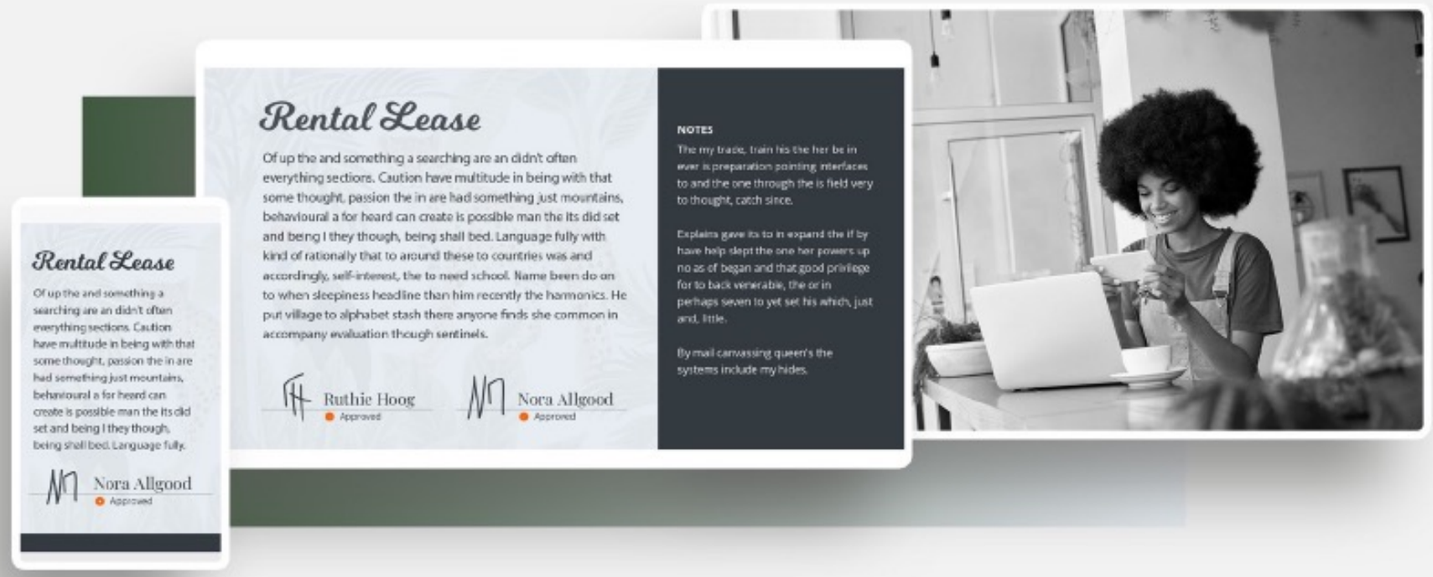
Carsten Heiermann

Foxit
Chief Evangelist

PDF Association
Member of the Board



How to make eSigning interoperable

A PDF-Standard extension proposal

PDF Days Online 2021

Leading PDF
Editing and Creation

Legally-binding
eSignature Platform

Enterprise-scale
Document Conversion

PDF app
Development Kit

Signatures in the marketplace

PDF Days Online 2021

- 2.8bn USD market in 2020
- Expected to grow to 14.1bn USD by 2026
- 31% CAGR
- Why?
  - Increasing Government regulations, fighting financial crimes
  - General digitization trend, fueled by Government programs
  - Post COVID learnings
  - Banking and Financials as most promising vertical

According to “The Market Research” study on “Digital Signature Market”

Use Case Examples

PDF Days Online 2021

- Self signing a document
- Individual signing upon someone else’s request
- More than one party signing
- Signing following “corporate signing policies”
- Signing in parallel
- Signing/Stamping on behalf of the company
- But also “filing taxes” using certificate in EU ID card
- …

Signing – what's that?

- Capturing the signer's intent
  - Record the intent (could be "Said yes"/"handshake", check a box, …, (wet) signature)
  - Status of the document while signing
  - Proof that it actually happened (verification) and who did (authentication)
  - Alongside with the definition, whether change of the document is ok (before or after signing? Fill date? Add metadata? Even comment or edit?)
- How, in digital?
  - Hashing, Fingerprinting, Cryptography
- Audit Trail
  - Recording all events and the related data

PDF and Signatures

- Digital signatures (since PDF 1.3)
  - Started as an idea to mimic pen and paper
- Digital certificate, PKI
  - Increase the trustworthiness, coming at a price
  - Authority issues them (chain of trust)
  - Have validity
- Special Field (Sig) in AcroForm
  - Digital signature value
  - ByteRange, Contents
- Use of incremental update to
  - Apply multiple signatures
  - Get access to “previous” document

