

## AEROSPACE KNOW-HOW

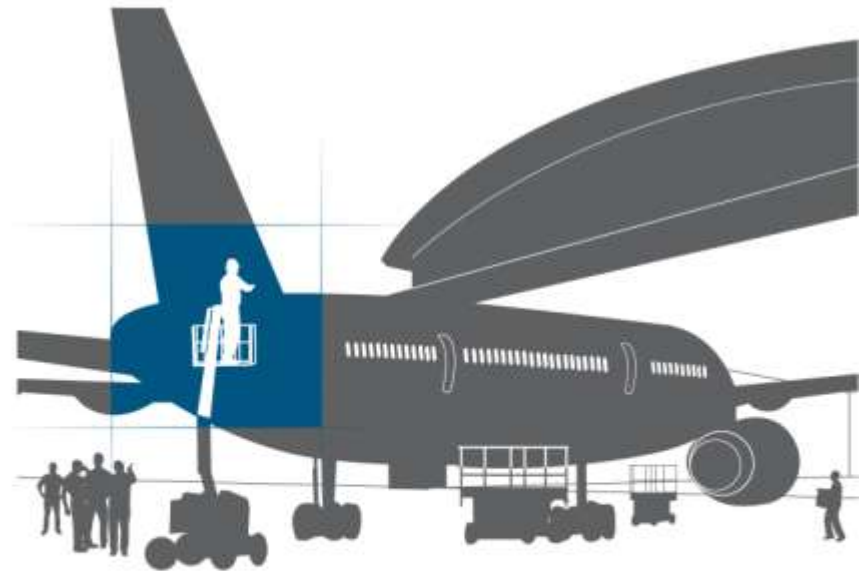
# Electronic Authorized Release Certificates

*Where are we on the journey from the industry standard to day to day reality ?*

Mansour Rezaei Mazinani, Lead Architect

ATA e-Business Forum

Montreal, 8 June 2011



# Today's reality and the industry vision

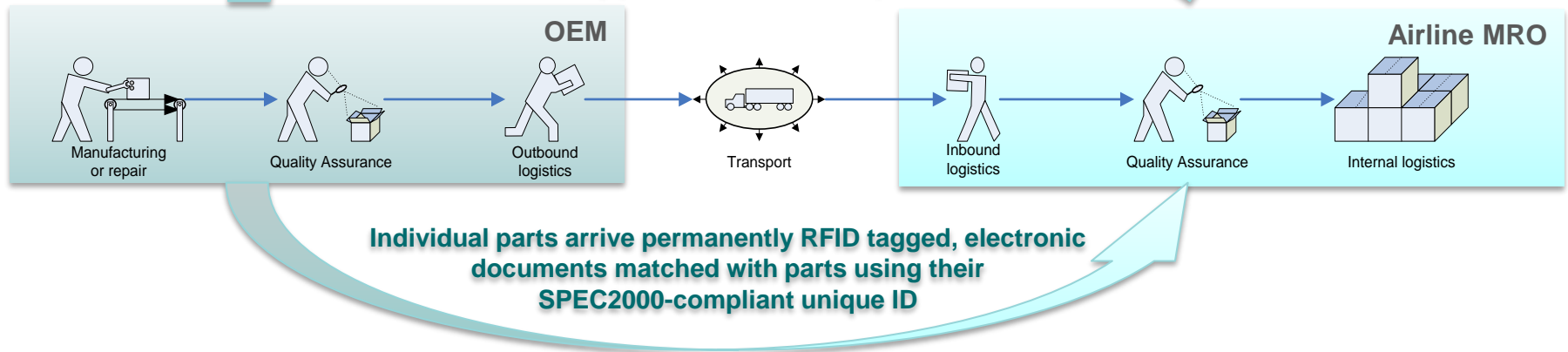
58%

... of the time it takes to move a part "from the dock to the bin" is spent on administrative (read 'paperwork') activities that could be automated.

More than  
10

different paper documents and tags are involved in the part's journey. These could all be electronic and automatically linked to automatically identified parts *8130, Certificate of Conformance, Teardown report, Shipping advice, Invoice, Asset tracking tag, Box tag, Routing document, ....*

**SPEC2000-compliant electronic documents delivered reliably prior to the arrival of parts**



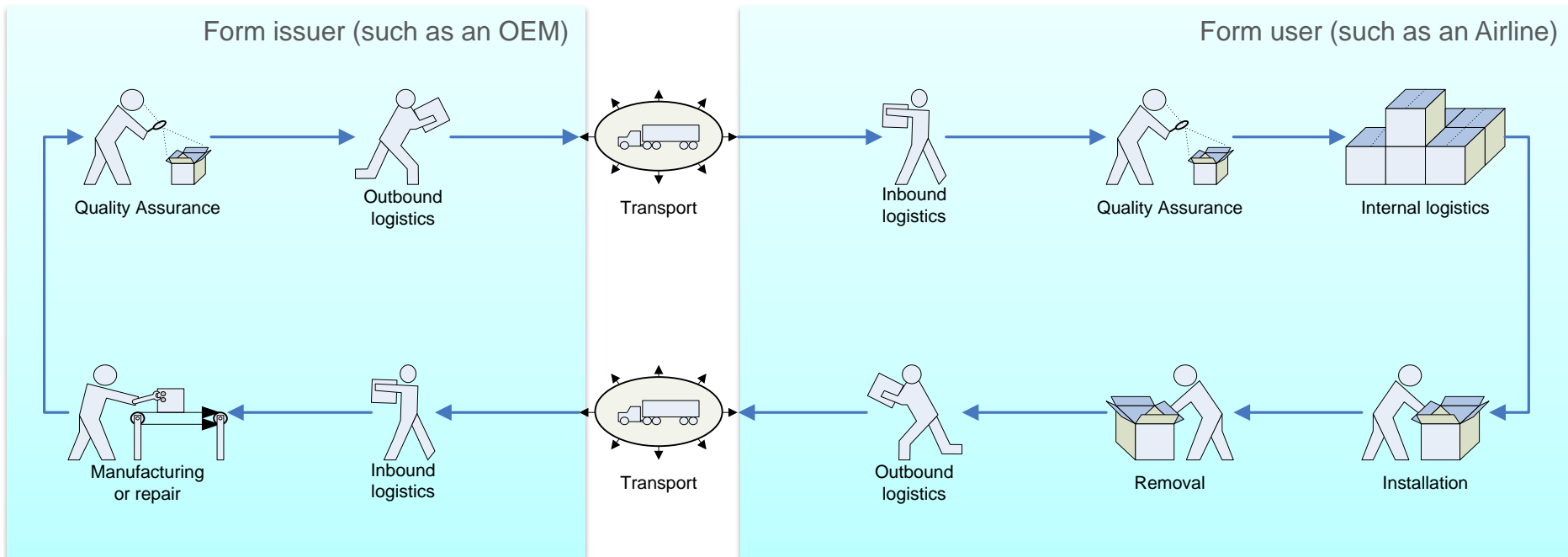
**Individual parts arrive permanently RFID tagged, electronic documents matched with parts using their SPEC2000-compliant unique ID**

