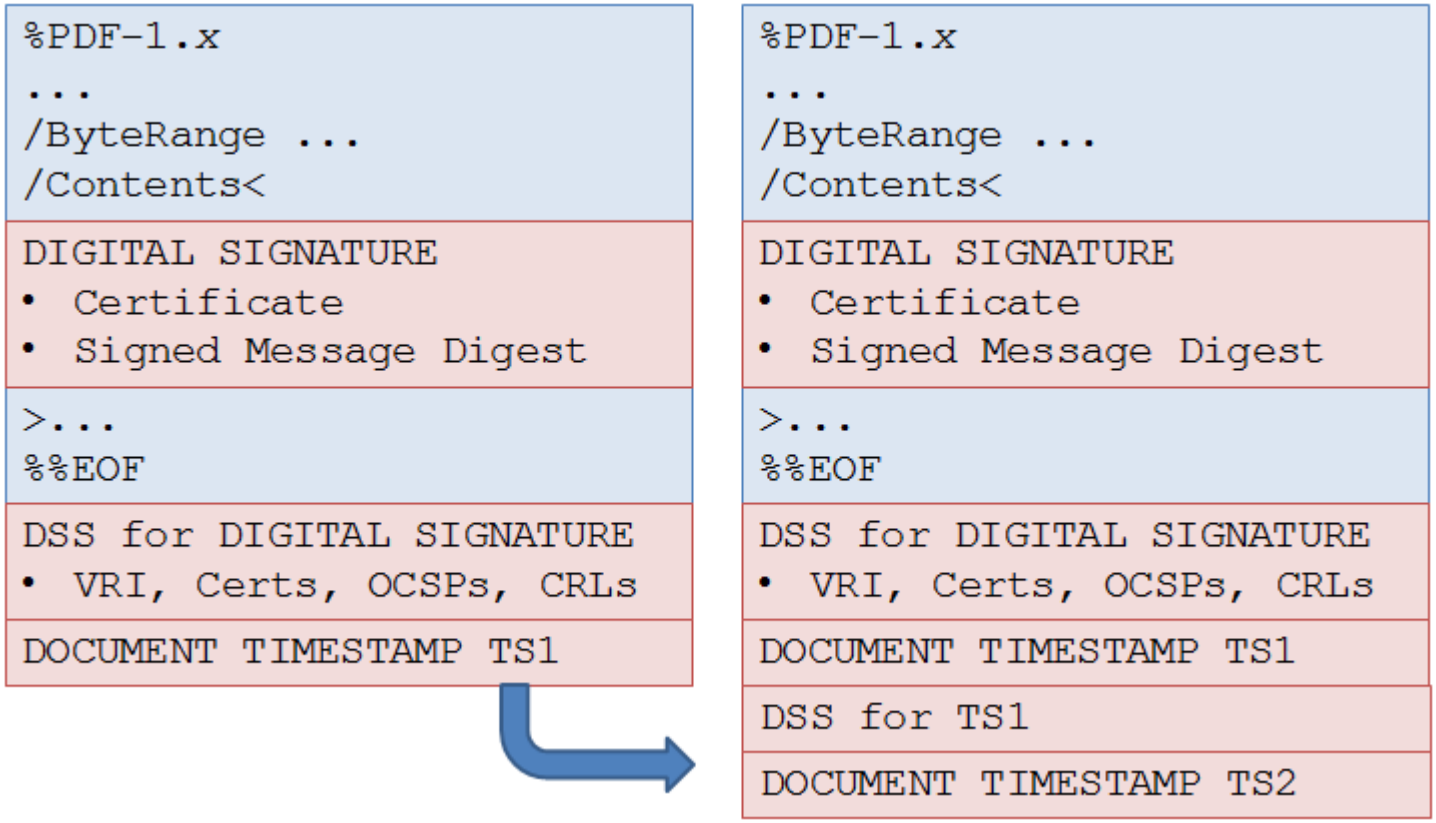
SERIAL SIGNATURES: WORKFLOW



