working together!

PDF Days Europe 2022 | Berlin

Interoperable document based signatures

Roman Toda - Foxit

Signature marketplace

- 3bn USD market in 2021
- 4.05bn projected for 2022
- 35bn USD by 2029
- 36.1% CAGR 2022-2029
- Growth 34.4% in 2020 (compared with 2019)
- Adoption cutting down cost by 80%
- Software 56%, Hardware and services are equal at around 22%
- Key factor for market growth:
  - Improved security
  - Operational efficiency
  - Seamless workflow to propel market growth

History - Regulations

- Legal
  - USA: ESIGN Act(2000), UETA (1999)
  - Europe: ESD(1999), eIDAS(2014)
  - India: IT Act (2000)
- Technical
  - Digital signatures in PDF 1.3 (2000)
  - PAdES
  - ISO 3200-2 and signatures
    - ISO 32001
    - ISO 32002

Use cases

- Self signing a document
  - I sign my document and send
  - Someone prepares document I need to sign
- Multiple parties involved
  - Preparation of a document in advance
- Signing based on policies
- Signing on behalf of someone
- Notaries
- Signing in parallel

What is it?

- Conceptually
  - Capturing the signer's intent
  - Record the intent
  - Actual contract
  - Proof
- Technically
  - Wet signature
  - Digital signature
    - using public-private key infrastructure
    - Hashing, encrypting
    - Recording audit trail

Implementations

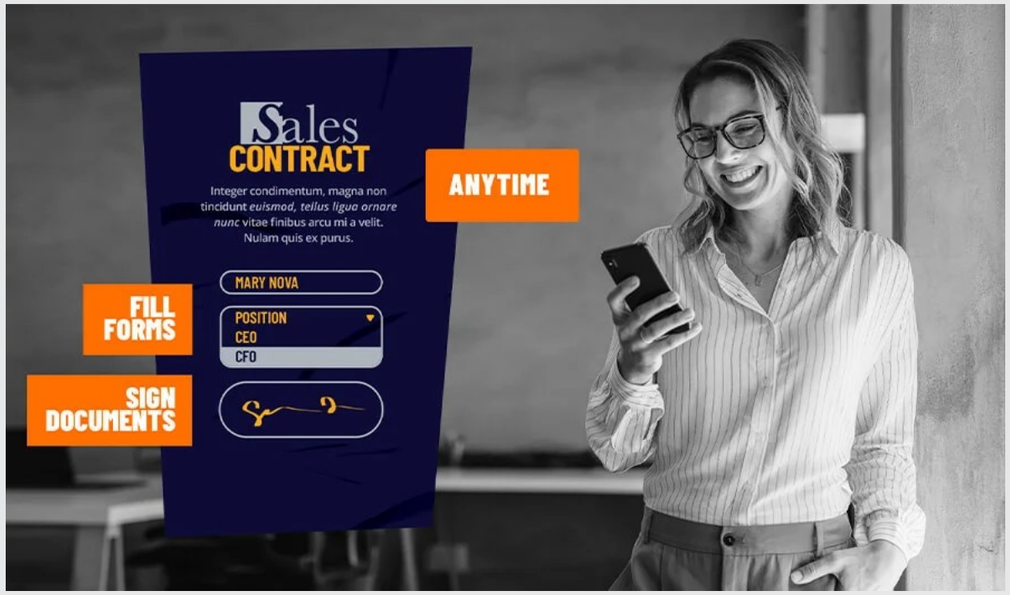
A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authencity), and that the message was not altered in transit (integrity)

vs.