15-20  
minutes

... of an inspector's time on average saved per receiving of a single rotatable part. This is an administrative activity which does not add any business value. Time savings can be used to carry out more inspections (and reduce bottlenecks at Incoming Inspection)

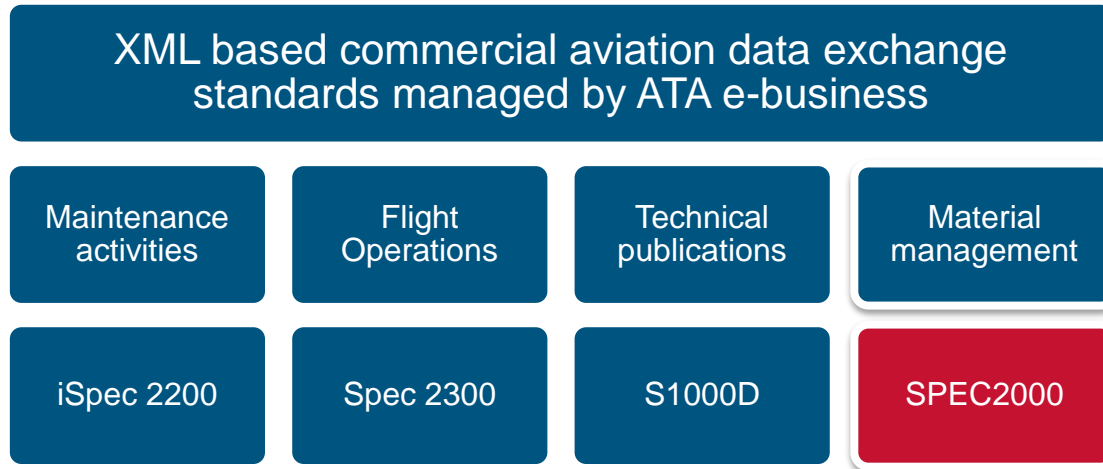
*Estimates based on process analysis conducted by SITA and Continental Airlines,. Results are smoothed to represent generic airline situation.*

# Our understanding of the overall requirement



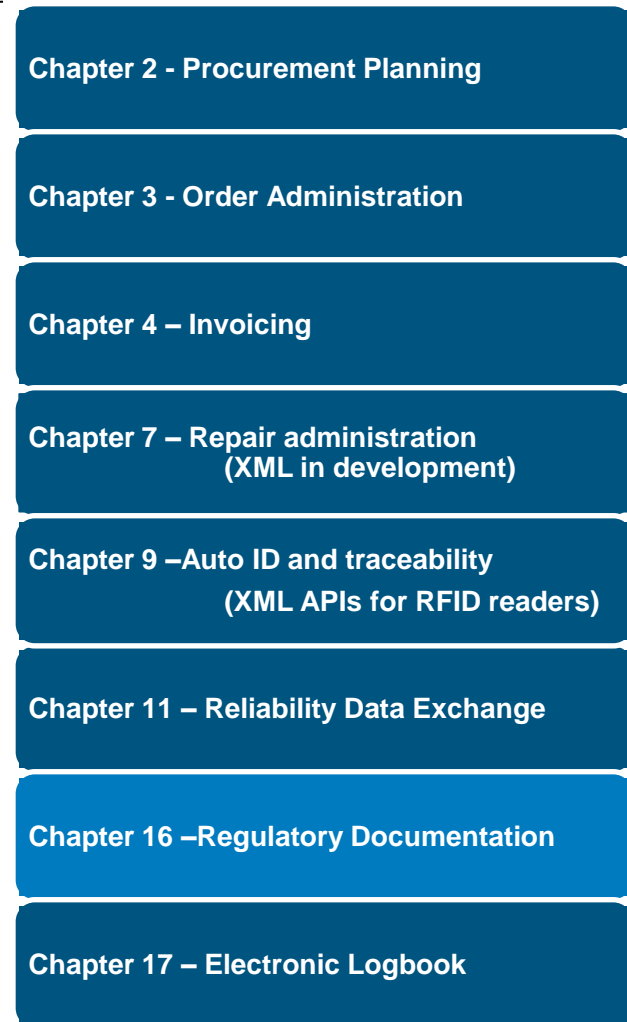
Complete traceability of an aircraft part throughout its lifecycle, completely paperless, secure and available in real time while respecting data confidentiality

# SPEC2000 : Material Management Standard for Commercial Aircraft Maintenance



- Originated as a standard for EDI and file exchange (i.e. provisioning files for placing aircraft orders)
- EDI and file transfer standards are no longer updated, all new developments are in XML
- **Digital security practice is defined in SPEC42**

