



Open Standards for Electronic Documents and Digital Signatures

James C. King

Senior Principal Scientist

Adobe Systems Incorporated

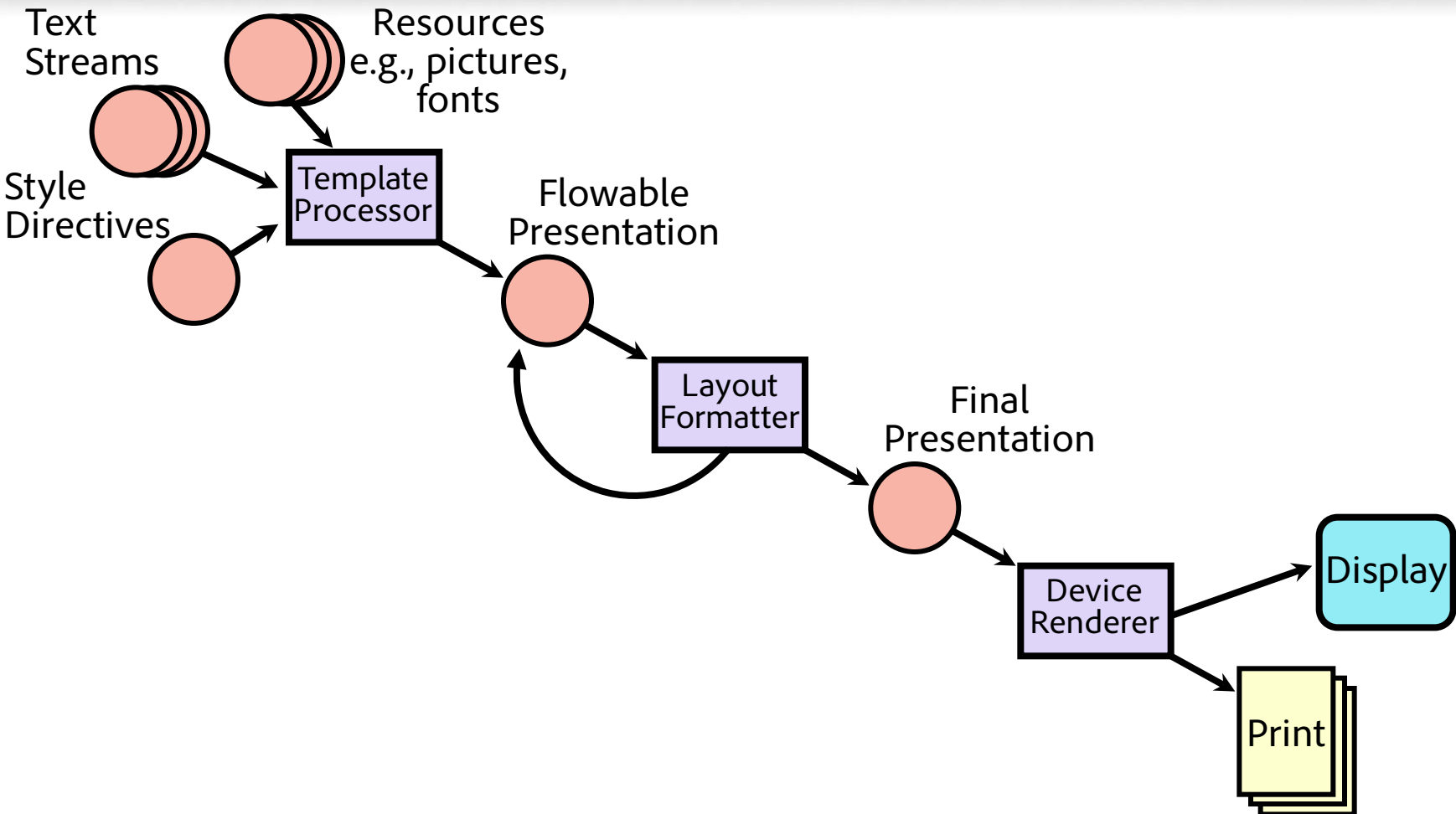




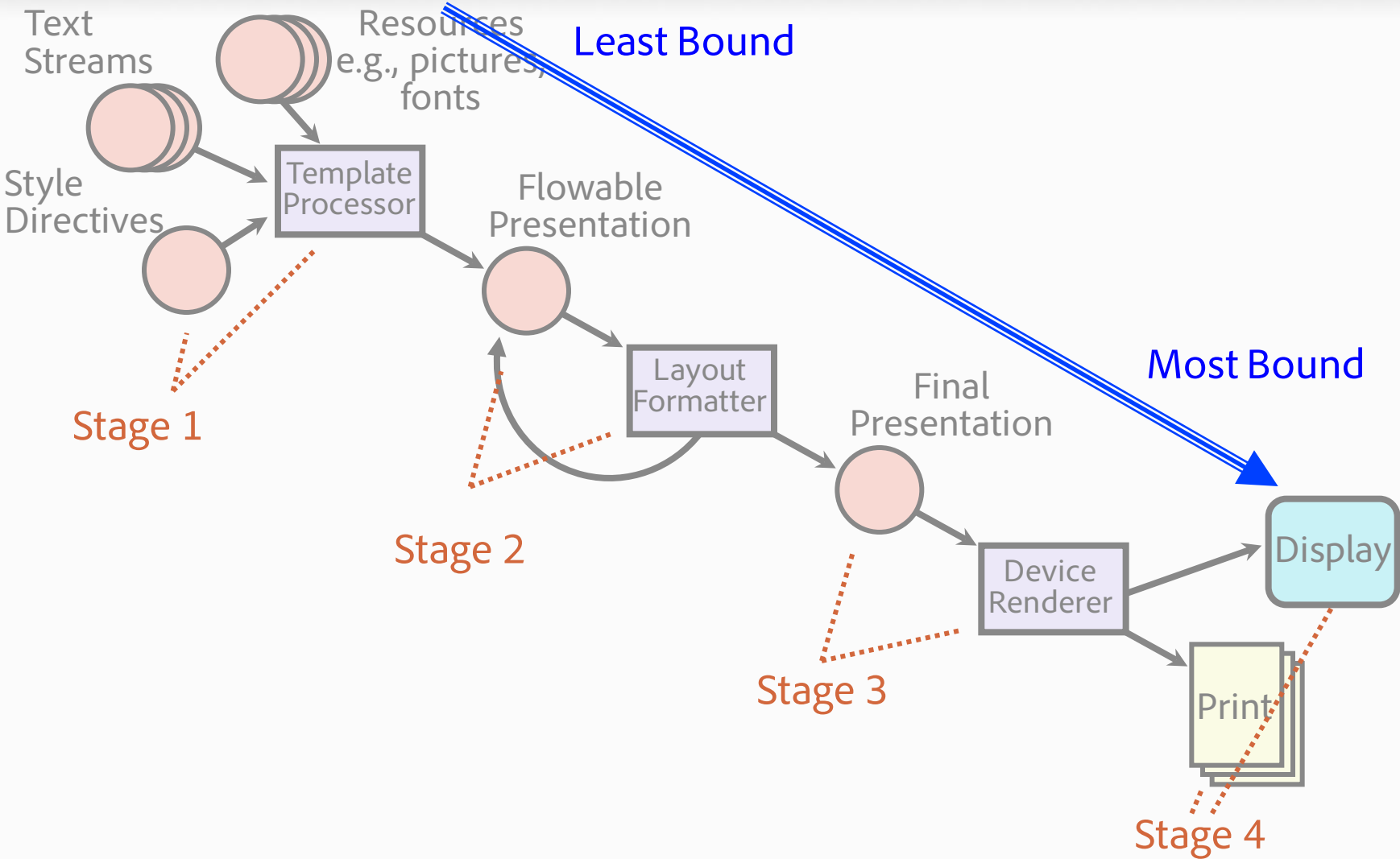
A Presentation in Four Parts

- Stages of Document Development
- Portable Document Format (PDF)
- Digital Signatures for Documents
- PAdES