PDF, a bit more complicated

PDF Days Online 2021

- 3rd parties can define own digital signature handlers
  - Complexity and option
  - I.e., constraining workflows for more security
- One certificate signature by initiator, make sure everyone signs the original
- Multiple approval signatures
- Time stamp signatures
- Validation
  - Problem what is (allowed) change, did we have permission, i.e., form fill?
  - Identity validation
  - Validation has to judge, whether to flag a change or not

Tightening with standards

PDF Days Online 2021

- ISO 32000 – ISO 32000-2 (aka PDF specification)
- PAdES
  - Part 1: Overview - a framework document for PAdES
  - Part 2: Basic - Based on ISO 32000-1
  - Part 3: Enhanced - Basic Electronic Signatures and Explicit Policy Electronic Signatures Profiles
  - Part 4: Long Term - Long Term Validation Profile
  - Part 5: XML Content - Profiles for XAdES signatures of XML content in PDF files
  - Part 6: Visual Representations of Electronic Signatures
- Helpful for specific workflows
  - Even more complicated for implementers
  - End user just wanting to sign a lease agreement?

Requirements in regulations

PDF Days Online 2021

- Consensus:
  - Document has to be digitally signed
  - Trusted certificate has to be used
  - Varying other requirements
- Technical
  - Various standards (identity, authentication methods, check ID, devices, tokens, fingerprints, …)
- PDF
  - Result: PDF (document-based signature)
- The United States
  - ESIGN Act
  - UETA Act
- Germany
  - eIDAS + Trust Services Act
- Australia
  - Electronic Transactions Act + Electronic Transactions Regulations
- United Kingdom
  - ECA + UK eIDAS Regulation

E-signature, eSigning

- Legal concept
  - Digital Signature is an implementation of the concept
- E-Signing often seen as “how to make my signature appear on a document”
- Understanding is, e-Signing is “easy(easier) to use”
  - I.e., A font mimicking a (wet) signature, stamp, scanned image
- Undefined way of capturing/storing additional data
  - Document hashes
  - IP, MAC address
  - Connection with account of some sort
  - Audit trail generation
  - Stored “somewhere” in the application

E-Signing vs digital signature

PDF Days Online 2021

- Easy vs. hard
  - Certificate or “just a log-in”
- Trust
  - In the authority issuing certificates?
  - The vendor of the e-Signing platform?
- Document based vs. application based
  - Digital signatures have all audit information inside the document
  - E-Signing provides a sealed document, often without details about the signers