## SPEC2000 Chapters with defined XML schemas

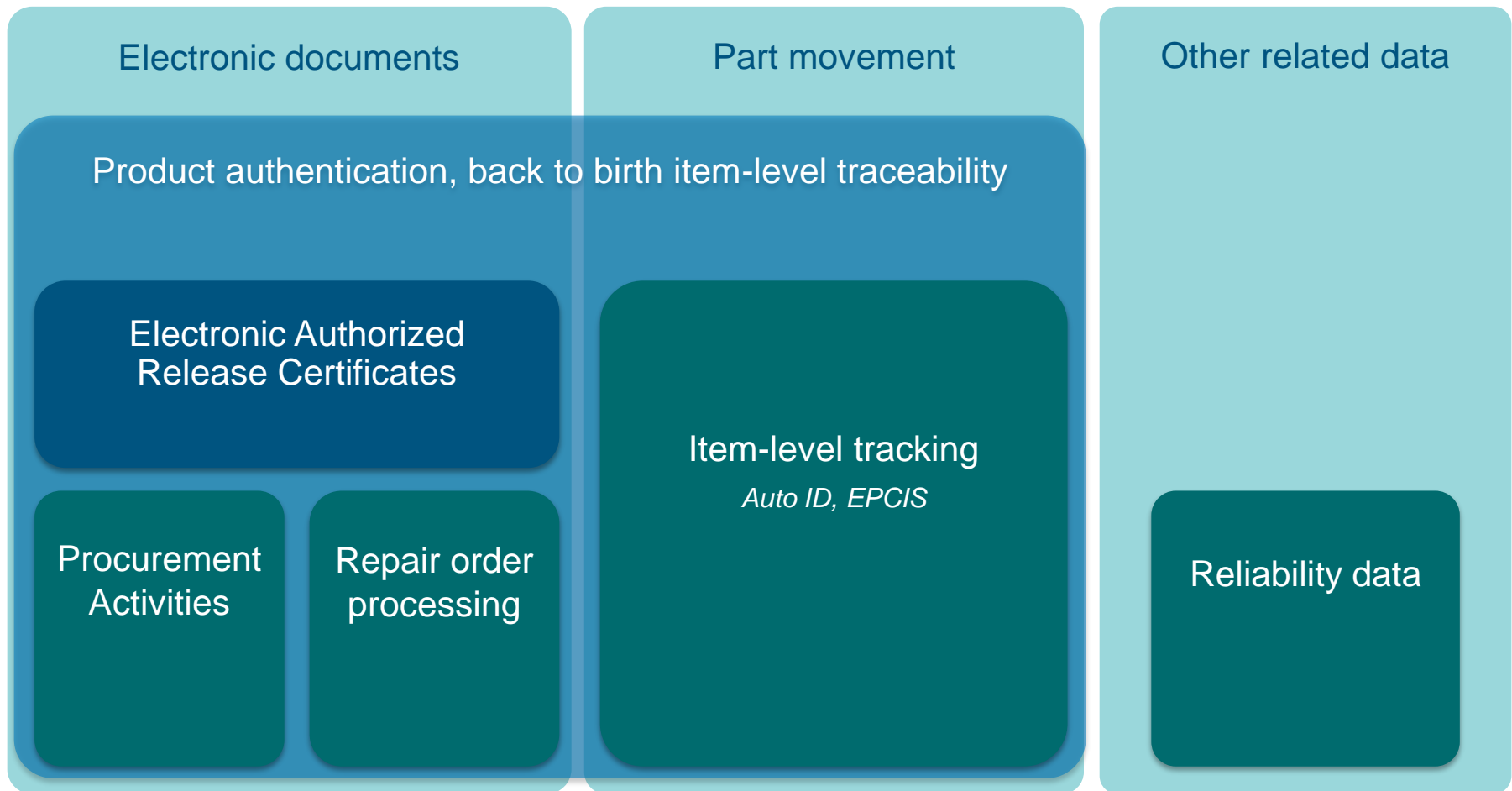


# Common industry goals (quoting the FAA instruction 8130-21G)

- 1) 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.
- 2) 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.
- 3) **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.
- 4) The **frequency of lost, damaged, and unreadable documents** can be significantly reduced.
- 5) The automated processes for generating, transmitting, and processing data will significantly **reduce costly human** errors.
- 6) The cost and difficulty **to store, retrieve, and analyze information** can be substantially reduced.

# Data sharing needs in the MRO supply chain

(SPEC2000 evolution and adoption)



AEROSPACE KNOW-HOW



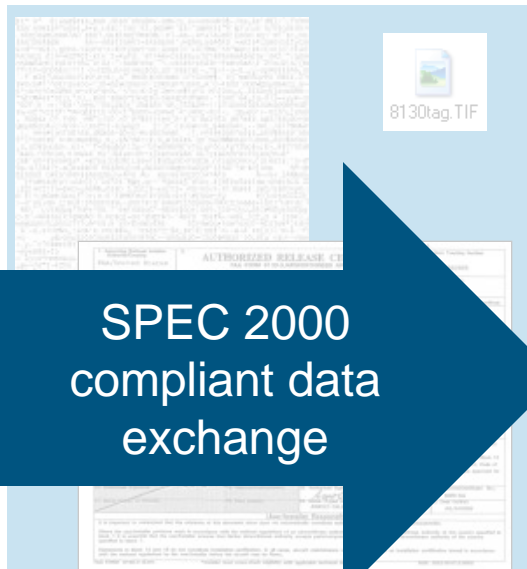
# Authorized Release Certificate moving from paper to electronic XML payload

## Paper document



- ✗ Electronic transfer & storage
- ✗ Digital signature
- ✗ Import of data to recipient's system
- ✗ SPEC2000 compliant e-form
- ✗ Automated validation of data

## Scanned image



SPEC 2000 compliant data exchange

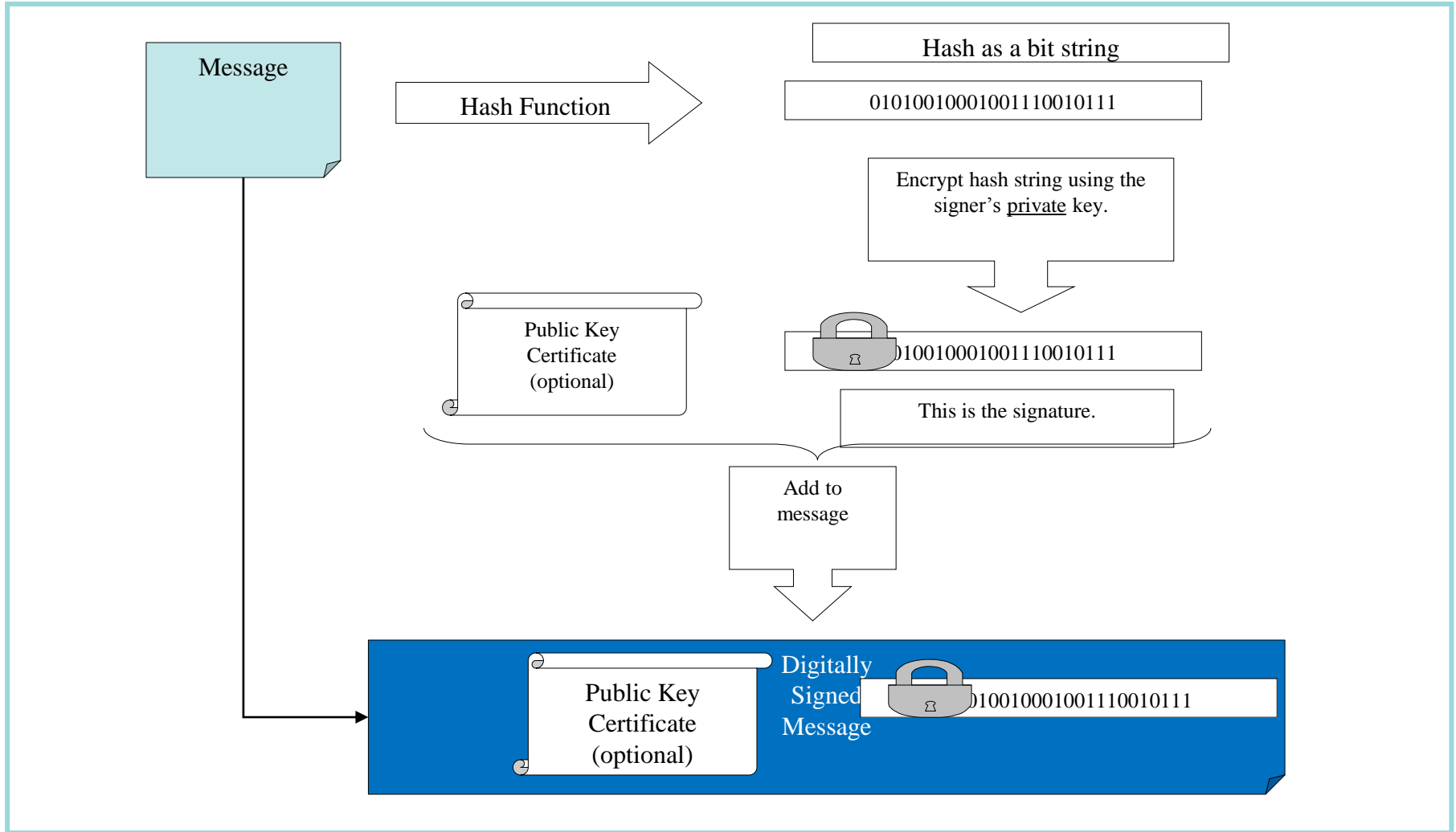
- ✓ Electronic form transfer & storage
- ✓ Digital signature possible
- ✗ Import of data to recipient's system
- ✗ SPEC2000 compliant e-form
- ✗ Automated validation of data

