



# Implementing FAA Form 8130-3 electronically

## Replacing Paper-Based Forms with eForms

### Stan Engdahl

BEDS Product Manager &  
Loadable Software Manufacturing and Process Engineering,  
Loadable Software - Software Control Library Parts Plant,  
Boeing Commercial Airplane

- As part of the deployment of Boeing's 787, e8130-3s will replace existing paper based FAA Form 8130-3, in support of electronic software distribution. These forms are based on FAA Order 8130-21G, the ATA Spec 2000 Chapter 16 XML standard format, and leverage the ATA Spec 42 PKI standard.

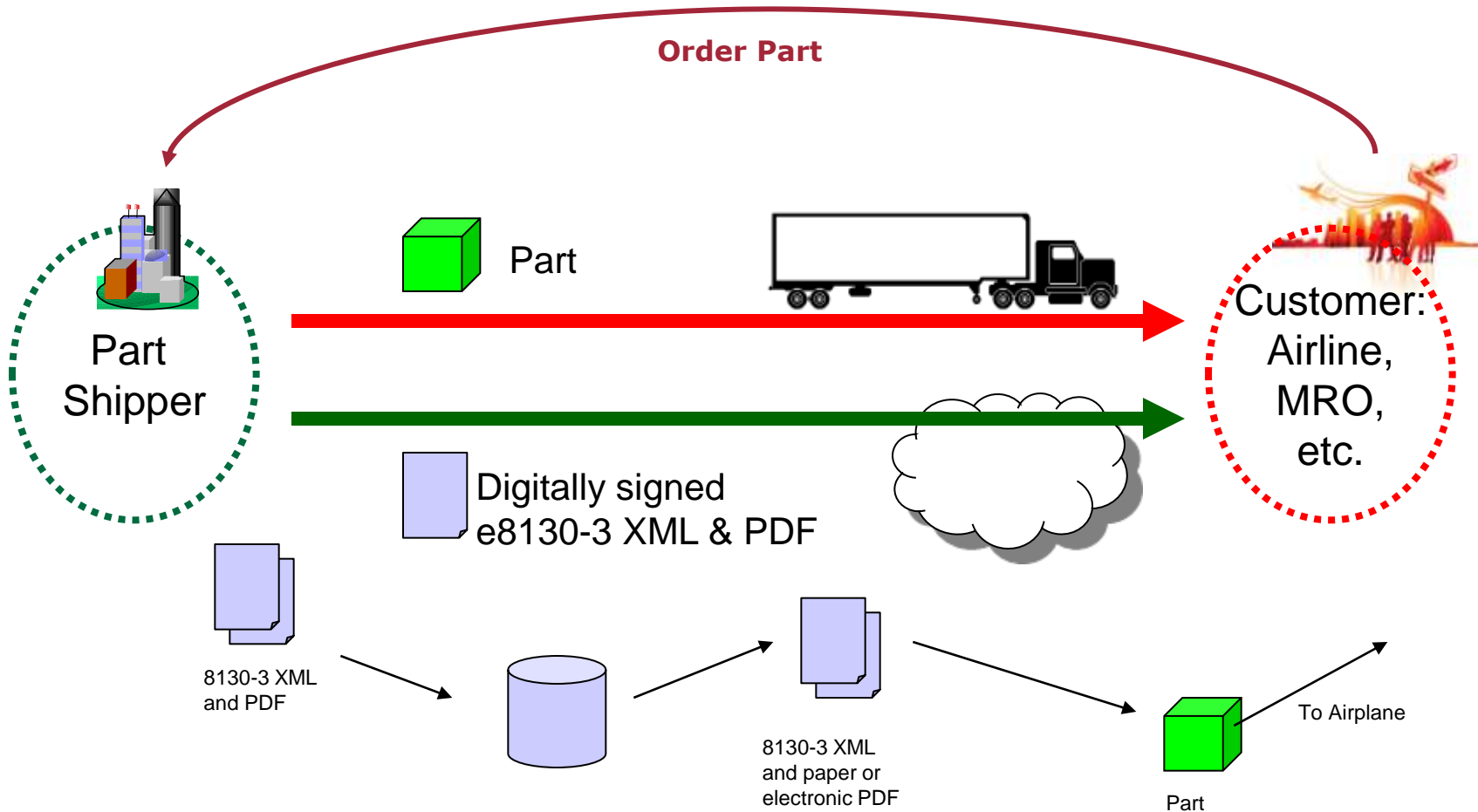
# Benefit for using e8130-3

Per FAA Order 8130-21G,

- The use and acceptance of electronic FAA eForm 8130-3 offers several distinct advantages over the current paper format:
  - Through the use of standard data semantics and structures contained in ATA Spec 2000, chapter 16, a higher degree of data reliability and consistency will be achieved.
  - Through adoption of common, widely available digital security technologies, it is considerably more difficult to forge or alter data without being detected, and the data can more easily be traced directly to the source.
  - Identifying a document signer (signatory) will be easier through the elimination of traceability difficulties associated with illegible handwritten entries and the deterioration of paper documents.
  - The frequency of lost, damaged, and unreadable documents can be significantly reduced.
  - The automated processes for generating, transmitting, and processing data will significantly reduce costly human errors.
  - The cost and difficulty to store, retrieve, and analyze information can be substantially reduced.