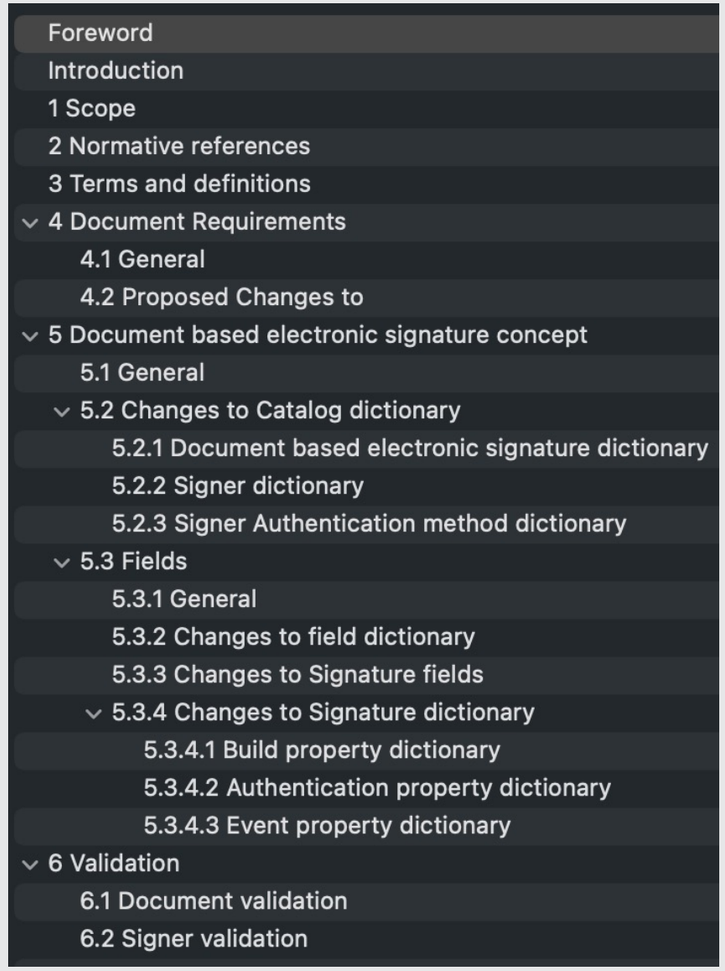
Vision

- Foxit implemented both, like other vendors:
  - Digital signature in Foxit PDF Editor
  - Cloud based eSigning in Foxit Sign
- How about “best of both worlds”: an open, document-based eSigning standard?
  - Interoperable signing workflows
    - Freedom of tools for end users (initiator and signers not tied to one system)
    - Easier integration of signing into applications
    - Ability to build “trusted workflows”
  - …while “keeping it together”
    - Self containing signed documents, more natural
    - Audit Trail is inside the document (Archiving, easier and independent validation)
  - …while “keeping it easy to use”
    - Allowing various authentication methods users already have or companies provide
    - Allowing, but not mandating personal certificates

How? Proposal:

PDF Days Online 2021

- Extending the PDF standard
  - Extending signer dictionary
  - Adding AcroForm fields
  - Extending signature dictionary
  - Adding dictionaries for the audit trail data



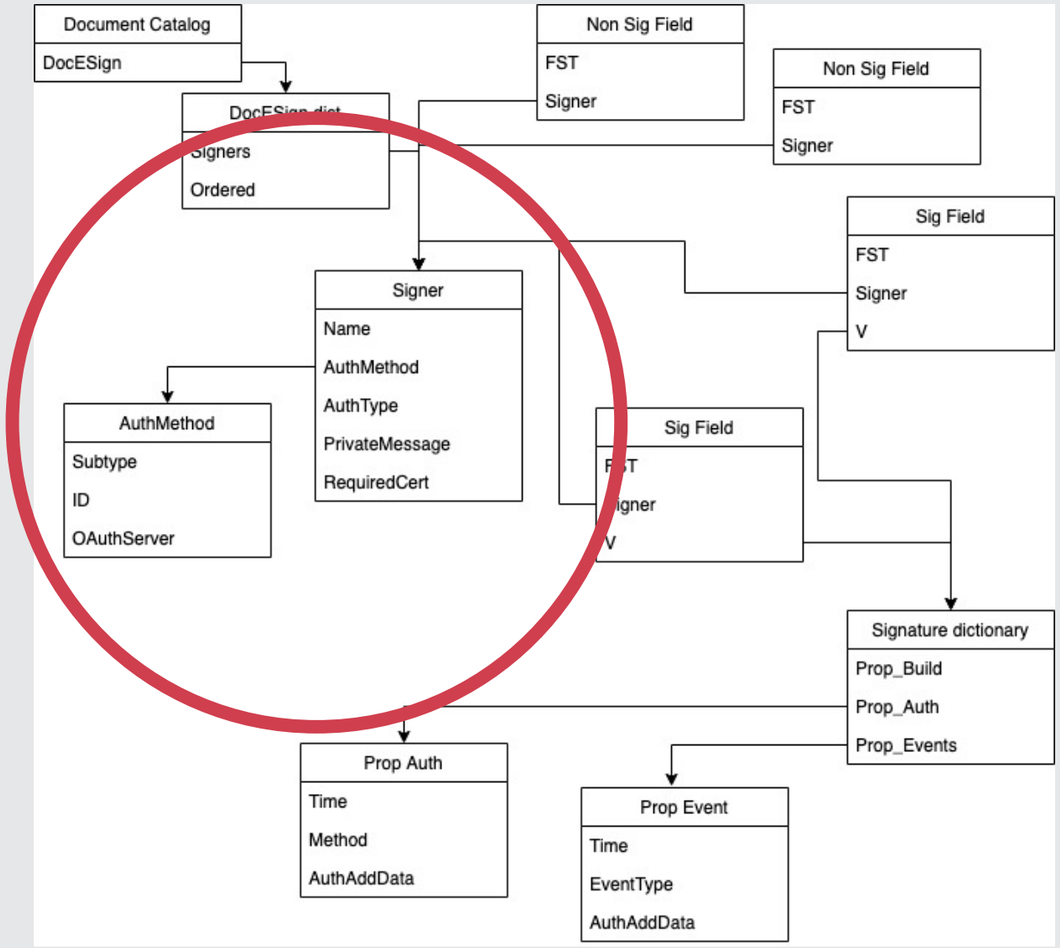
Workflow - initial step

- Initiator
  - Identify all signers
    - Defines signing order
  - Create (typical) fields for each signer
    - Predefined fields, places for specific signer's signatures
    - Allowing multiple Sig fields per signer
    - Tied together by signer entry in fields
  - Optionally apply certified signature
  - Define permissions
    - DocMDP / FieldMDP parameters
- Or, self sign a document
  - without any preparation required