## Digitally signed XML file

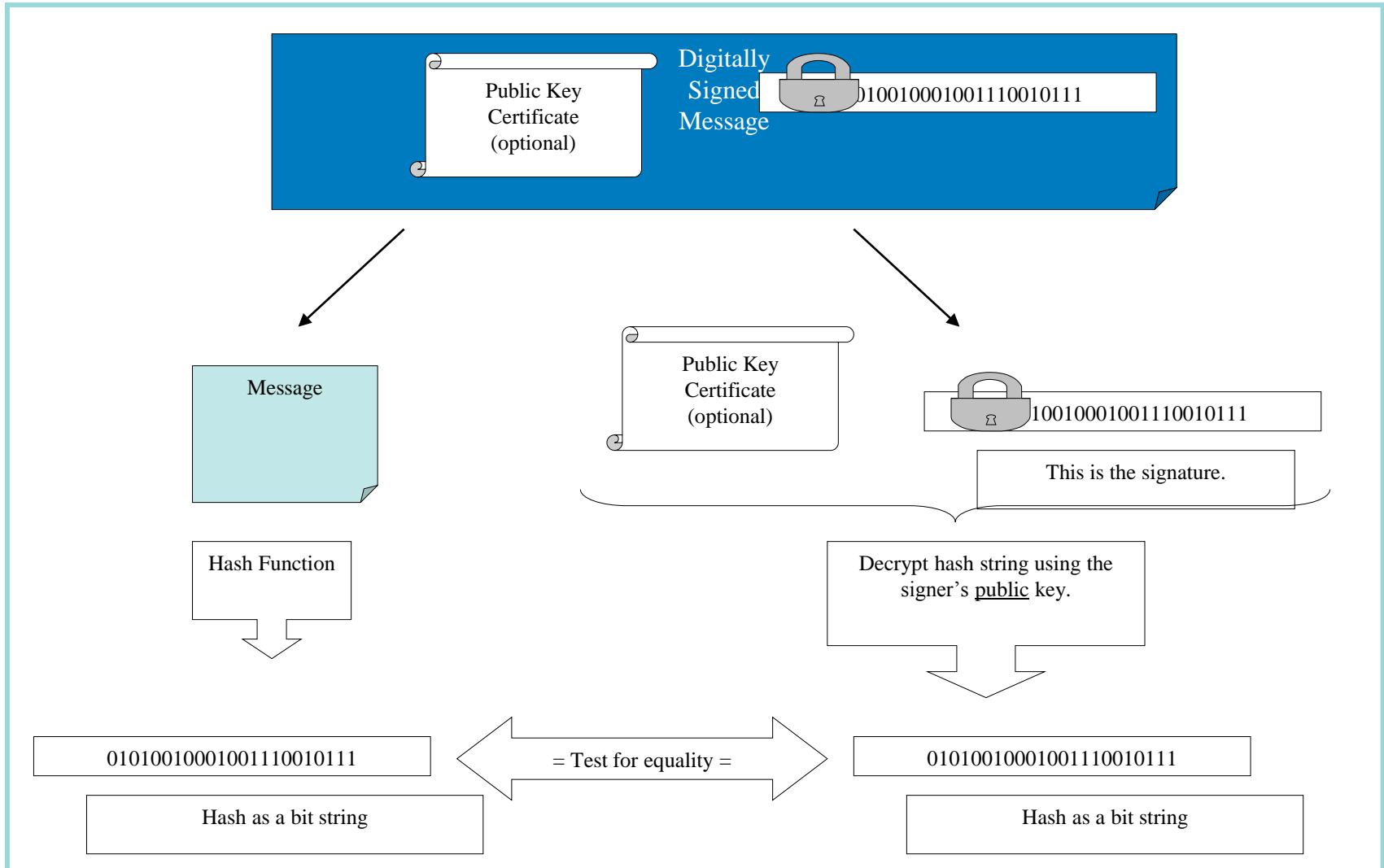


- ✓ Electronic transfer & storage
- ✓ Digital signature
- ✓ Import of data to recipient's system
- ✓ SPEC2000 compliant e-form
- ✓ Automated validation of data

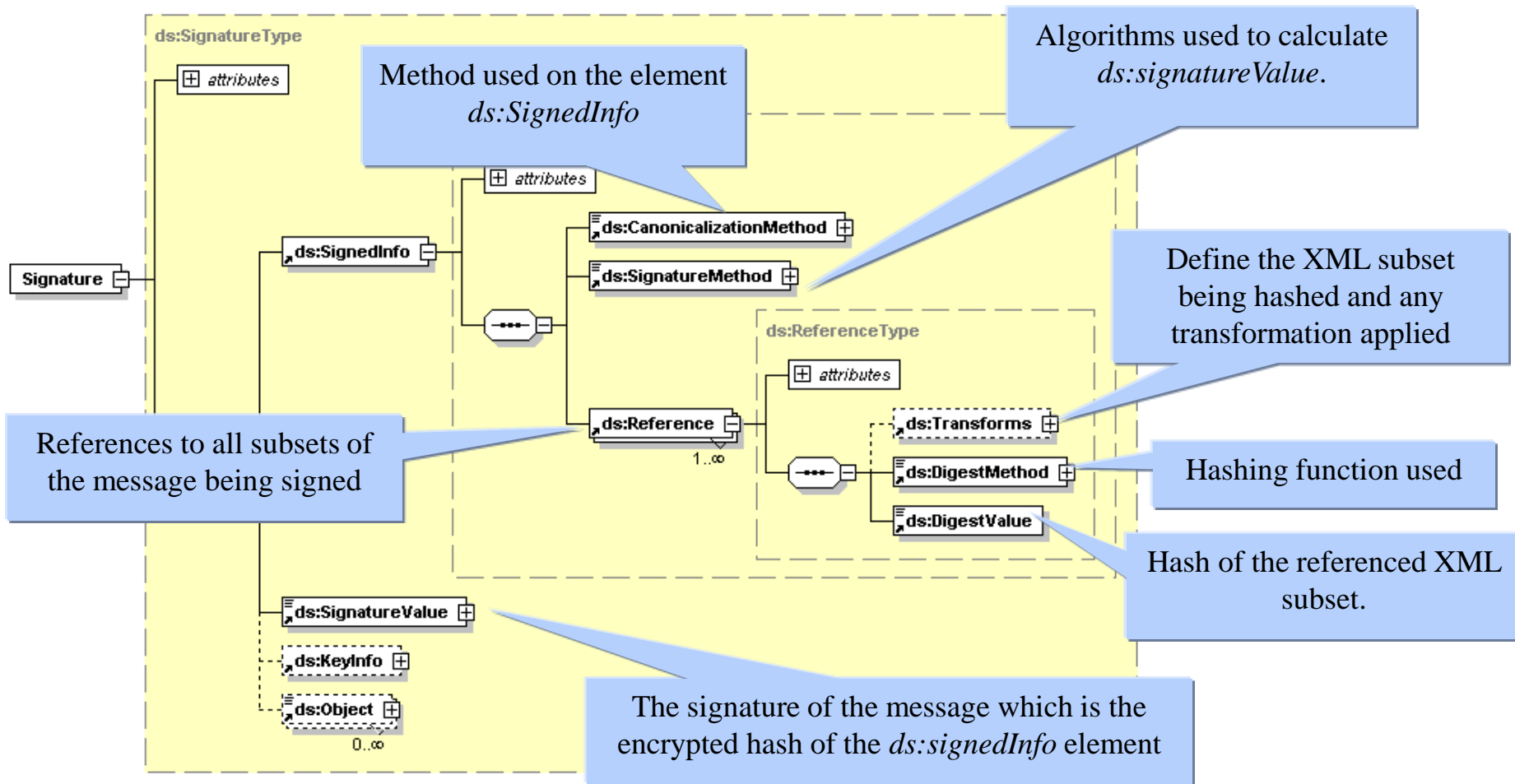
# Fundamentals: digital signature - signing