# Process Flow Cartoon

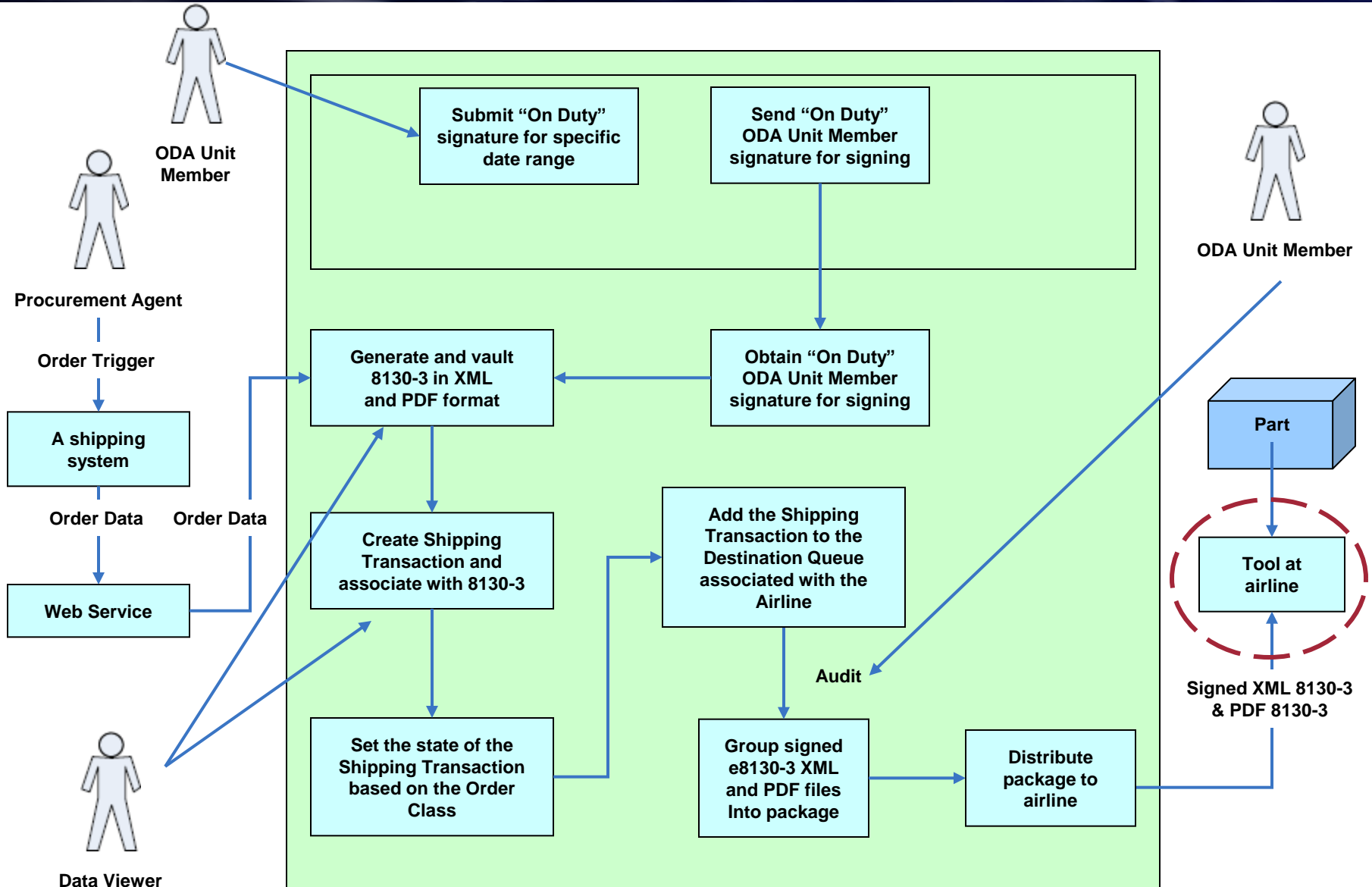
## Shipping a Part



# Things to consider

- Can the receiving party “read” and authenticate the e-8130-3, tool or application, agreed to implementation of “standard”?
- What are the agreed to certificate authorities that will be used in trusting the Digital signatures?
- What have both parties agree will constitute a authentic e8130 Digital Signature?
- What Crypto libraries are to be used?
- What Crypto Algorithms are to be used?
- How long will the e8130 need to be kept in a form that can be authenticated?