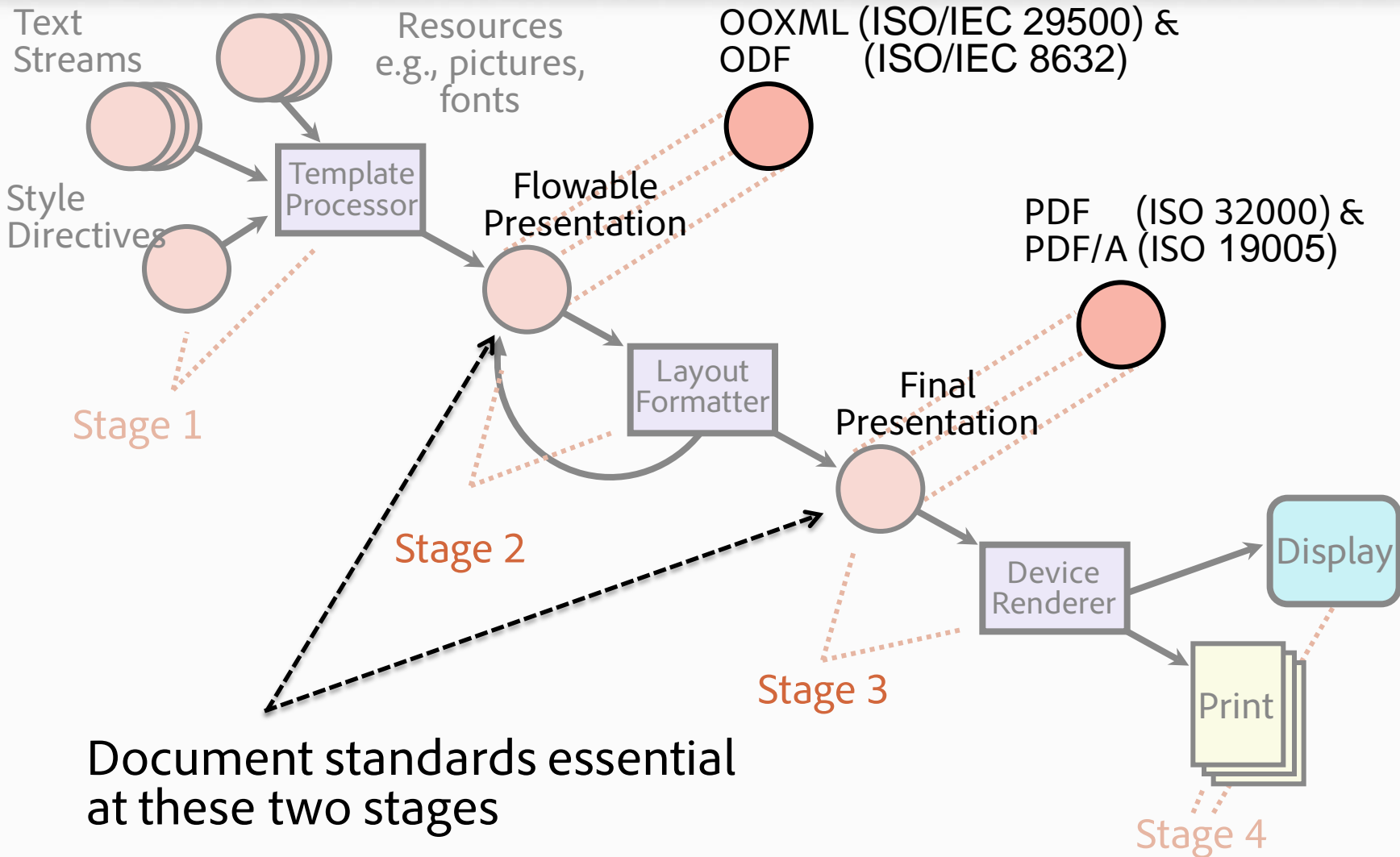
Stages of Document Development



Being Bound to the Output Device – the Stages



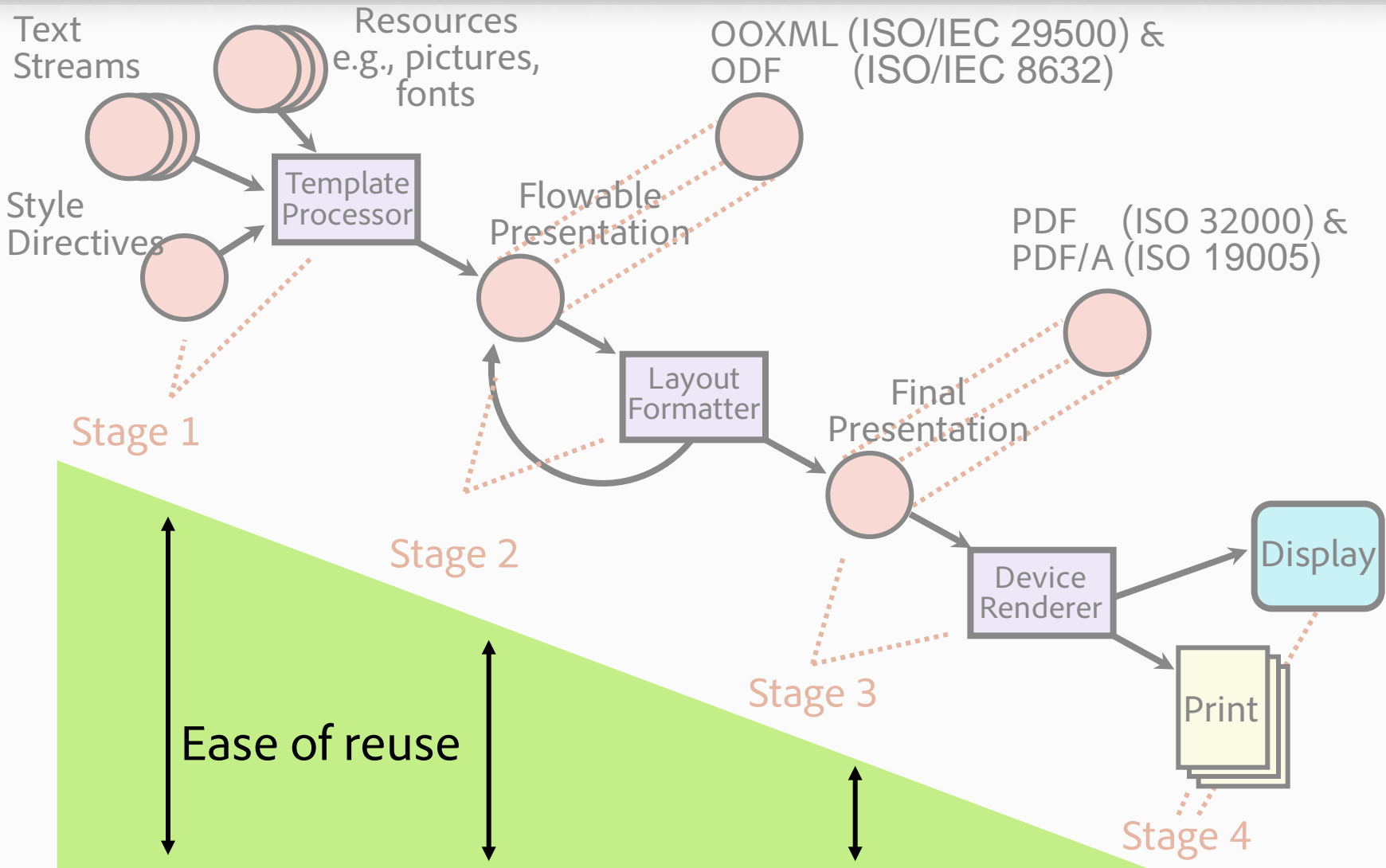
ISO Document Format Standards at Stage 2 and Stage 3