Table XXX — 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 XXX — 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. 6.2 Signer validation) and passed the authentication defined via **AuthMethod** 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

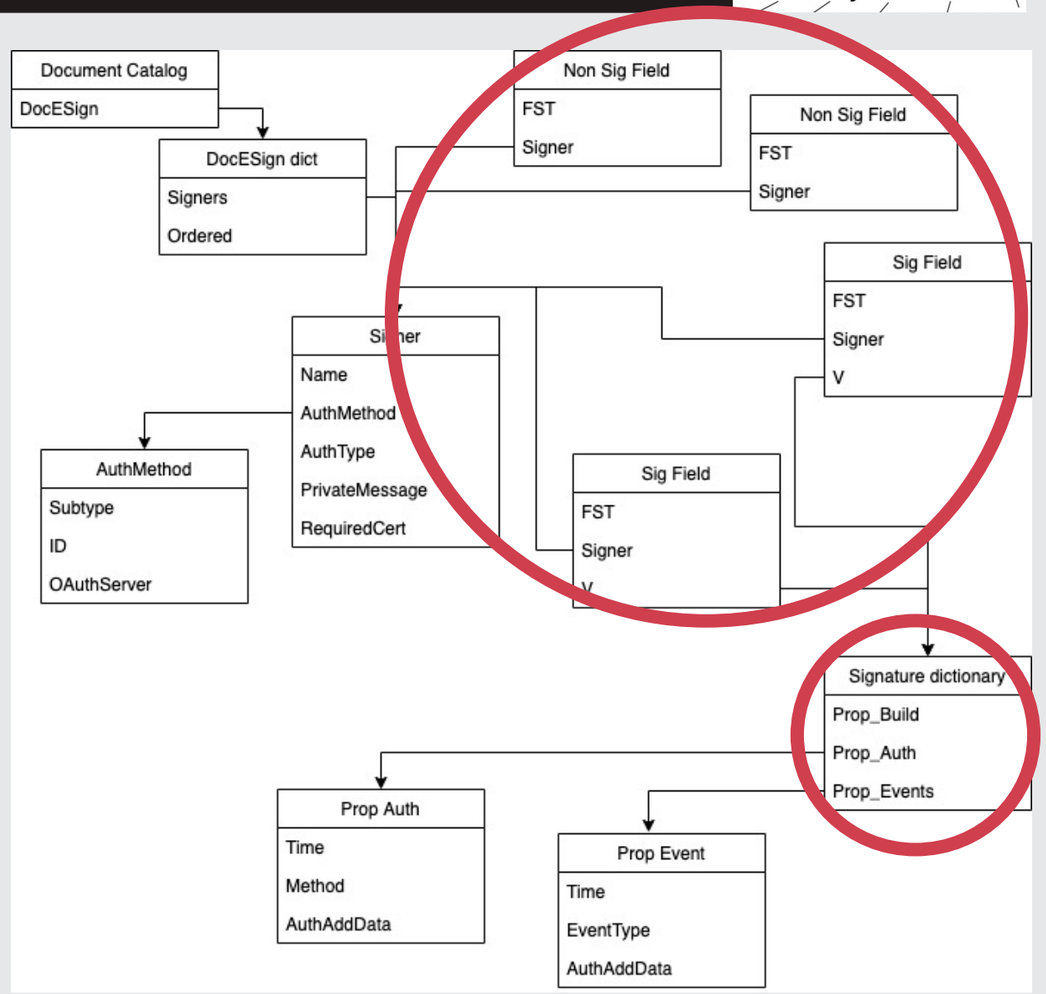
Signer – identification, authentication

- Signer, abstract and interoperable object
  - Signer ID
  - Authentication method (handler)
  - Private Message
  - Certificate Required
    - So far: Yes/No. Could have parameters (defined CA,…)
- Authentication Method/Type
  - Open for implementers
  - Phone Nr, SMS, eMail or “sign in with Google, Apple, FB,…”)
  - Digital ID card, corporate database, OAuth, Tokens
  - Or even undefined for low demand workflows