Print & Sign & Scan

E-sign

- It appears as if:
  - don’t care about authentication
  - We believe in integrity
  - We are not expecting to go to court to “prove”
- Reality
  - Digital signature is the implementation of the concept
  - The certificate is used
  - Vendor collects the data (audit trail)
  - Vendor can prove the integrity and authenticity

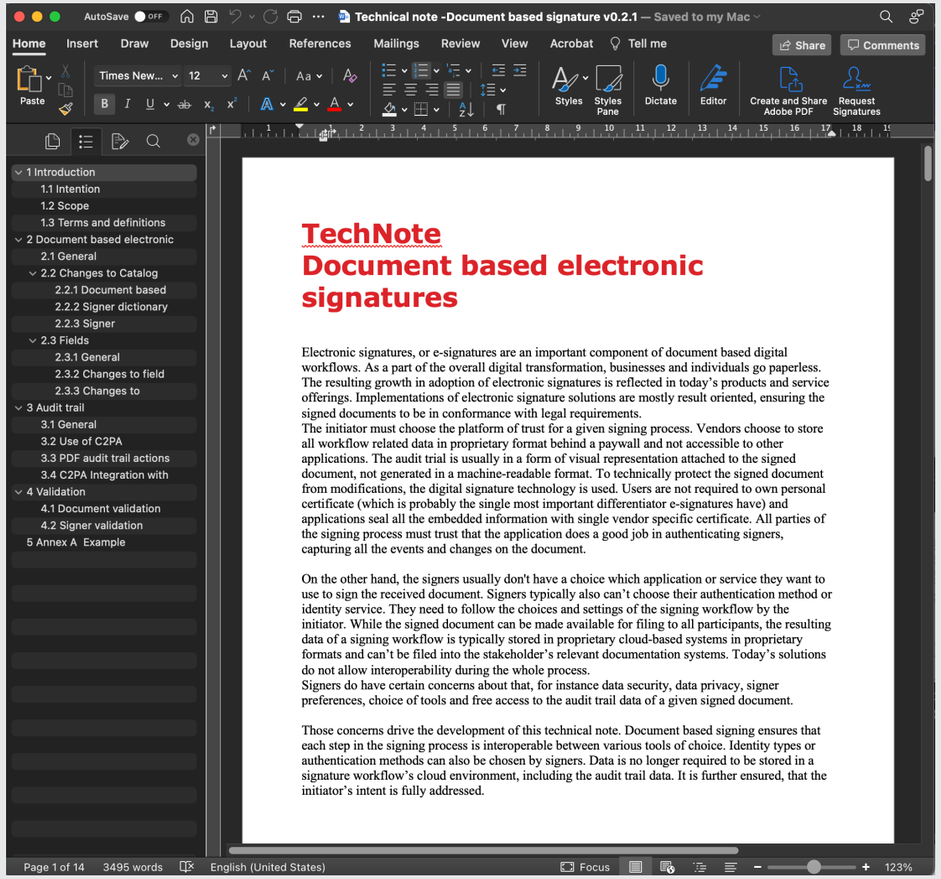


Problems

- Trust in vendor
  - How auth works?
- Audit trail is visual appearance
  - How accurate it is?
- Interoperability
  - Multiple different authentication methods
  - Choice of tools
- Collaboration
  - What means a change on the document?

Document based electronic signature concept

- Easy and verifiable way
- Starts with a document to be signed
- Ends with signed document
- Workflow can be integrated
- Supporting different types of identities
- All information are part of the document
- Standardized data structures
- Backward compatible



WORLD'S #2 PDF PROVIDER

Innovative and Customer-Focused.

CUSTOMERS

485,000+

From SMBs to Global Enterprises

USERS

700m+

EMPLOYEES

850+

ENGINEERS

400+

WORLDWIDE OFFICES

SILICON VALLEY HQ

How?

- We are offering an extension to PDF
- Few prerequisites
  - Document has to be digitally signed (yes – the math stuff)
  - We leverage AcroForm functionality
  - Audit trail is machine readable and protected
- We would cover use cases:
  - Self sign
  - Transaction-based signing
  - Internal control and audit

Technical details

- Perfectly aligned with existing concept of digital signature in PDF
  - can use certificate signature
  - can apply multiple approval signatures
  - can apply time stamp signature
  - can be compatible with PAdES, QES
- Extending
  - Defining a Signer entity
  - Extending AcroForm fields
  - Attaching audit trail information (machine readable)
  - Providing Validation provisions

Workflow

Initiator	Signer(s)	All
• Prepares document • Identifies signers • Defines order • Defines fields (for signers)	• Authenticates • Filles the fields • Applies signature(s) to required fields	• Collection • Validation • Archiving