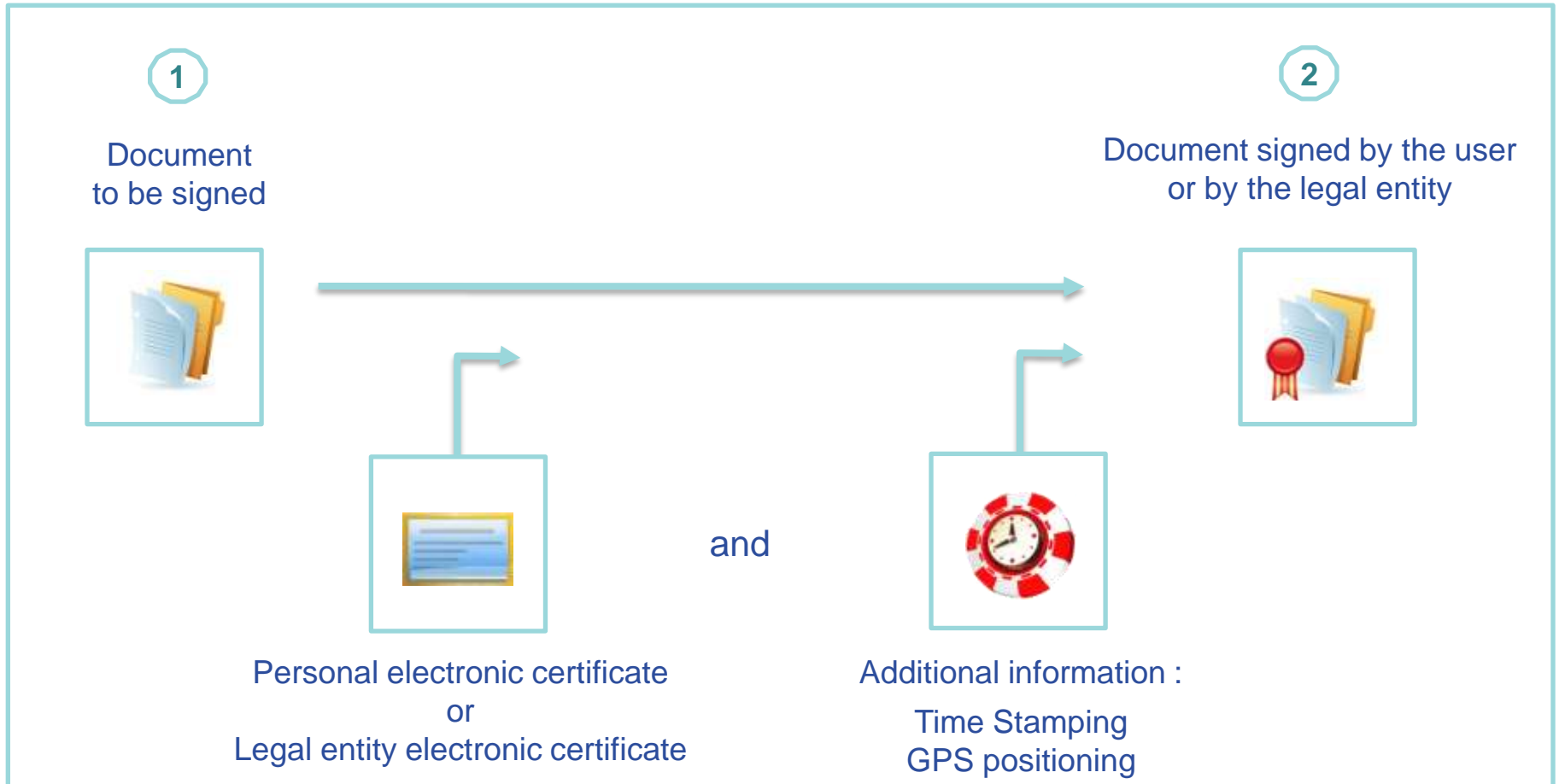
# Fundamentals: digital signature - validation



# W3C XML Digital Signature



# Legal digital signing : how does it work ?



# Some elements exist already ...

... some need to be installed

Form Issuer's ICT infrastructure

Identity & access control

PKI infrastructure

Back office (e.g. ERP)

Digital signature & timestamp

Reliable delivery

Validation & integrity

Secure digital archive

Form Receiver's ICT infrastructure

Identity & access control

Back office systems (ERP, MRO, A/C records)