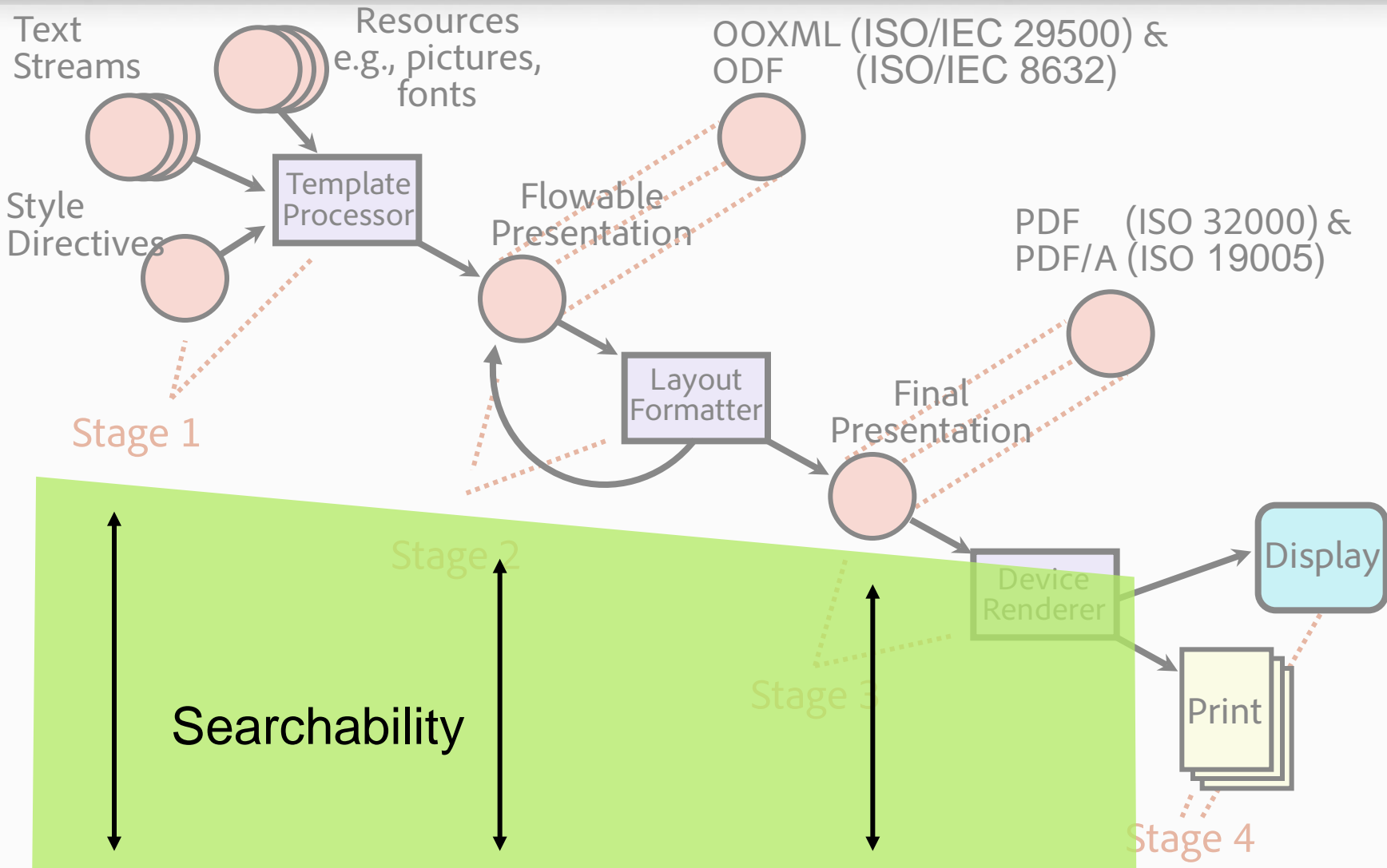


Document Reuse, Search and Presentation Fidelity

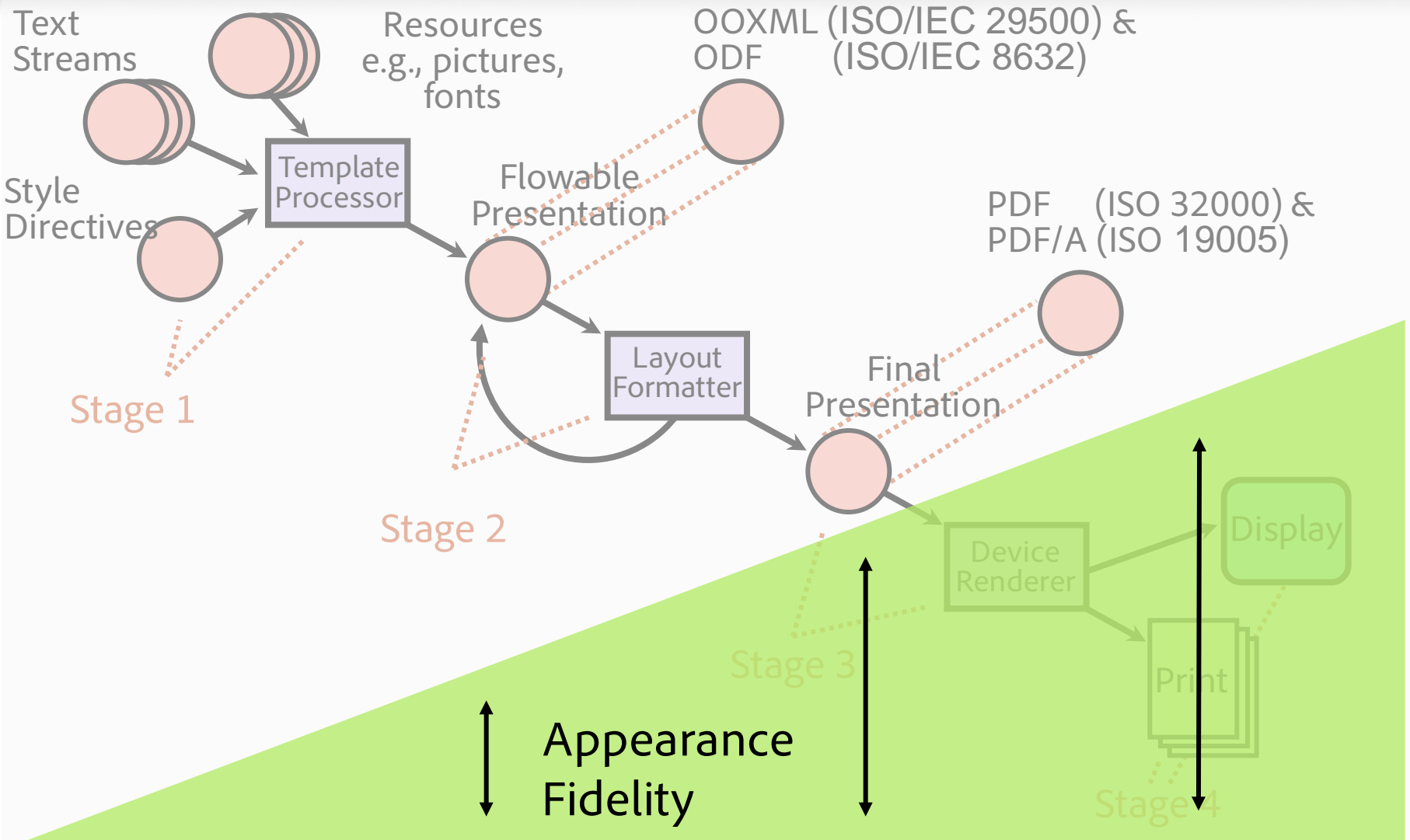
Reusing Document Content



Searching Document Content



Preserving Author's Design

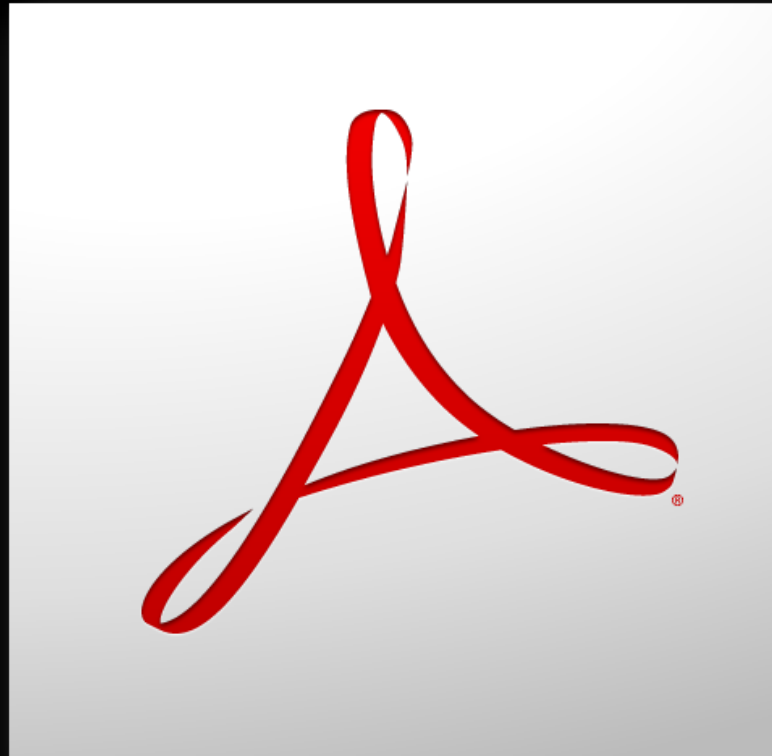




Stages of Document Development and Digital Signatures

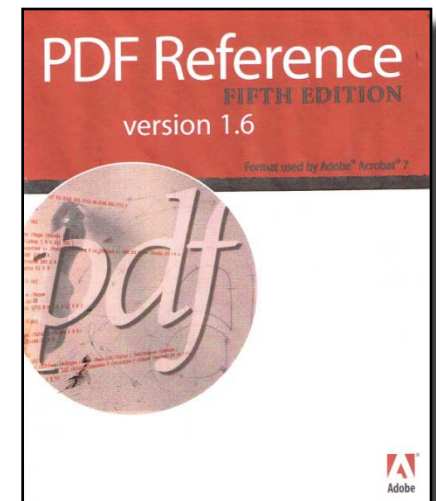
- Signing and change
- Digital signatures detect changes in the document
- If format supports an “undo” function
 - Sign, change, sign
 - Really two documents, original signed and changed signed
- PDF supports appended incremental update