# A high level Architecture Cartoon



# Was there a Signing ceremony? Who signs a e8130-3?

- The Digital Signature signing ceremony is very important, it gives context and legality to document to which it is applied.
- To make a Digital Signature carry the same standing as a INK signature the digital signature must be applied in a similar manor or ceremony as a INK signature.
- The person signing must be presented with the document to be signed and a attestation as to what the Digital Signature will represent must be presented to the person signing.
- This typically takes the form
  - Document
  - Attestation ( I Hereby attest that this document is complete and....)
  - Digital signature application



# The Digital Signatures, Uses

Authentication

Is the e8130-3 authentic, at receipt and in the future

- Digital Signature

Integrity

Is the e8130-3 integral

- Digital Signature

Nonrepudiation

Can the signing person, or company deny that they signed the e8130-3

- Digital Signature

Authorization

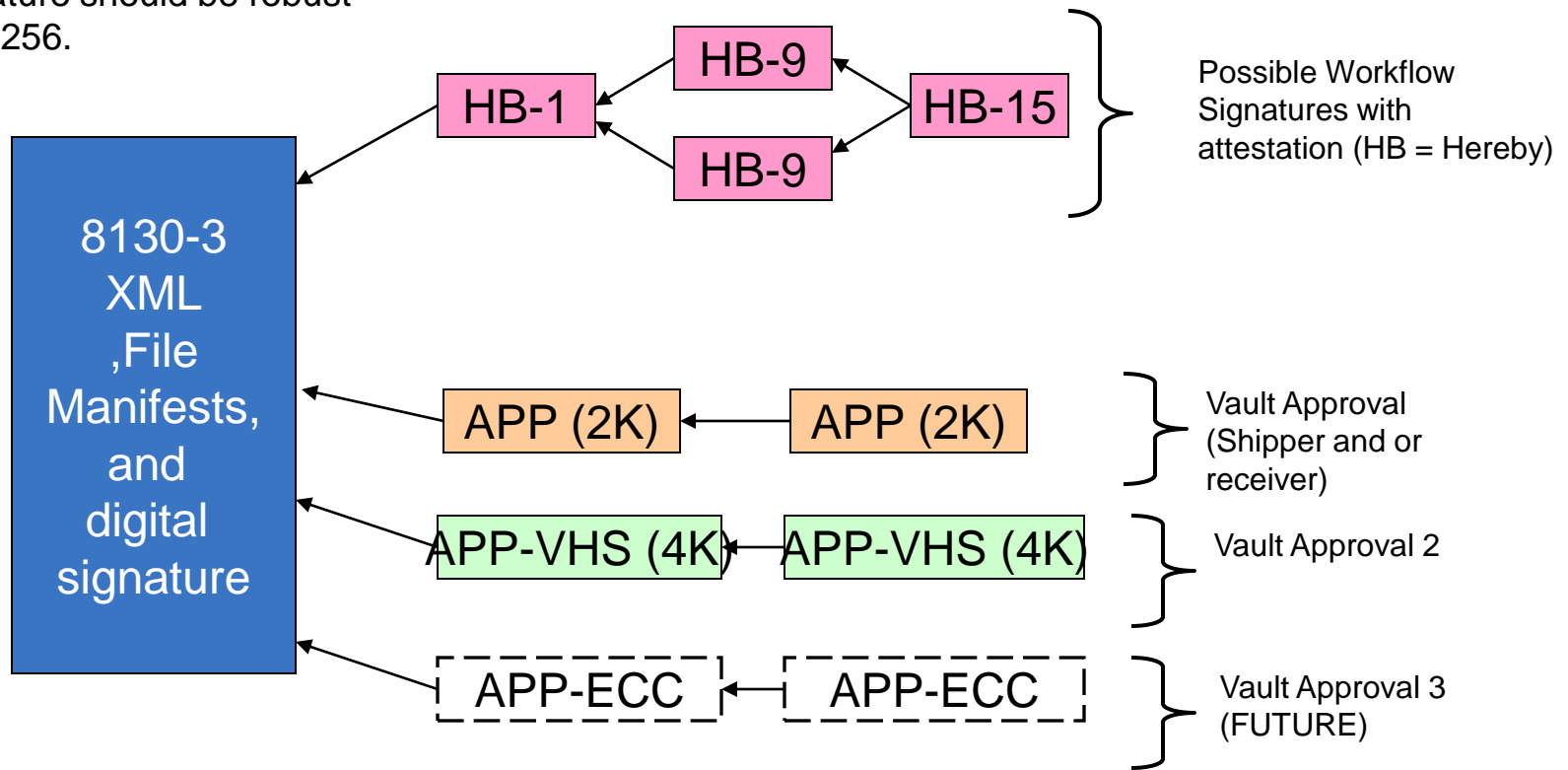
Used for access control typically, may be useful in the implementation of a tool