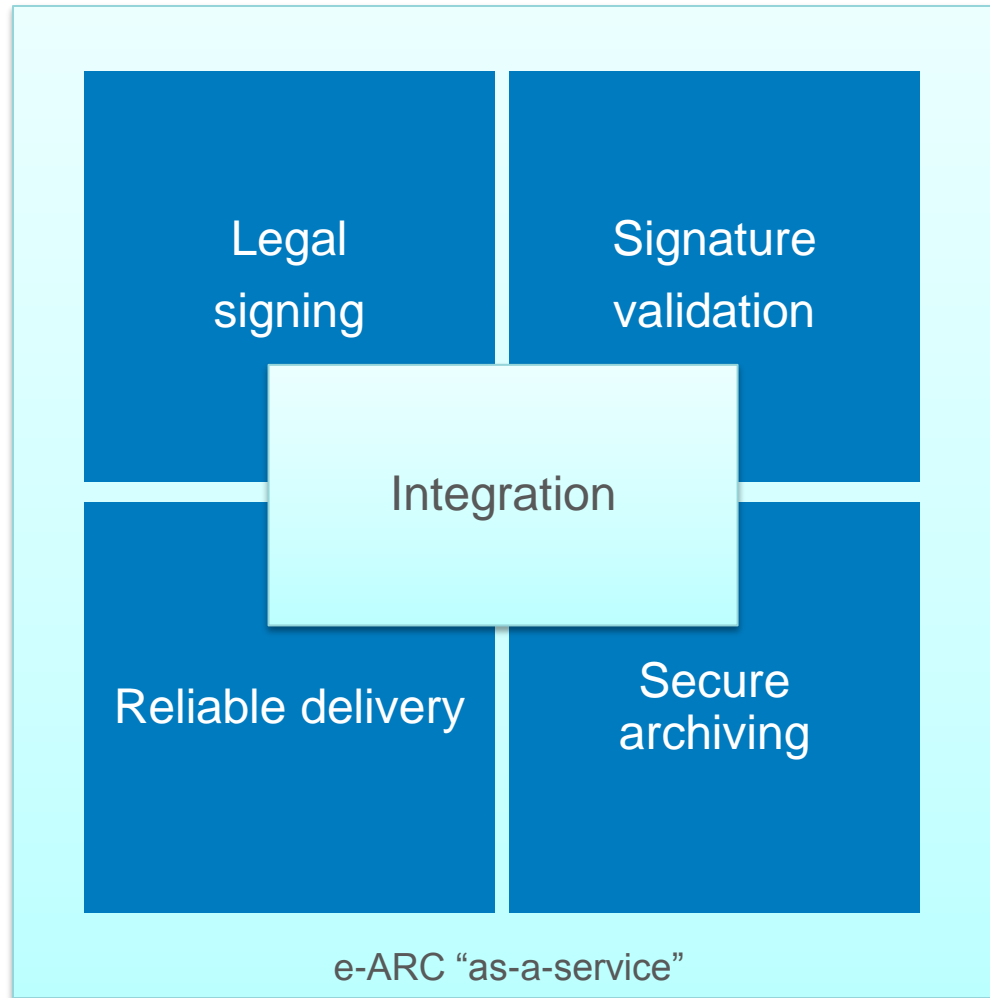
Secure digital archive

Global ICT infrastructure

Industry PKI standards & infrastructure

Industry messaging and communications standards and infrastructure

# Components of a solution



Legal signing

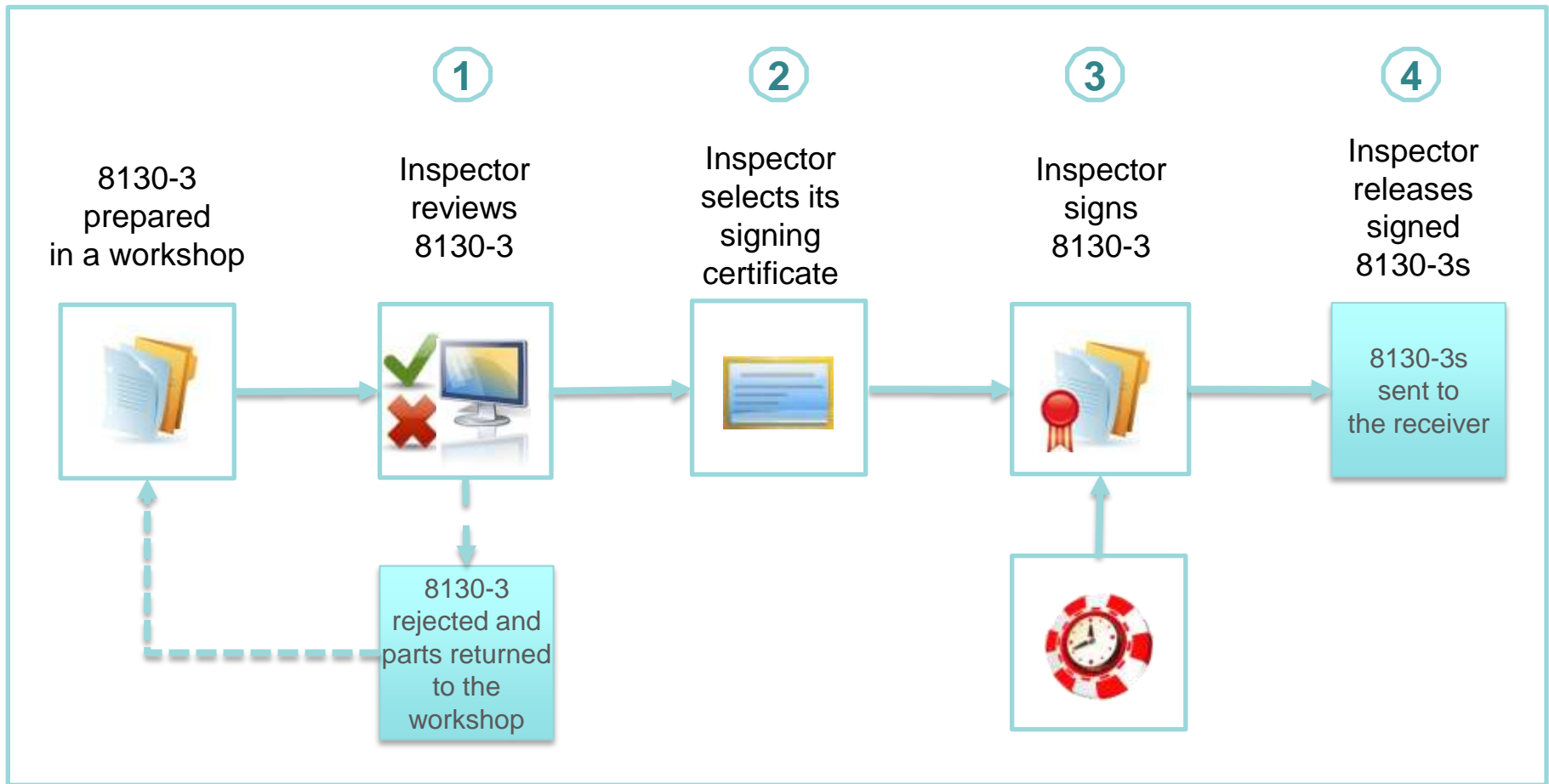
Signature validation

Reliable delivery

Secure archiving

e-ARC "as-a-service"