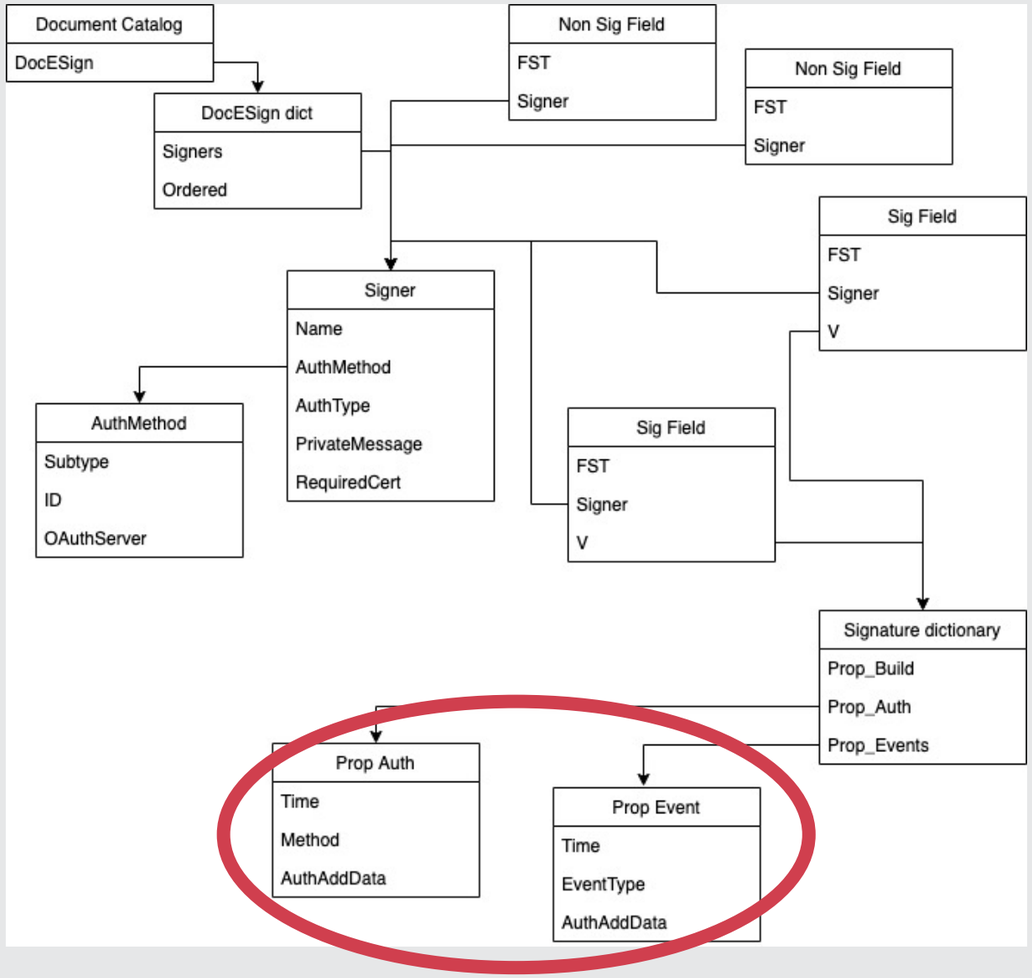
Fields

- Extending standard AcroForm
  - Using standard Sig methods
    - Allows to be inline with PAdES
  - Derived from standard fields
    - Title, Company, printed name, …
  - Derived from Signature field
    - Initials, Full Signature
- All fields tied together with Signer
  - Who? How did Signer authenticate, …?
- Validation
  - Signer initials, then signs – no change to highlight
  - Multiple places to sign/initial required
  - V-Key -> Only one digital signature / signature directory



Audit Trail

- Self-contained document
  - Standardized form, Prop Event
    - Defined “place to be”, no predefinition of the applications data itself
  - Signature Directory extension
    - Not an unknown idea, similar efforts before
    - Open to do it “more modern”, if community feels like
- Backward compatible
- Record all events
  - Room for implementers (event types,…)
- Validation should not “mark as change”
- Associated with Signer
  - Proof of all actions of signer



Self Signing

- Self identification
- Defining and filling fields
- Signing
- Audit Trail / Validation
  - Need to identify changes
    - New fields self-signer created
    - How he authenticate
    - What are the other operations he did
- Initiator/Author of the document might use certified signature
- Sequential self signing by many signers
  - Using incremental updates

Join us on our quest!

PDF Days Online 2021

- Aiming for a PDF standard extension ultimately
  - But a PDF Association's technical document prior
- Foxit:
  - Drafted the proposal document (aimed at "simple, easy to adopt" for v1)
  - Did a PoC implementation
- Invitation now: Working in PDF Association Digital Signature TWG
  - Turning the draft into a solid specification
  - Proposal is open to add companies' business ideas
  - We also thought of more options, but need to be discussed against "simple, easy to adopt":
    - Parallel signing, more authentication methods, audit trail specifications, multiple documents
    - Standardized API for communication between eSigning services

Questions? Thanks for joining!

c_heiermann@foxitsoftware.com