Confidentiality

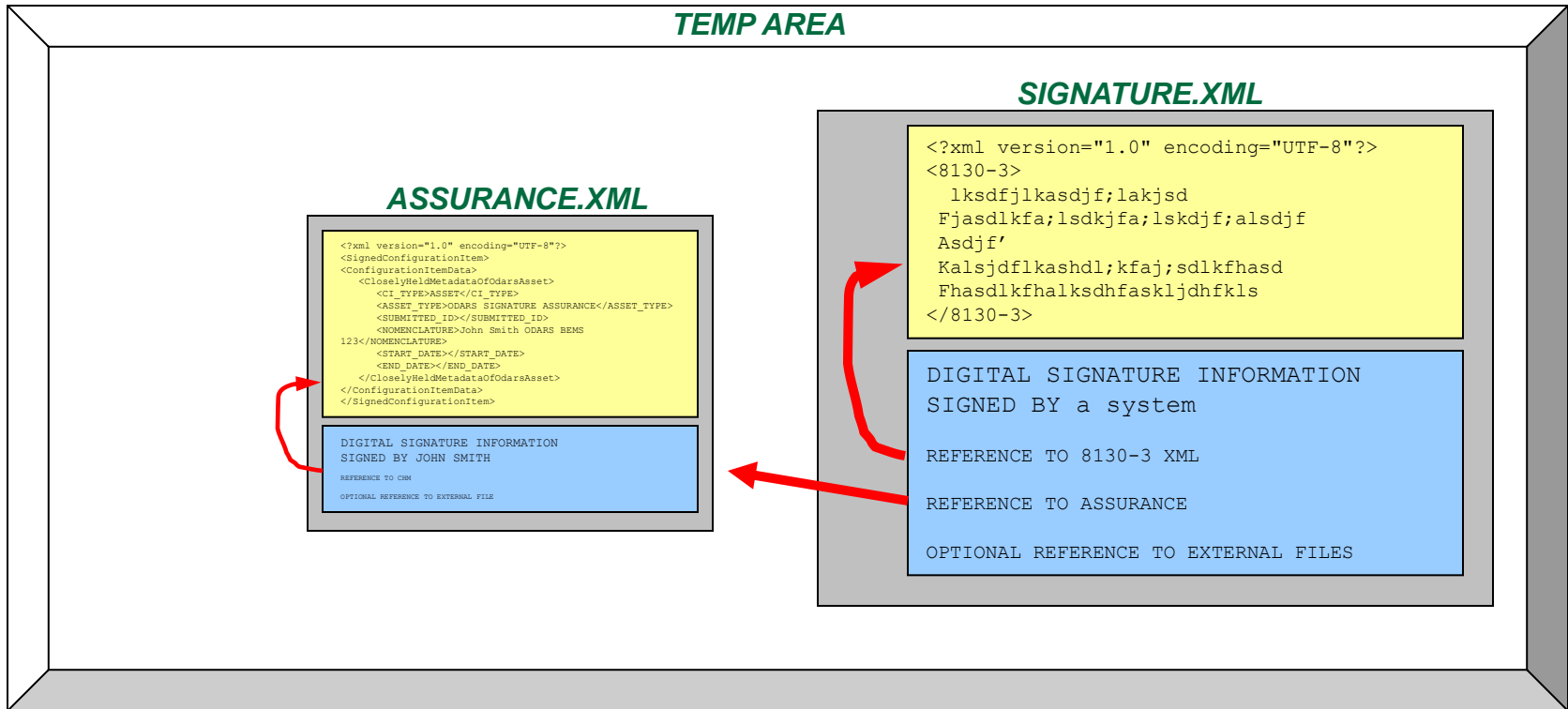
Protection of Intellectual Property

# Different signature states, considerations for World Wide Web Consortium (W3C) Digital Signatures

Note: All digests for manifest and signature should be robust like SHA-256.



# The 8130-3 and the ODA Signature Assurance are bound together



When generating an e8130-3, generate the e8130-3 XML then sign the e8130-3 XML plus countersigns the ODA assurance document.

The resulting XML file has the 8130-3 and the assurance files tightly bound by the encompassing digital signature.

# What is agreed to be an authentic signature?

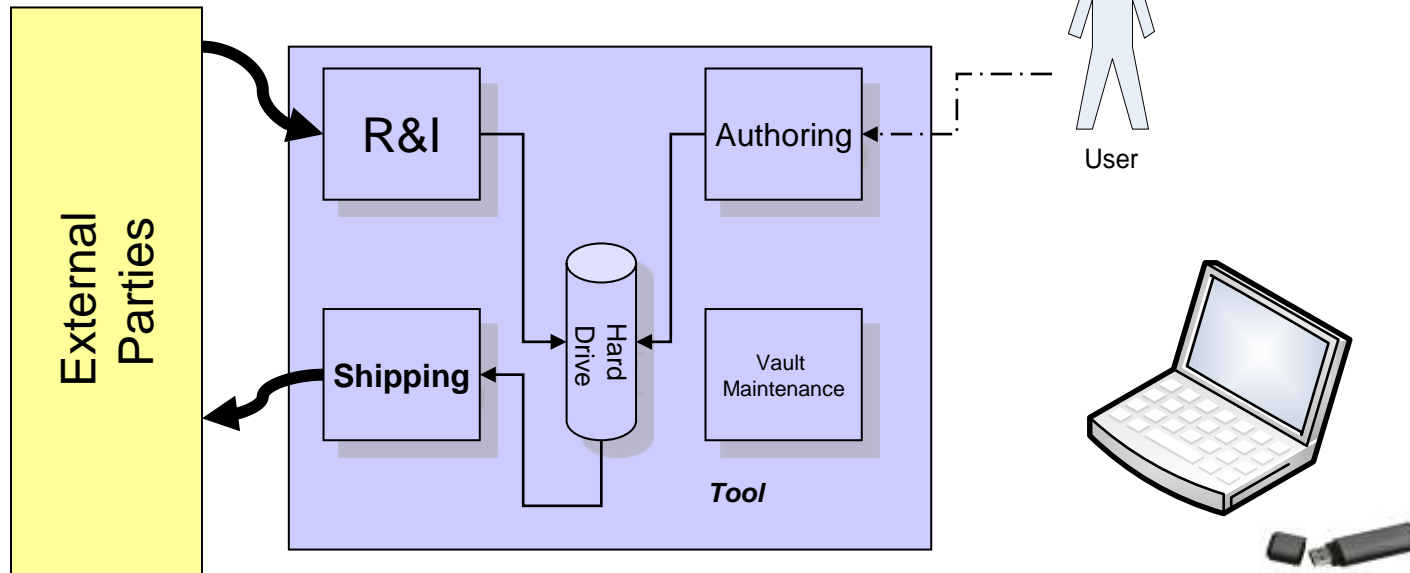
Not all aspects of the e8130-3 Digital signature need to “validate” to trust the Digital signature for a given time and or Place.