Portable Document Format PDF



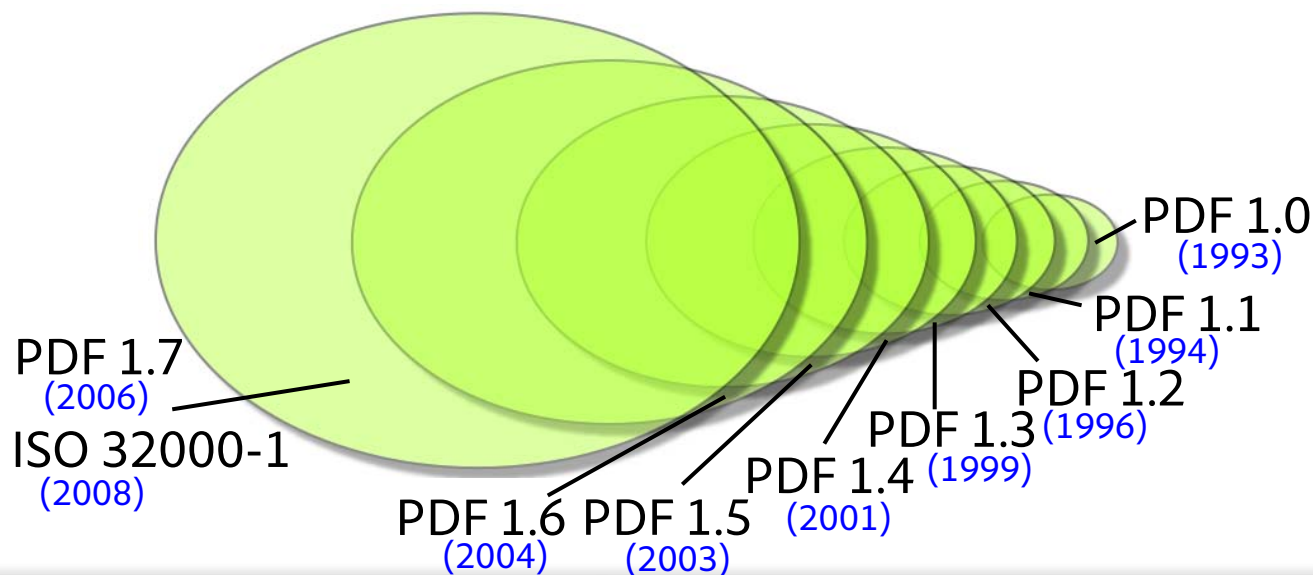
Portable Document Format (PDF)

- Defined by Adobe
 - Full specification released as Addison Wesley book in June 1993
 - Specification on Adobe's website and/or revised book for each new release
- **Thousands** of software applications that process PDFs
- Created by **hundreds** of developers
- **Billions** of PDF files
- Large existing ecosystem



PDF (1993 – 2008)

- An ISO standard: [ISO 32000-1](#)
 - Approved by ISO in January 2008
 - Published by ISO in July 2008
 - Same as PDF 1.7 which includes digital signatures
- Adobe has signed an intellectual property agreement with ISO
 - No Adobe restrictions to develop software to process PDF; never was



**Once a PDF,
always a PDF**



Digital Signatures for Documents

PDF Digital Signatures





PDF Document Digital Signatures

- ISO 32000-1 (PDF 1.7)
- Uses existing standards to sign PDF files
 - PKCS#1, PKCS#7
 - ASN.1, X.509 (CRL, OCSP, TSP, SHAnn, RPKM)
 - XMLDigSig
- Embeds the signature within the PDF file
- Can show visual appearance of signature as form field



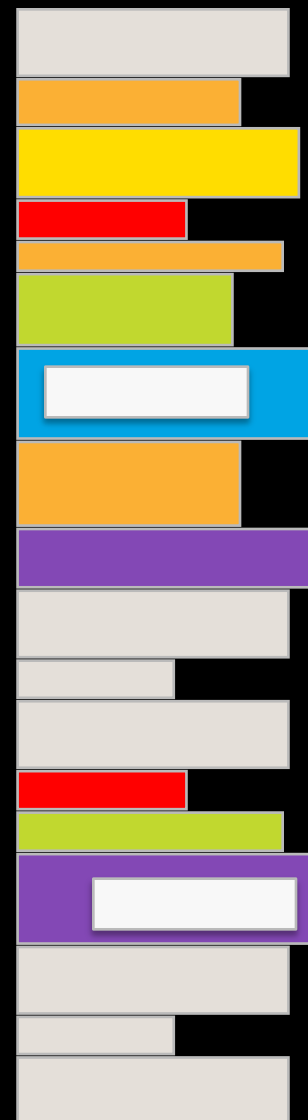
Certified Document Demonstration

- Certify this file with a certificate held in USB Smart Token
 - Hash is transferred to USB Token where it is encrypted (signed) and returned
- Status summarized in ribbon at top of window
- The signature panel can be opened to display all details



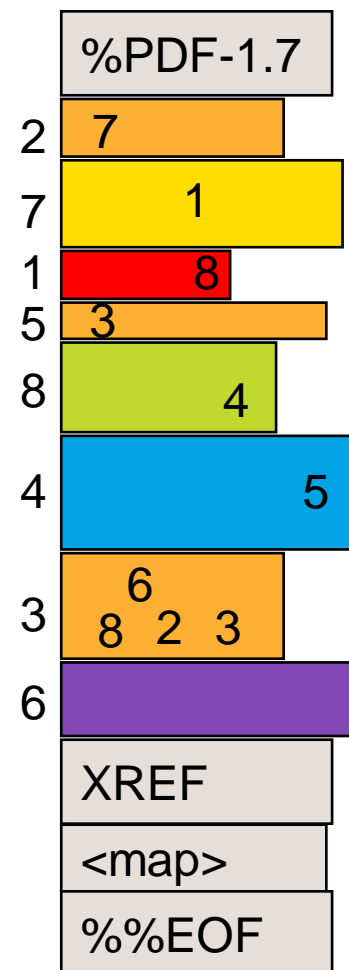
PDF Architecture

PDF Objects (COS)