Workflow definition

- Document catalog dictionary
- Define signers
- Timestamp, certificate signature, permissions (DocMDP, FieldMDP)

Table TN.1 — Document based electronic signature dictionary

KEY	TYPE	VALUE
Type	name	*(Optional)* shall be *DocESign*
Signers	dictionary or array	*(Optional)* If present, shall be an indirect reference to a signer dictionary or an array of such dictionaries. (see *Signer dictionary*, Table TN.2 — Signer dictionary) The signer represents a person, or an entity entitled to sign the document.
Ordered	boolean	*(Optional)* Indicates whether the **Signers** entry shall be treated as ordered. If initiator wishes to treat the list of signers in specific order, the PDF processor shall only allow signing of the document to the first signer who haven't signed the document yet (see. Signer validation) and passed the authentication defined via **AuthPolicy** in the signer dictionary. If the value is false (or not present), the order in which signers sign the document is implementation dependent. Default value: false

Signer

- Abstract object
- Attributes (name, certificate required, private message etc..)
- Authentication method(s)

Table TN.2 — Signer dictionary

KEY	TYPE	VALUE
Type	name	*(Optional)* The type of PDF object that this dictionary describes; if present, shall be *Signer* for a signer dictionary
Name	text string	*(Optional)* The human-readable representation of the name of the person or entity signing the document. The PDF processor may check provided name with the name acquired through one of used authentication methods. In case of self-signing process this value is provided in implementation dependent way.
AuthPolicy	dictionary or array	*(Optional)* A signer Authentication method dictionary or an array of such dictionaries (see Signer Authentication policy dictionary) used to capture the authentication method for verifying signer's identity If empty array or not present the authentication isn't required
AuthType	name	*(Optional; shall only be present if* **AuthPolicy** *is an array)* A name specifying how the authentication method are processed. Valid values shall be: *All* – all authentication methods defined by **AuthPolicy** array shall be successfully processed *OneOf* – the PDF processor may decide (or let user decide) which authentication method is used Default value: *All*
PrivateMessage	text string	*(Optional)* A text string that is used to specify any information the initiator wishes to present to the signer in an implementation dependent way.

Authentication method

- AuthMethod is a handler
- AuthPolicy definition
- Open for implementers
- OAuth2, Tokens, corporate DB, cloud accounts .. Open ended

Table TN.3 — Signer Authentication policy dictionary

KEY	TYPE	VALUE
Type	name	*(Optional)* Shall be *AuthPolicy*
Subtype	name	*(Required)*The name of authentication method The used values would typically be: *OAuth2, Email, Phone, SMS* A second class name may be used (see ISO 32000-2 Annex E, "Extending PDF") to identify vendor's specific authentication methods.
URL	string	*(Optional; Required if **Subtype** is a second class name)* A URL that refers to the documentation for this authentication method.

Fields

- The use of AcroForms
- Predefined subtypes (Date, Company, Print name etc..)
- Standard Sig field is used
  - Allowed subtype being full signature and initials
- Fields contain a connection with Signer
- V (value) key is shared between Sig fields = single digital signature