- The Public Key can “open” the digital signature.
- The computed Digest matches the Digital Signatures digest .
- There is a trusted Certificate “cached” or accessible “on-line” that matches the one use to sign.
- The Certificate is not expired
- Digital signatures for some signature state may have “issues” but at least one is completely valid and trusted
- The certificate is not on the Certificate Revocation List (CRL)
- The OID of the Certificate is correct for its use
- Your organization has chosen to Trust the Certificate issued by the Certificate Authority used for the Digital signature.

# A tool that implements the standards and other agreed to considerations

## Some functional components

@ using parties site



- All configurations can be hosted general computing device
- Use of USB HW keystore / credentials.

# XML 8130-3 files are in a sister folder

- Create and Distribute

This slide shows the content of the folder that contains the XML version of the 8130-3.

Name	Size	Type	Date Modified
assurance.xml	11 KB	XML Document	10/11/20
faa81303PdfSignatureXml.xml	6 KB	XML Document	10/11/20
signature.xml	8 KB	XML Document	10/11/20

The XML version of the 8130-3 can be viewed by opening signature.xml in a browser or an XML editor like MS Word or Altova XMLSpy.

The next slide shows a signature.xml opened in Altova XMLSpy.

# Open the XML 8130-3 with an XML editor/viewer

- Create and Distribute

```
1 <CurrentCertificate>
2   <ATA_PartCertificationForm id="ID-38461-582249" version="1.0">
3     <Block2>
4       <CET FVI="6-01">FAA Form 8130-3</CET>
5     </Block2>
6     <Block3>
7       <TDN>582249</TDN>
8     </Block3>
9     <Block4>
10      <IssuerDetail>
11        <SPL>81205</SPL>
12        <WHO>Boeing Company - Boeing Commercial Airplane Group</WHO>
13        <ADL>7755 East Marginal Way South</ADL>
14        <CIY>Seattle</CIY>
15        <ZIP>98124</ZIP>
16        <CNT>US</CNT>
17        <STP>WA</STP>
18        <PCH>PC 700</PCH>
19      </IssuerDetail>
20    </Block4>
21    <Block5>
```

signature.xml

# e8130-3 packages are unpacked to local file system

- Create and Distribute

The XML and PDF versions of an 8130-3 are unpacked into separate folders nested within a shared parent folder.

The folder that contains the PDF version is shown here.

Below we show the content of the folder that contains the XML version of the 8130-3.

Name	Size	Type	Date Modified
Form_8130_3_38461-582249.pdf	25 KB	Adobe Acrobat...	9/28/2010 5:22 PM
signature.xml	6 KB	XML Document	10/11/2010 4:57 PM

The PDF 8130-3 can be viewed by opening this file with a PDF viewer like Adobe Reader.

A double-click on the file name opens the window shown on the next slide.

# Rendering on the Fly or pre-Render into a PDF

- The FOP (Formatted Object Processor) Transform is invoked:
  - It takes in 8130-3 Xml doc and file location for PDF
  - and locates FAA81303 XSL to use as an input stream
  - then invokes the FOP library API for XSLT transformation



Similar approach could be used to render “On the Fly” to HTML, or other display or print format.

# Open the PDF 8130-3 with a PDF Viewer

- Create and Distribute

Form\_8130\_3\_38461-582249.pdf - Adobe Reader

File Edit View Document Tools Window Help

1 (1 of 1) 48.9% Find

1. Approving National Aviation Authority/ Country  
FAA/United States

2. **AUTHORIZED RELEASE CERTIFICATE**  
FAA Form 8130-3, AIRWORTHINESS APPROVAL TAG

3. Form Tasking Number  
102048

4. Organization Name and Address  
Boeing Company - Boeing Commercial Airplane Group, 7705 East Marginal Way South, Seattle, WA 98134, US  
Supplier Code: 81205  
Certificate Number: PC 730

5. Work Order/Contract/Invoice Number  
Customer Order No: 102048  
Customer ID Code: DLA

6. Item:	7. Description:	8. Part Number:	9. Eligibility:	10. Quantity:	11. Serial/Part Number:	12. Status/Work
1	PUSH REPORT BY WORK LOCATION - AIRPLANE MODEL: 787-9	529C33C-4-0277-6234 -020-47418E25152-44	EA	1	EA	NEW

13. Remarks  
Manufacturer Code: 81205  
AIRWORTHINESS APPROVAL - PARTS. THIS FORM IS NOT AN EXPORT APPROVAL. (THIS 8130-3 IS USED FOR TESTING PURPOSES ONLY.)