PDF Objects

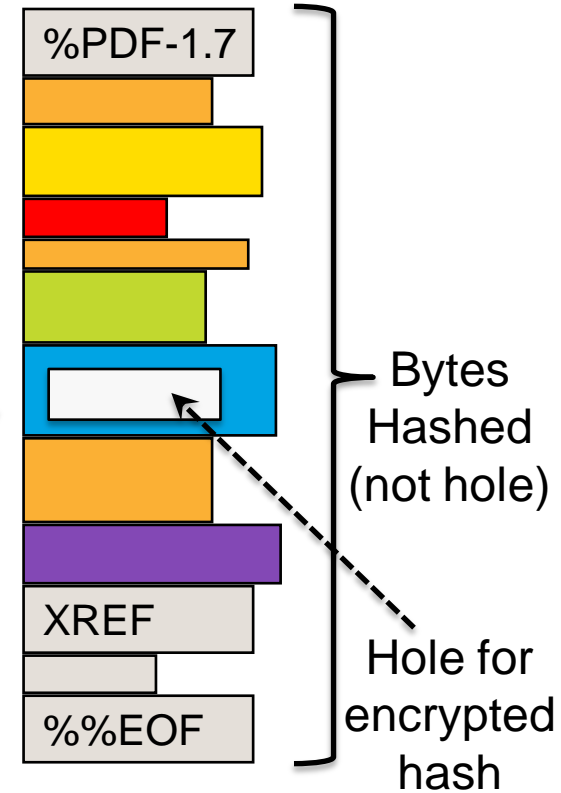
- PDF file is a collection of numbered objects
- Objects can reference each other by their numbers
- XREF at end of file maps numbers to file offsets
- Objects include: numbers, arrays, dictionaries, names, true, false, strings, streams



Signature Object

- Signature Object contains encrypted message digest
 - Digesting skips the hole
 - Avoids the circular problem of digesting the digest
 - Digest dropped into hole after hash & encryption