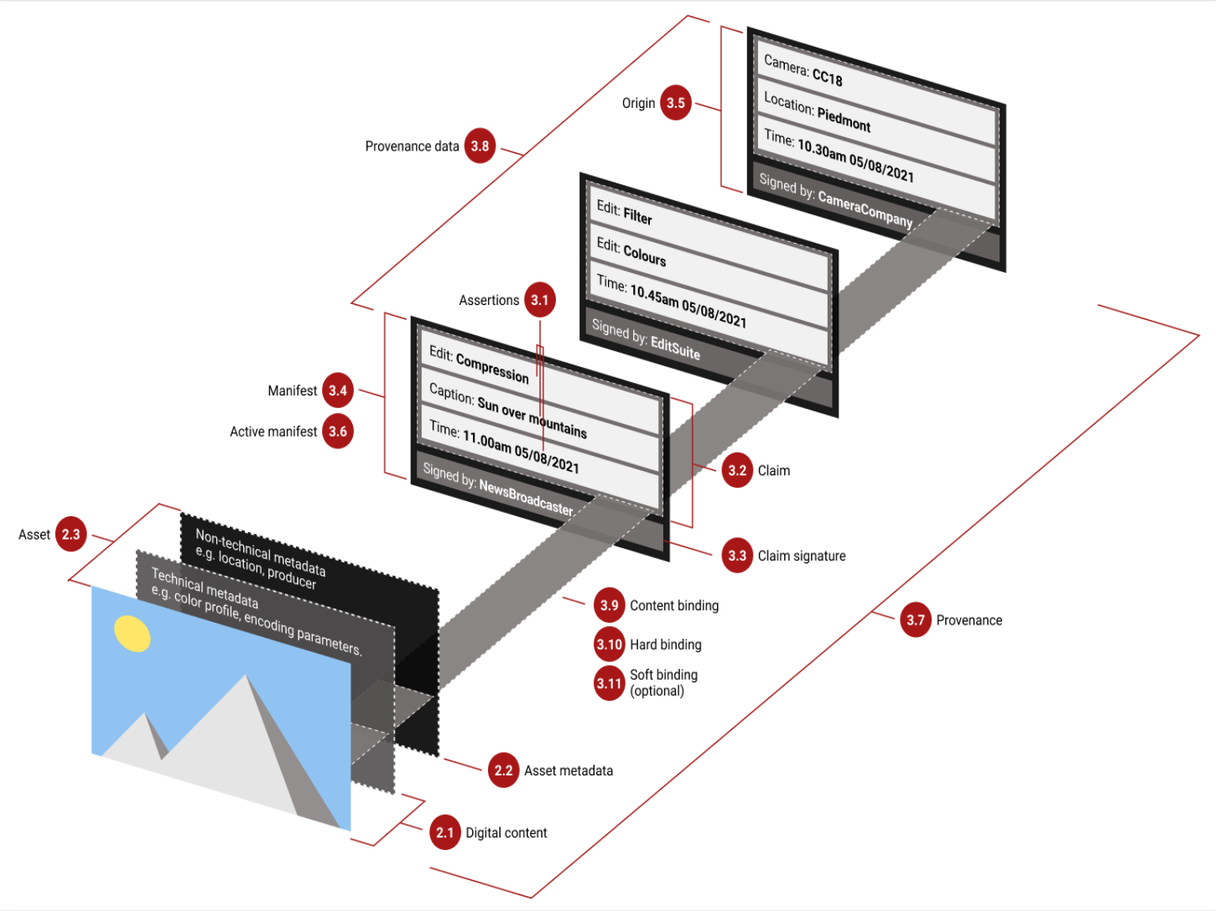
Addition to section ISO 32000-2, 12.7.4 Field dictionaries

Table 226 — Entries common to all field dictionaries

KEY	TYPE	VALUE
FST	name	*(Optional)* Field subtype, the name representing the field type Valid values shall be: *Title* *Company* *Name* *Email* *Initials* *FullSignature* Values *Initials* and *FullSignature* shall only be used for Signature fields when **FT** is *Sig* and the field dictionary is a subject of additional requirements as defined in Changes to Signature dictionary. The use of other values is implementation dependent. NOTE: It is valid for example to use the field subtype Company in a Choice field dictionary as well as in a Text field dictionary
Signer	dictionary	*(Required if **FST** is present)* a Signer dictionary (see Signer dictionary). If the signer was predefined by the initiator, then this entry shall be an indirect reference and shall also be included in the **Signers** entry in the document based electronic signature dictionary (see Document based electronic signature dictionary) Otherwise, the field create with self-signing method