# Legal signing in 8130-3 context



AEROSPACE KNOW-HOW



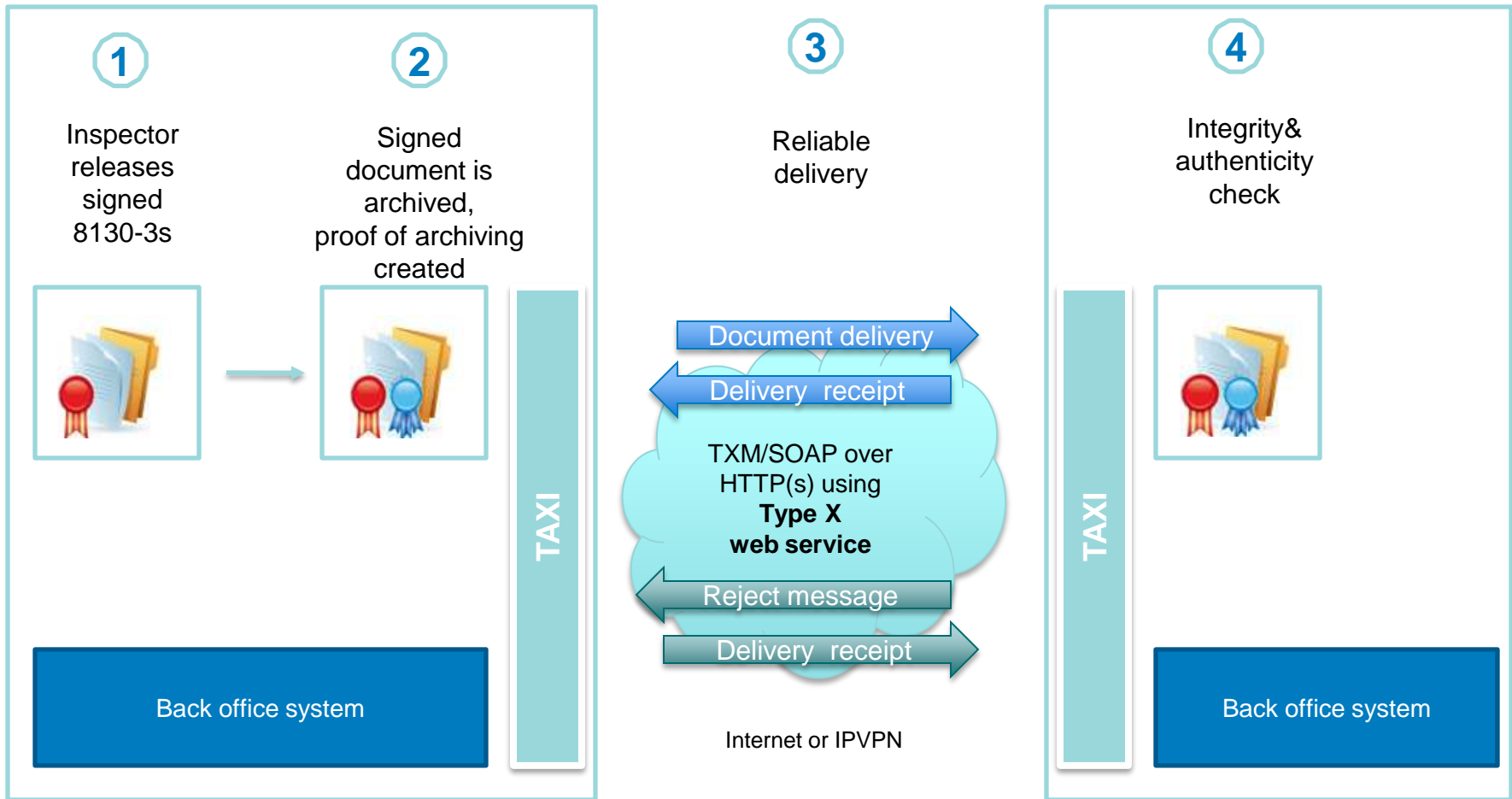
# Legal signing: what should it do ?

## Digital signature under full user's control

- Determination of technical configuration of the user's workstation
- Digital signature applied on user's workstation or a mobile device
- Work as a separate tool or seamlessly integrated in ERP
- Support hardware or software certificates
  - can be stored in the browser or on a smartcard, USB, token...
- Filtering certificates
- Signatory in full control of the signing process
- Rule based workflow to ensure compliance with regulations
  - user must view the form before signing
  - signature is applied at a designated workplace
- Authentication performed as part of signing process
- "Any" device can be used to apply signature
- Integrates with archive and sending function

# Reliable delivery

Legal signing	Signature validation
Reliable delivery	Secure archiving
e-ARC "as-a-service"	