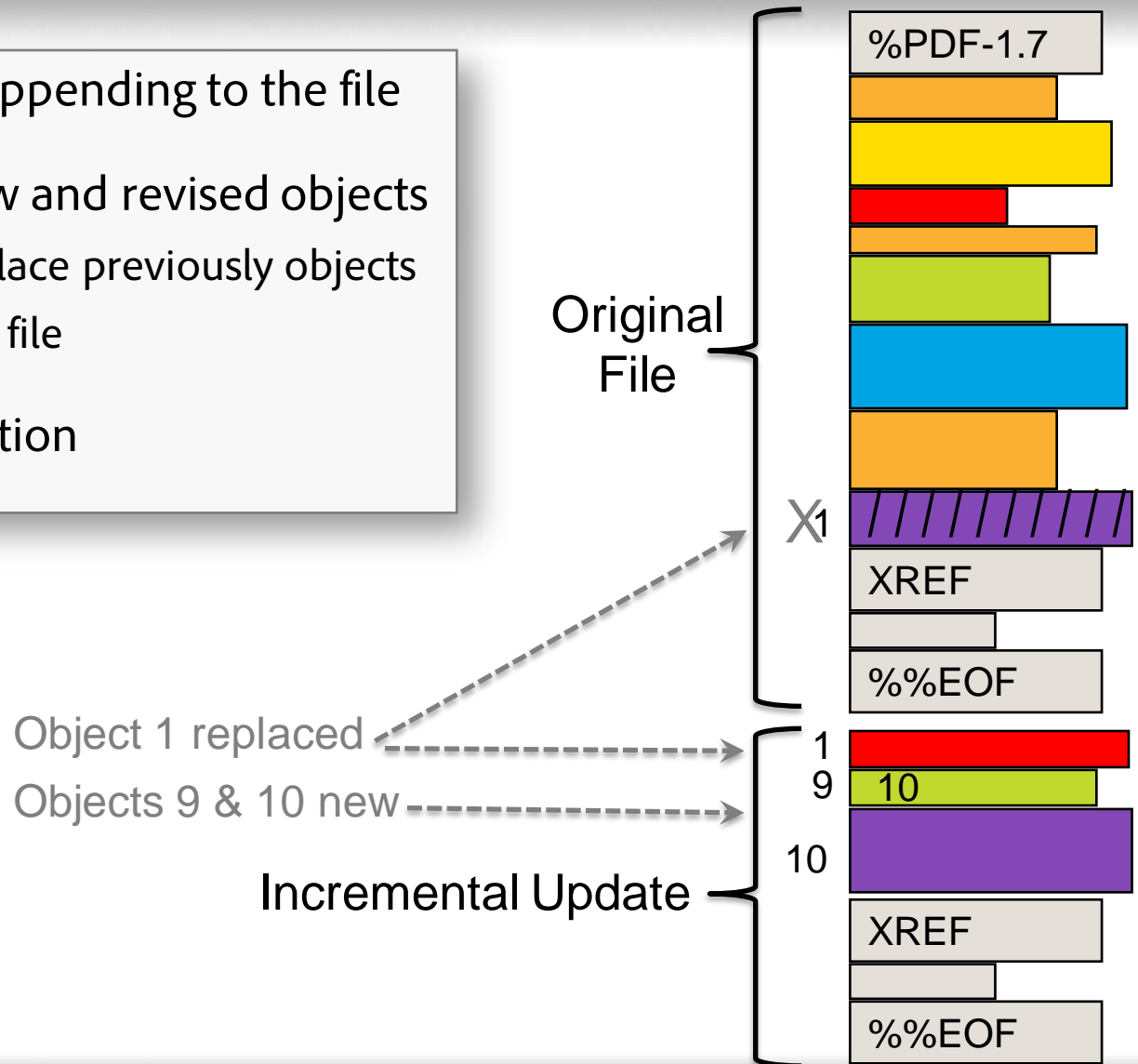
Signature Dictionary Object



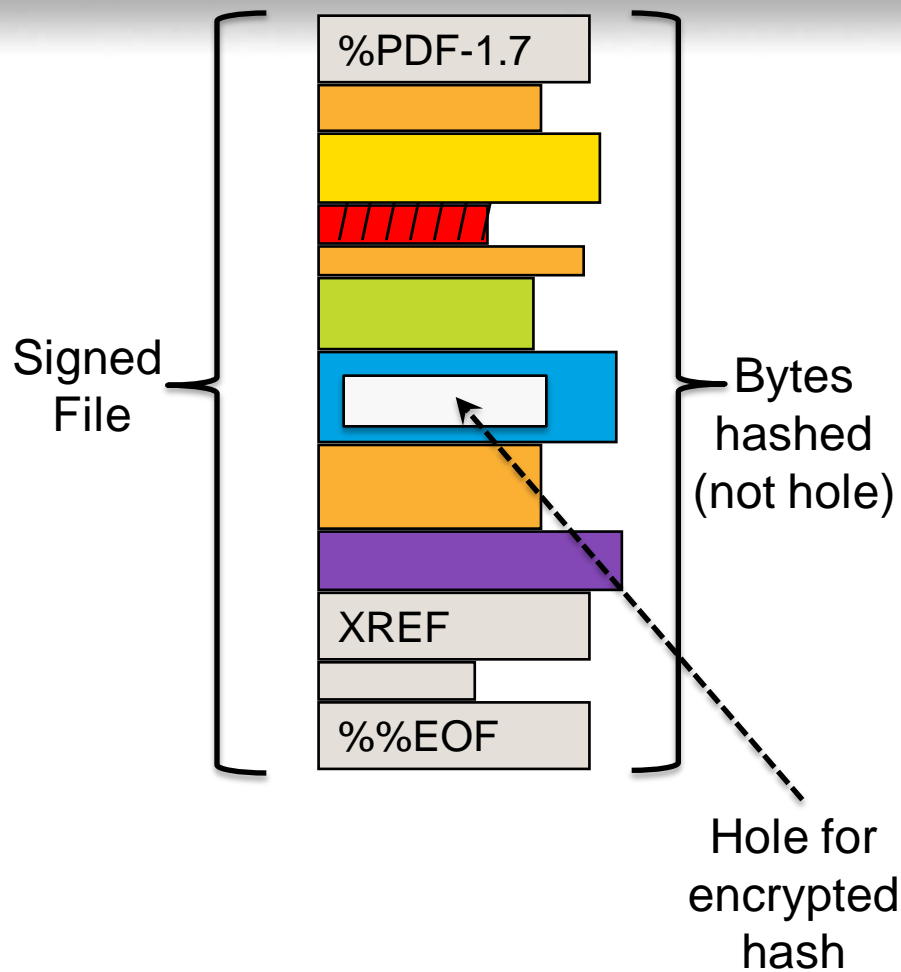
Signed PDF File

Incremental Update

- Incremental update by appending to the file
- Appendage contains new and revised objects
 - Matching numbers replace previously objects
 - Unlimited updates to a file
- Provides for "undo" function



A Signed File





Sample Form To Be Signed

~~~Lease Agreement~~~

Lease agreement for property at 6698 Happy Mountain Road, Sleepy Hollow, NL. Rent is €1200,00 per month payable on the first day of each month. The lease