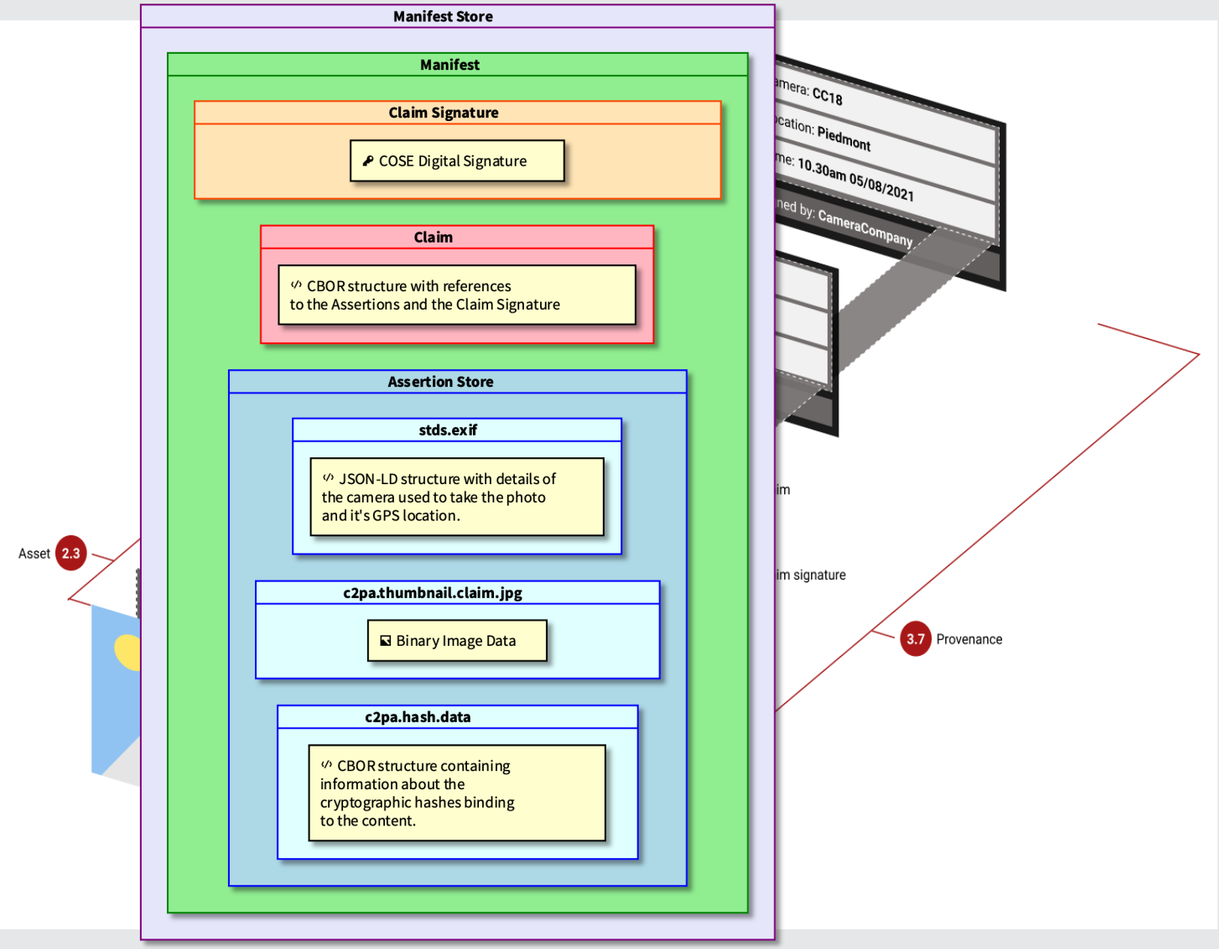
Audit trail

- From straightforward ideas
  - PDF based dictionaries
  - Attached log file in native format
  - Audit trail handler ?
- C2PA
  - Open specification
  - JSON based, structured list of actions
  - Secured by digital signature
  - Attachment annotation on PDF with such JSON