14. Certifies the items identified above were manufactured in conformity to:  
 Approved design data and are in a condition for safe operation.  
 Non-approved design data specified in Block 13.

15. [ ] 14 CFR 43.9 Return to Service [ ] Other registration specified in Block 13  
Certifies that unless otherwise specified in Block 13, the work identified in Block 12 and described in Block 13 was accomplished in accordance with Title 14, Code of Federal Regulations, part 43 and in regard to that work, the items are approved for return to service.

15. Authorized Signature:	16. Approval/Multisignature No.:	20. Authorized Signature:	21. Approval/Certificate No.:
Digital signature on file	00A-102048-104		

17. Name (Typed or Printed):	18. Date (Printed):	22. Name (Typed or Printed):	23. Date (Printed):
Moby, Nrupal D	Sep 27 2010		

**User/Installer Responsibilities**

It is important to understand that the existence of this document alone does not automatically constitute authority to install the part/component/assembly.

Where the user/installer performs work in accordance with the national regulations of an airworthiness authority different than the airworthiness authority of the country specified in Block 1, it is essential that the user/installer ensures that higher airworthiness authority accepts part/component/assembly from the airworthiness authority of the country specified in Block 1.

Statements in Blocks 14 and 15 do not constitute installation certification. In all cases, aircraft maintenance records must contain an installation certification issued in accordance with the national regulations by the user/installer before the aircraft may be flown.

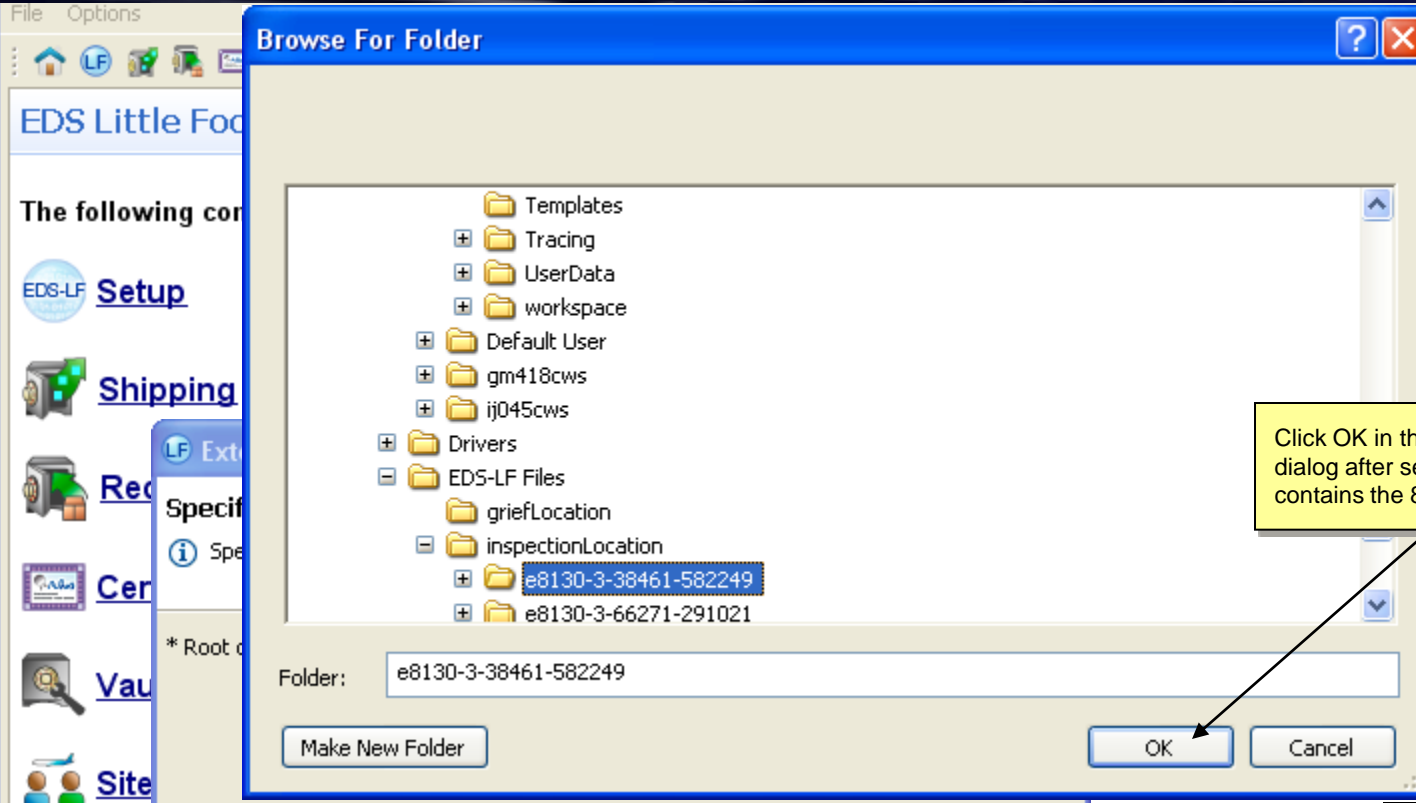
FAA Form 8130-3 (9-07) \*Installer must cross-check eligibility with applicable technical data. ISBN: 000-00-010-0000