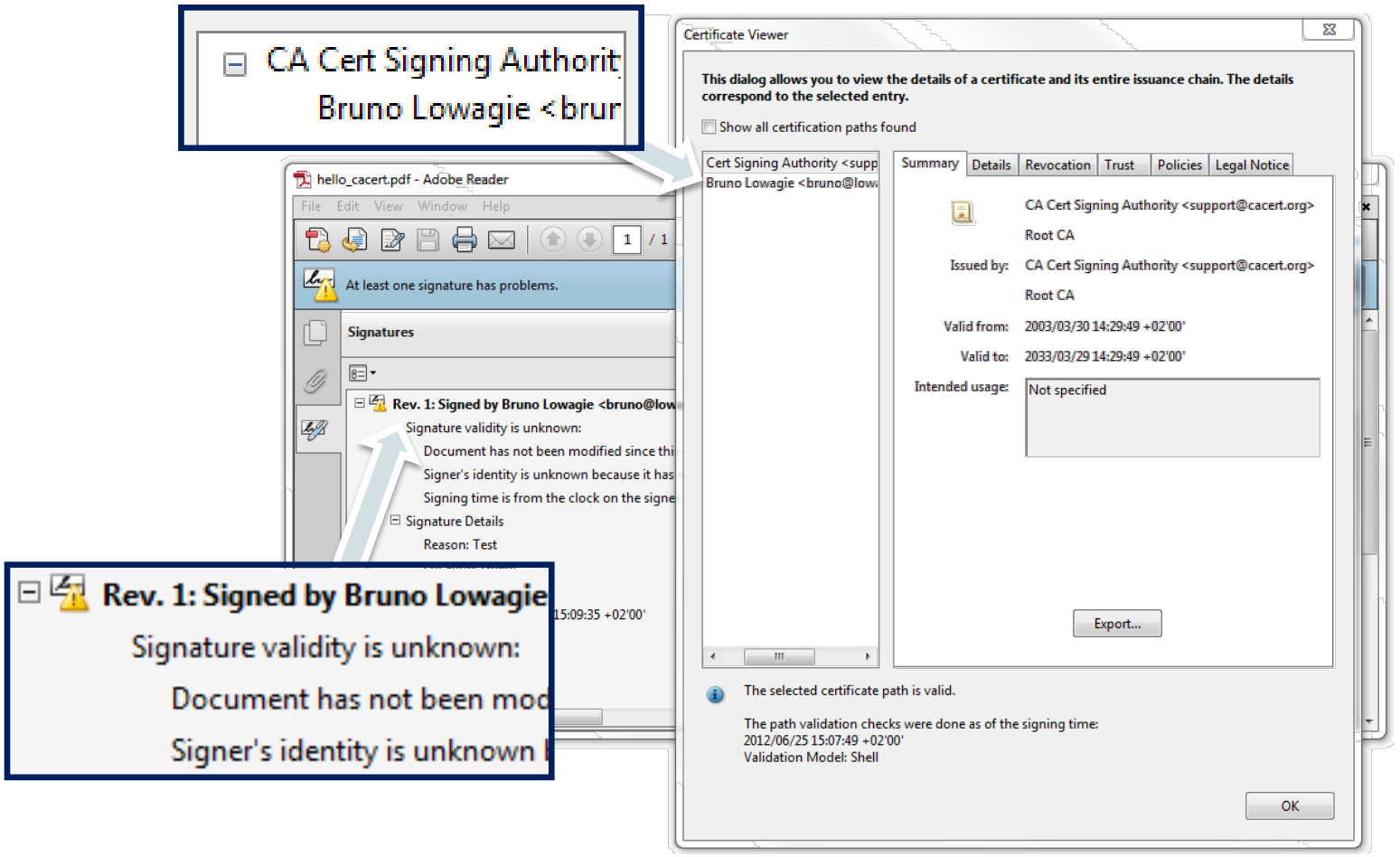
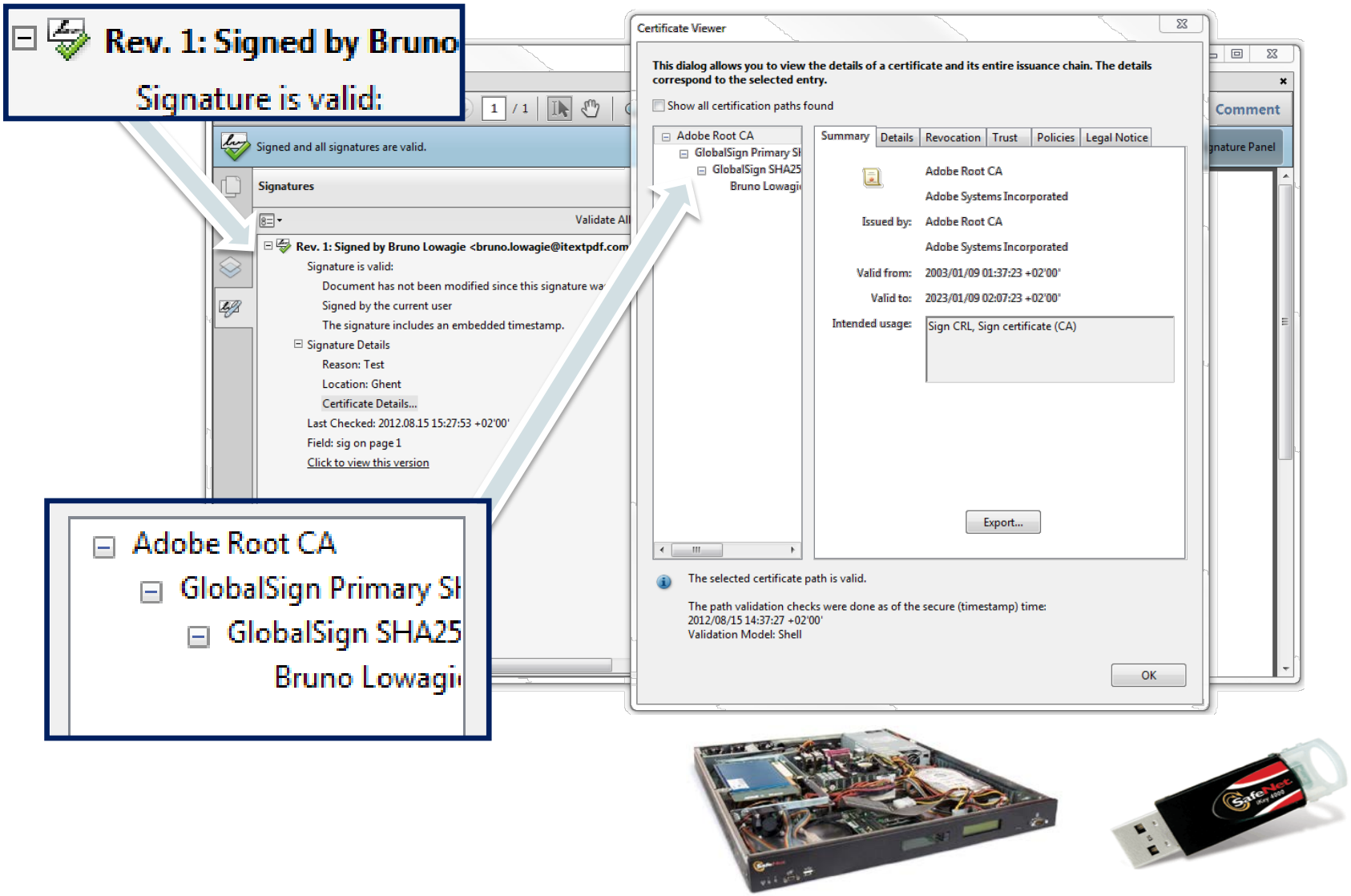
SERIAL SIGNATURES: LTV



LONG TERM VALIDATION



YELLOW TRIANGLE



GREEN CHECK MARK: CDS / AATL