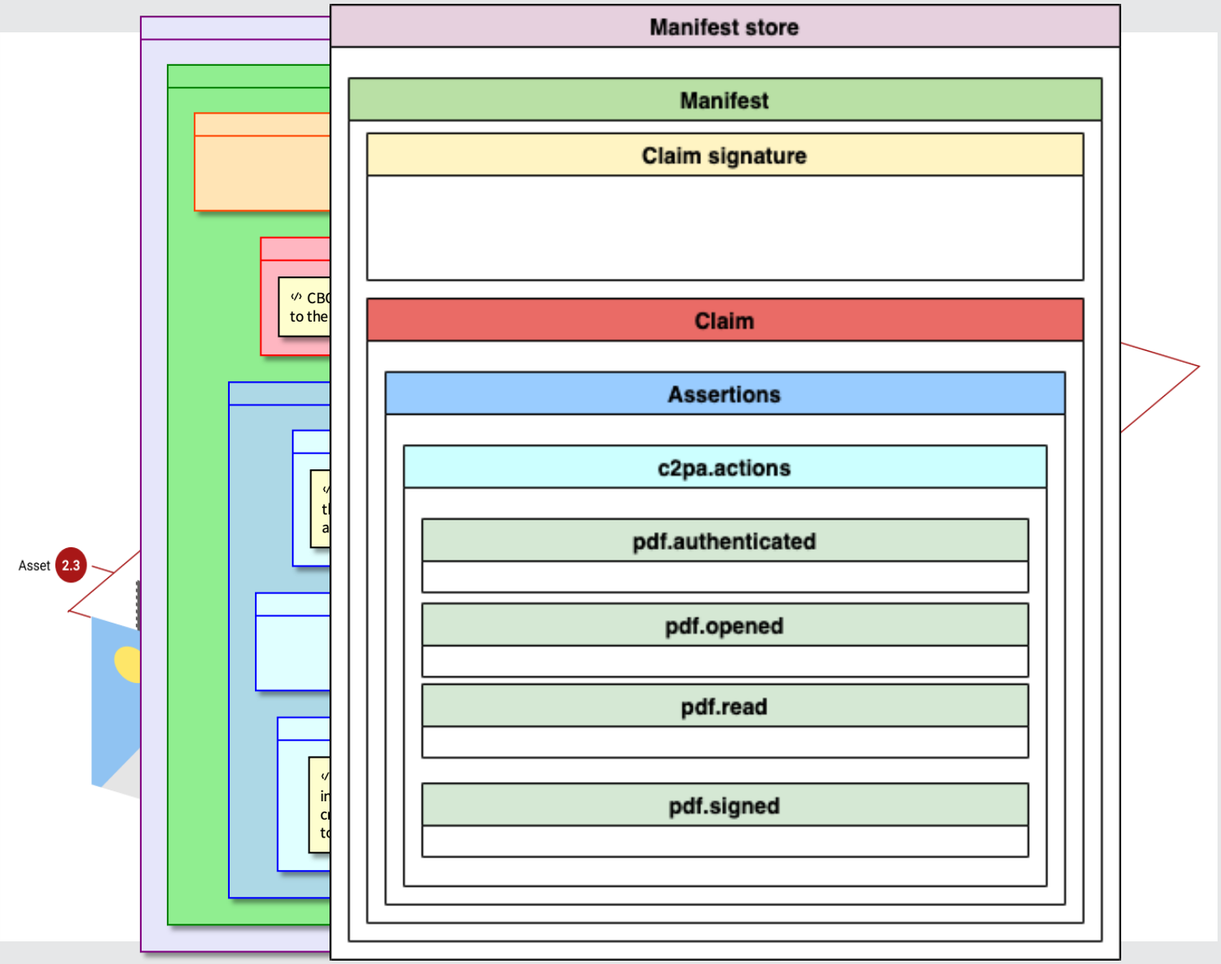
Audit trail

- From straightforward ideas
  - PDF based dictionaries
  - Attached log file in native format
  - Audit trail handler ?
- C2PA
  - Open specification
  - JSON based, structured list of actions
  - Secured by digital signature
  - Attachment annotation on PDF with such JSON



Audit trail

- From straightforward ideas
  - PDF based dictionaries
  - Attached log file in native format
  - Audit trail handler ?
- C2PA
  - Open specification
  - JSON based, structured list of actions
  - Secured by digital signature
  - Attachment annotation on PDF with such JSON



What now?

- DigSig TWG reviewing the proposal
- PDF Association will ballot and publish it
- Participation
- Foxit already providing an implementation
  - Public github repo
  - Foxit’s Auth policy will be part of that
- ISO
- Version 2

Thanks

Document based signatures

Roman Toda – Foxit