**Paperwork Reduction Act Statement:**  
An Agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number associated with this collection of information is 2120-0076. Comments concerning the accuracy of this burden and suggestions for reducing the burden should be directed to the FAA at 800 Independence Ave. SW, Washington, DC 20591. AEO: Information Collection Clearance CP-Rule: AEA-20.

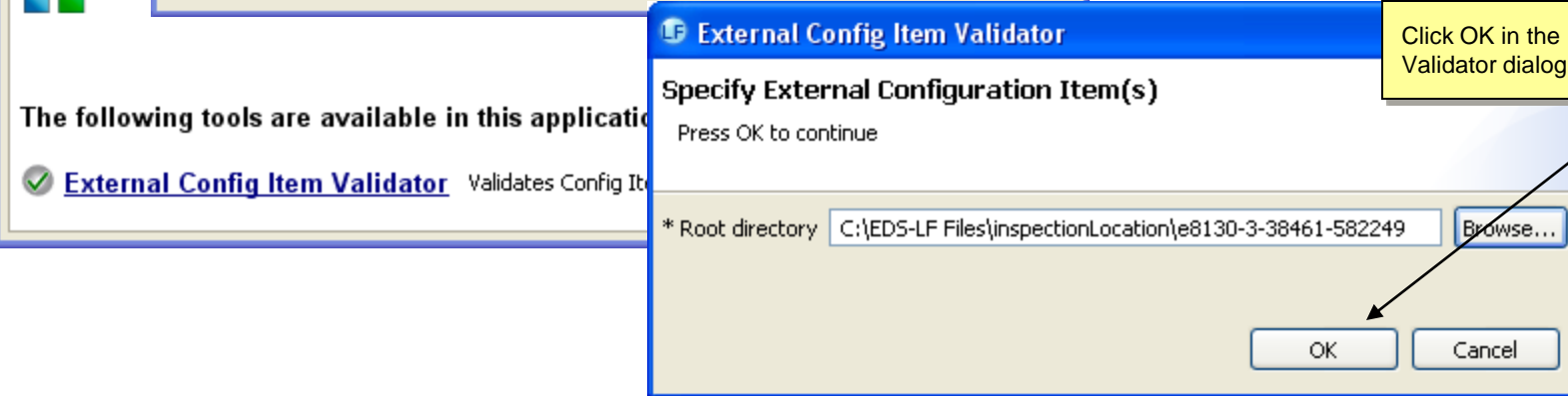
# What is required to continue to be able to Authenticate a signed Item into the future?

- Signing of the Item with the Airline Private Key and retaining the item in a electronic store/vault.
  - Provides ability to check Authenticity and Integrity of stored item in future.
- Resign the item again with the Airlines “NEW” Private Key before the “OLD” Airline private key expires.
  - Specifically obtain a “NEW” Certificate and generate new Airline Private keys for resigning of items before “OLD” Certificate expires.
  - Keeps a current signature on the items providing the ability to check authenticity and integrity.

# Validate an e8130-3



Click OK in the Browse For Folder dialog after selecting the folder that contains the 8130-3 of interest



Click OK in the External Config Item Validator dialog to validate the 8130-3s

# Using a tool to validate 8130-3s - PDF

- Create and Distribute

The screenshot shows the 'External Config Item Validator' application window. On the left, a file list contains 'FORM\_8130\_3\_PDF' and 'FORM\_8130\_3\_XML'. The main area displays 'CHM Signature Validation' results for two items:

- HB-24** (Signed at Thursday, December 17, 2009 7:25:24 AM PST per Time reference not supplied by seantp.services.boeing.com) This certifies that this document has been generated and signed by an authorized EDS repository and is compliant with current EDS processes, further all subordinate human initiated digital signatures associated with the workflow leading to its approval are attached or on file.
  - Signed: Test BEDS Approval Certificate applications, Boeing US
  - Expiration: 30 June 2011 18:00:05
  - Validity: Signature is valid
  - Trust: Considered trusted without CRL check
  - Revocation: Confirmed not revoked
- APP (Approved for Distribution)** (Signed at Thursday, December 17, 2009 7:25:24 AM PST per Time reference not supplied by seantp.services.boeing.com)
  - Signed: Test BEDS Approval Certificate applications, Boeing US
  - Expiration: 30 June 2011 18:00:05
  - Validity: Signature is valid
  - Trust: Considered trusted without CRL check
  - Revocation: Confirmed not revoked

At the bottom of the window, there are two buttons: 'Save report for selected Config Item...' and 'Save reports for all Config Items...'.