is to run month to month with 5 day notice to terminate by either party. A deposit of one month's rent from Lessee is required upon signing this lease and will be return at the end of the term, excessive damage being paid for first.

Name of Landlord

Date signed

Signature of Landlord

Name of Lessee

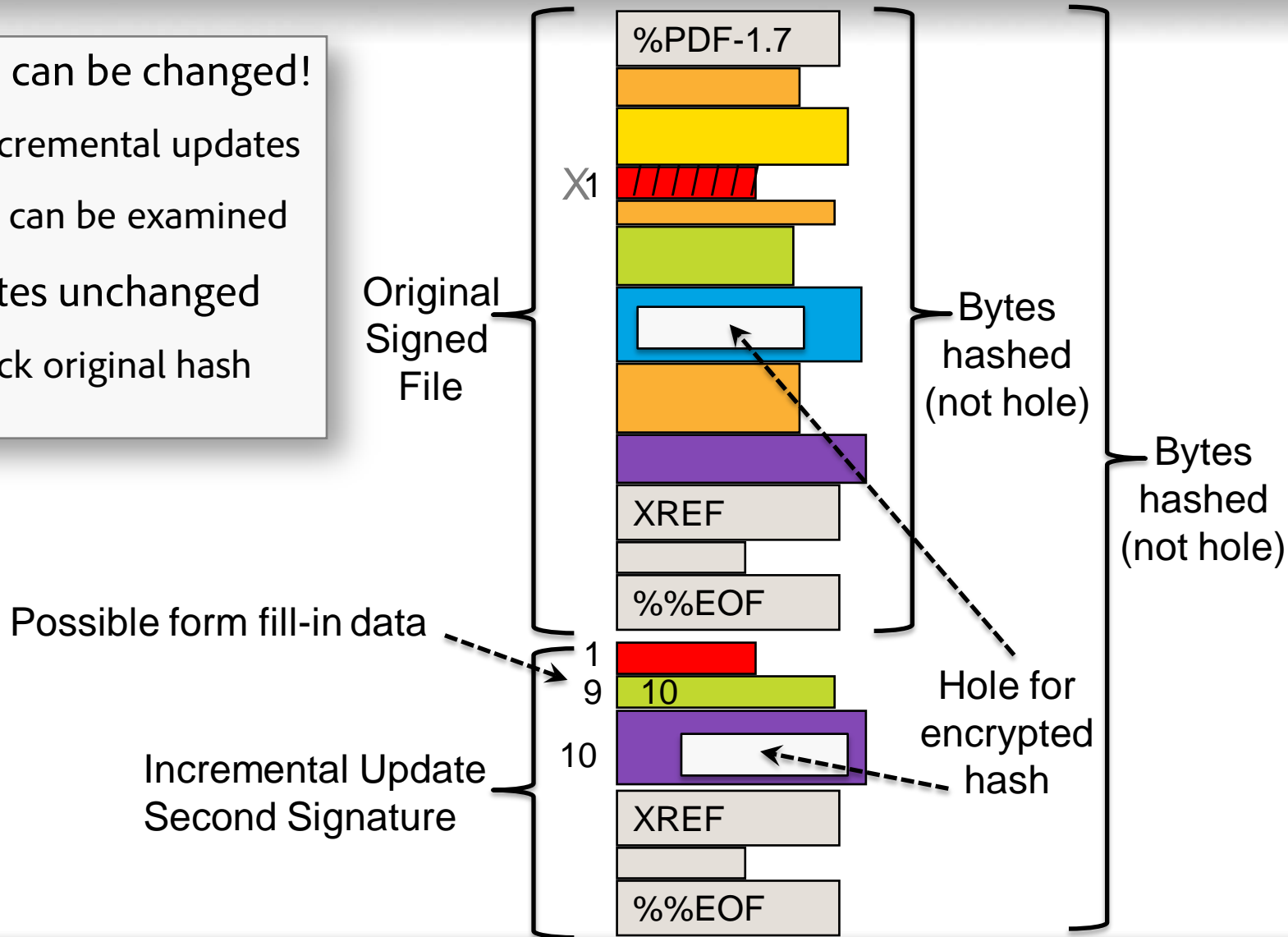
Date signed

Signature of Lessee

~~~~~

# Incremental Update to a Signed File

- Signed files can be changed!
  - Using incremental updates
  - changes can be examined
- Original bytes unchanged
  - Can check original hash