# Use a tool validate 8130-3s - XML

- Create and Distribute

The screenshot shows the 'External Config Item Validator' application window. On the left, a file list contains 'FORM\_8130\_3\_PDF' and 'FORM\_8130\_3\_XML'. The main area displays the 'FAA 8130-3 Validation' results for two items:

- HB-24** (Signed):
  - (Signed at Thursday, December 17, 2009 7:25:32 AM PST per Time reference not supplied by seantp.services.boeing.com) This certifies that this document has been generated and signed by an authorized EDS repository and is compliant with current EDS processes, further all subordinate human initiated digital signatures associated with the workflow leading to its approval are attached or on file.
  - Signed: Test BEDS Approval Certificate applications, Boeing US
  - Expiration: 30 June 2011 18:00:05
  - Validity: Signature is valid
  - Trust: Considered trusted without CRL check
  - Revocation: Confirmed not revoked
- APP (Approved for Distribution)** (Signed):
  - (Signed at Thursday, December 17, 2009 7:25:32 AM PST per Time reference not supplied by seantp.services.boeing.com)
  - Signed: Test BEDS Approval Certificate applications, Boeing US
  - Expiration: 30 June 2011 18:00:05
  - Validity: Signature is valid
  - Trust: Considered trusted without CRL check
  - Revocation: Confirmed not revoked

At the bottom of the window, there are two buttons: 'Save report for selected Config Item...' and 'Save reports for all Config Items...'.

# *Cryptographic Strength & Cryptographic Algorithms*



# NIST Guidelines (dated chart)

CRYPTOGRAPHIC STRENGTH	KEY SIZE RATIO	HASH ALGORITHM	ELLIPTIC CURVE ASYMMETRIC ALGORITHMS	RSA/DSA/DH ASYMMETRIC ALGORITHMS	EXPECTED LIFETIME EXPIRY
56 bits	DES	-	-	-	expired
80 bits	3DES (2 key)	SHA-1	160 bits	1024 bits	2010
112 bits	3DES (3 key)	SHA-224	224 bits	2048 bits	2030
128 bits *	AES-128	SHA-256	256 bits	3072 bits	2031+
192 bits	AES-192	SHA-384	384 bits	7680 bits	2031+
256 bits *	AES-256	SHA-512	512 bits	15360 bits	2031+

guidelines for public key sizes for AES – supplied by NIST

\* 128 bit is commercial strength and 256 bit is for classified information

- Desired cryptographic strength in bits times...
  - 1 = symmetric key length in bits
  - 2 = message digest length in bits
  - 2 = elliptic curve key length in bits
  - 6 - 60 = RSA or DSA key length in bits (growing multiplier)

# Strength Consideration (dated chart)

- Protection period
- Downside risk
- Processing performance
  
- Also see ATA Spec 42



Protection Period Until, Years	Symmetric Encryption	Message Digest	Elliptic Curve	non-ECC (RSA, DSA)
2008, 0 - 3	128	160	256	2048
2015, 3 - 10	128	256	256	4096
2035, 10 - 30	256	512	512	8192
2075, 30 - 70	256	512	512	15360

# Available Algorithms

- Lots to choose from...

- GOST-Hash
- MD5
- Panama
- RIPEMD-160
- SHA-1
- SHA-256, 384, 512
- Snefru-2
- Tiger
- Whirlpool
- 3-Way
- AES
- Blowfish
- Camellia
- CAST
- DEAL
- DES
- DESede
- DESX
- GOST
- ICE
- IDEA
- LOKI97
- MARS
- Panama
- RC4
- RC5
- RC6
- Rijndael
- SAFER
- Sapphire-II
- SEAL
- Serpent
- SHACAL
- SKIPJACK
- SPEED
- Square
- TEA
- Twofish
- WAKE
- ElGamal
- RSA
- DSA/SHA-1
- DSA/EMSA1
- CDSA/EMSA1
- ECNR/EMSA1
- ESIGN
- NR/EMSA1
- NR/PSS-MGF1
- RSA/PKCS1-1.5

...and others. Some are NIST approved, some ISO, some under evaluation, licenses may be required.

# Algorithms Considerations

Algorithm Type	Primary	Secondary
Message Digest	SHA-1	RIPEMD-160
	SHA-256	Whirlpool
	SHA-512	Whirlpool
Elliptic Curve Signing	ECDSA/SHA-1	ECNR/SHA-1
	ECDSA-256/SHA-256	ECNR-256/Whirlpool
	ECDSA-512/SHA-512	ECNR-512/Whirlpool
non-ECC Signing	DSA/SHA-1	RSA/SHA-1
Elliptic Curve Cipher	ECC-256	--
	ECC-512	--
non-ECC Cipher	RSA	EIGamal

***Agreement is need with trading parties as to what algorithms and libraries that implement them are going to be used.***

# How long will the e8130 need to be kept in a form that can be authenticated?

- In your organization
  - Will the e8130-3 (the digitally signed xml) only be used to receive a part to the store and then archived.
  - Or will the e8130-3 need to be retrieved as authentic at other locations, at later dates.
  - How long will the e8130-3 need to be retrieved and what has your certification authority deemed a valid method for production at a later date of a authentic e8130-3?

# Questions

- Thank you