# Reminder

- Changing the file cannot be prevented
  - We detect changes
  - Determine if they are allowed
  - Alert user, if not allowed

# PADES

PDF Advanced

Electronic Signatures



**European Telecommunications**  
**Standards Institute**

# PDF Advanced Electronic Signatures

- Introducing PAdES (available July 2009)
  - ETSI Standard
  - Brings AdES to PDF
  - Sibling to CAdES and XAdES
  - Profiles for the proper use of PDF digital signature in the EU
  
- TS 102 778 (in 5 Parts)



- CAAdES
  - Extends CMS (an extension of PKCS#7)

- PAdES

ISO 32000-1 compatible usage:

- PAdES Part 2 uses PKCS#7 with CMS and CAAdES options

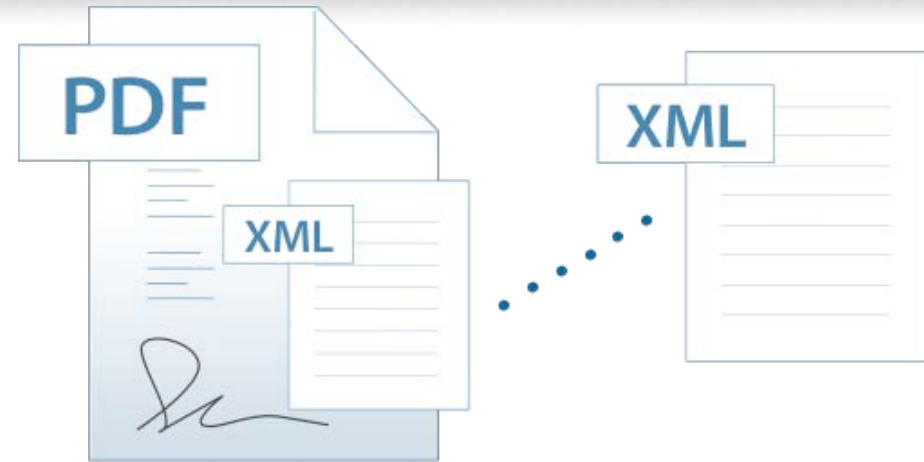
Extensions to ISO 32000-1 aimed for ISO 32000-2:

- PAdES Part 3 uses CMS exactly as CAAdES-BES
- PAdES Part 4 uses incremental update to add LTV features
- PAdES Part 5 uses XAdES instead of XMLDigSig
  
- PAdES Part 1 describes the framework for the other parts

# The AdES Family – A Comparison

## PAdES

- Signatures contained within the PDF
- Supports XML data
- Included in ISO 32000-1 standard
- Signing and verifying included in PDF software – no customization/programming required
- Support serial form-fill and signatures for approval workflows
- Signatures may include a visual appearance within the PDF content
- Long-term validity

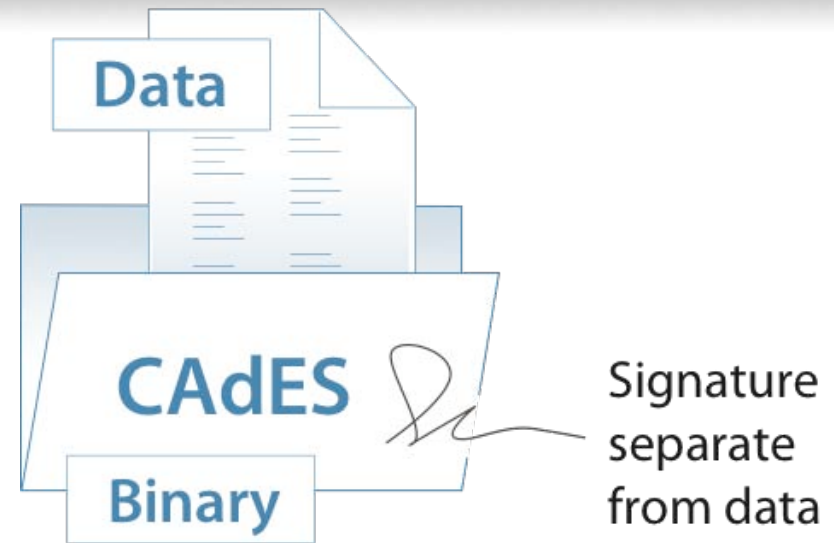


Self-contained  
signature

# The AdES Family – A Comparison

## CAdES

- Can sign any data including PDF
- Oriented toward binary data
- Two signing methods:
  - Detached: the data being signed is separate from the signature
  - Encapsulated: the data is wrapped within the signature structure
- Often requires customization of applications, or generic signing outside of application
- Support multiple signatures applied in parallel, serial by repeated signing
- Appearance is up to the application to provide
- Long-term validity



# The AdES Family – A Comparison

## XAdES

- Can provide an XML solution
- Can sign any data including PDF and binary
- Often requires customization of applications, or generic signing outside of application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Appearance is up to the application to provide
- Long-term validity





# Summary

- Need both editable **and** final form standards
- PDF is an open public standard (ISO 32000)
- ISO 32000 (PDF) supports digital signatures
- PAdES: ETSI standards for PDF digital signatures

- ISO 32000-1 (PDF 1.7)
  - [http://www.adobe.com/devnet/acrobat/pdfs/PDF32000\\_2008.pdf](http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf) OR
  - <http://www.iso.org/iso/pressrelease.htm?refid=Ref1141>
- PADES
  - Adobe white paper [http://blogs.adobe.com/security/91014620\\_eusig\\_wp\\_ue.pdf](http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf)
  - Part 1 : [http://webapp.etsi.org/workprogram/Report\\_WorkItem.asp?WKI\\_ID=31003](http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31003)
  - Part 2 : [http://webapp.etsi.org/workprogram/Report\\_WorkItem.asp?WKI\\_ID=31004](http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31004)
  - Part 3 : [http://webapp.etsi.org/workprogram/Report\\_WorkItem.asp?WKI\\_ID=31005](http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31005)
  - Part 4 : [http://webapp.etsi.org/workprogram/Report\\_WorkItem.asp?WKI\\_ID=31007](http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31007)
  - Part 5 : [http://webapp.etsi.org/workprogram/Report\\_WorkItem.asp?WKI\\_ID=31008](http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31008)
- InsidePDF Blog <http://blogs.adobe.com/insidepdf> (By Jim King)
- Adobe Security Blog <http://blogs.adobe.com/security> (by John B. Harris)
- Home page <http://www.adobe.com/technology/people/sanjose/king.html>



**Adobe**