AEROSPACE KNOW-HOW

# Reliable delivery using IATA standard

Legal  
signing

Signature  
validation

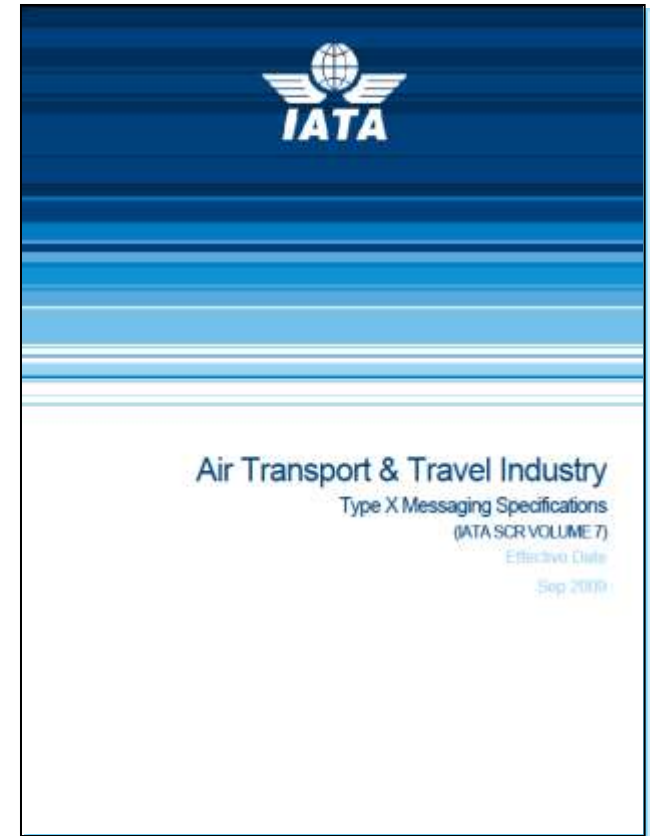
Reliable  
delivery

Secure  
archiving

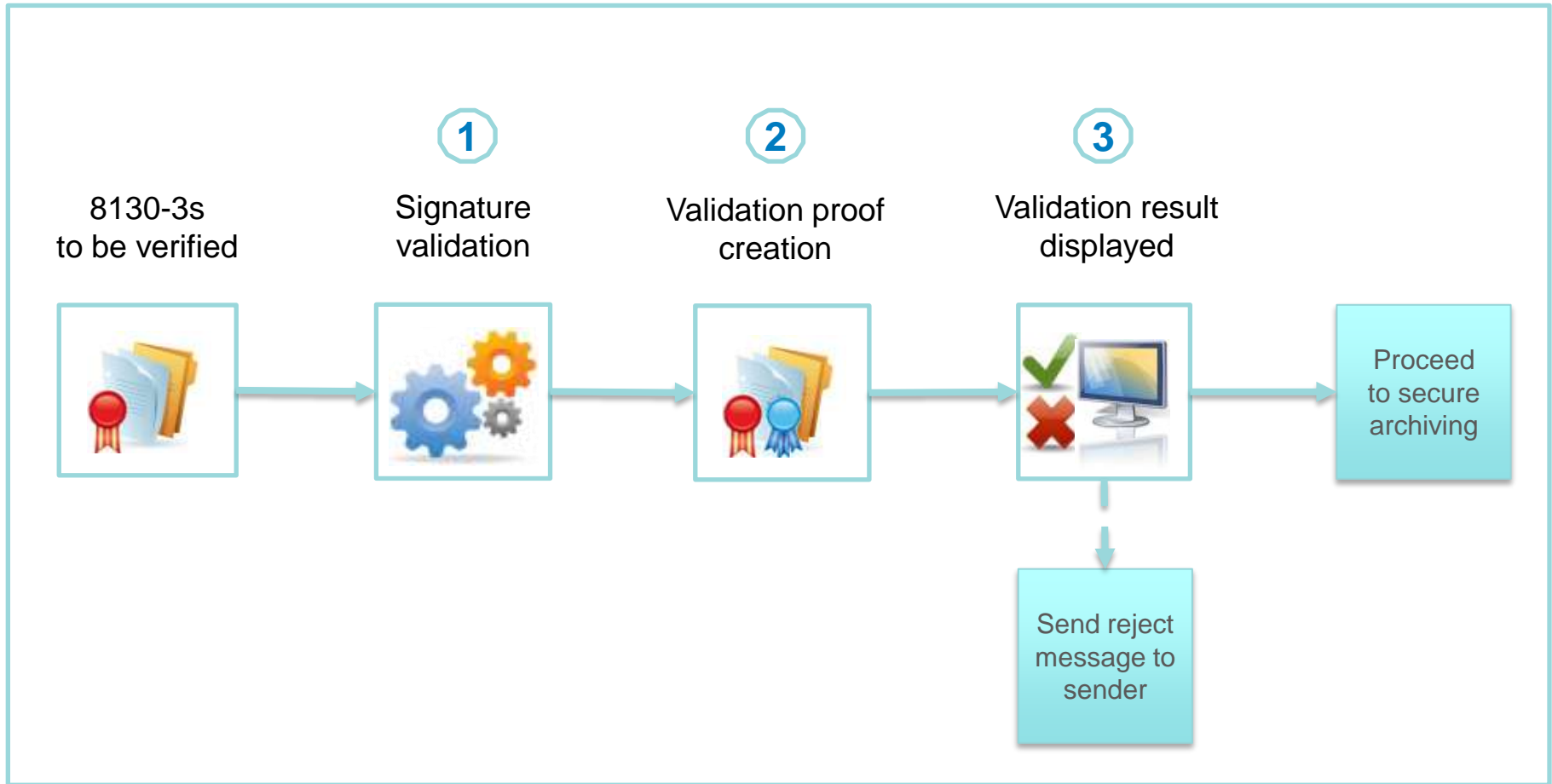
e-ARC "as-a-service"

## Properties

- Compatible with air transport business practices
- Support for all standard ATI message exchange patterns
- Full message delivery assurance and reliability
- All XML based with SOAP, JMS and HTTP bindings
- Security options by composing with W3C standards
- Multicast (one message to many recipients)
- End-to-End addressing (originator to recipient)
- Proof of delivery
- Full traceability
- Permits detection of duplicate messages
- Simplified integration
- Currently used with Spec2000XML



# Signature validation in 8130-3 context



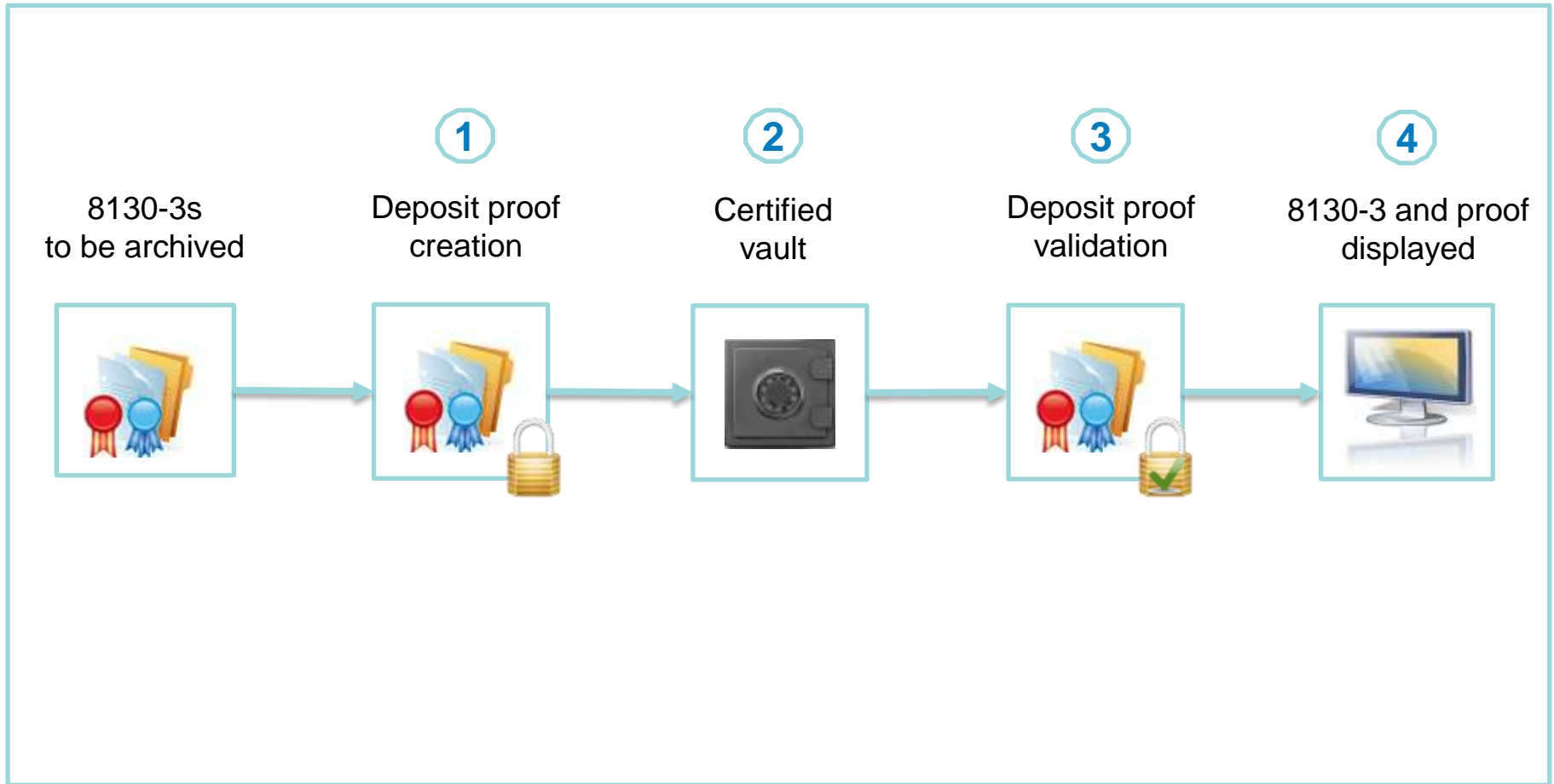
# Signature validation: what should it do ?



## Signature validation and integrity check upon receipt

- Integrate with document receiving function
- Authentication includes certificate validation with OSCP services or CRL
- Generate “reject” message back to sender if authentication fails
- Rule based workflow ensures no invalid documents proceed to QA
- Only authentic documents can proceed to archiving, QA and business systems
- All archived documents with “proof of deposit” showing the check was performed
- No overload with invalid documents
- Full audit trail of “rejects”

# Secure archiving in 8130-3 context



# Secure archiving: user groups

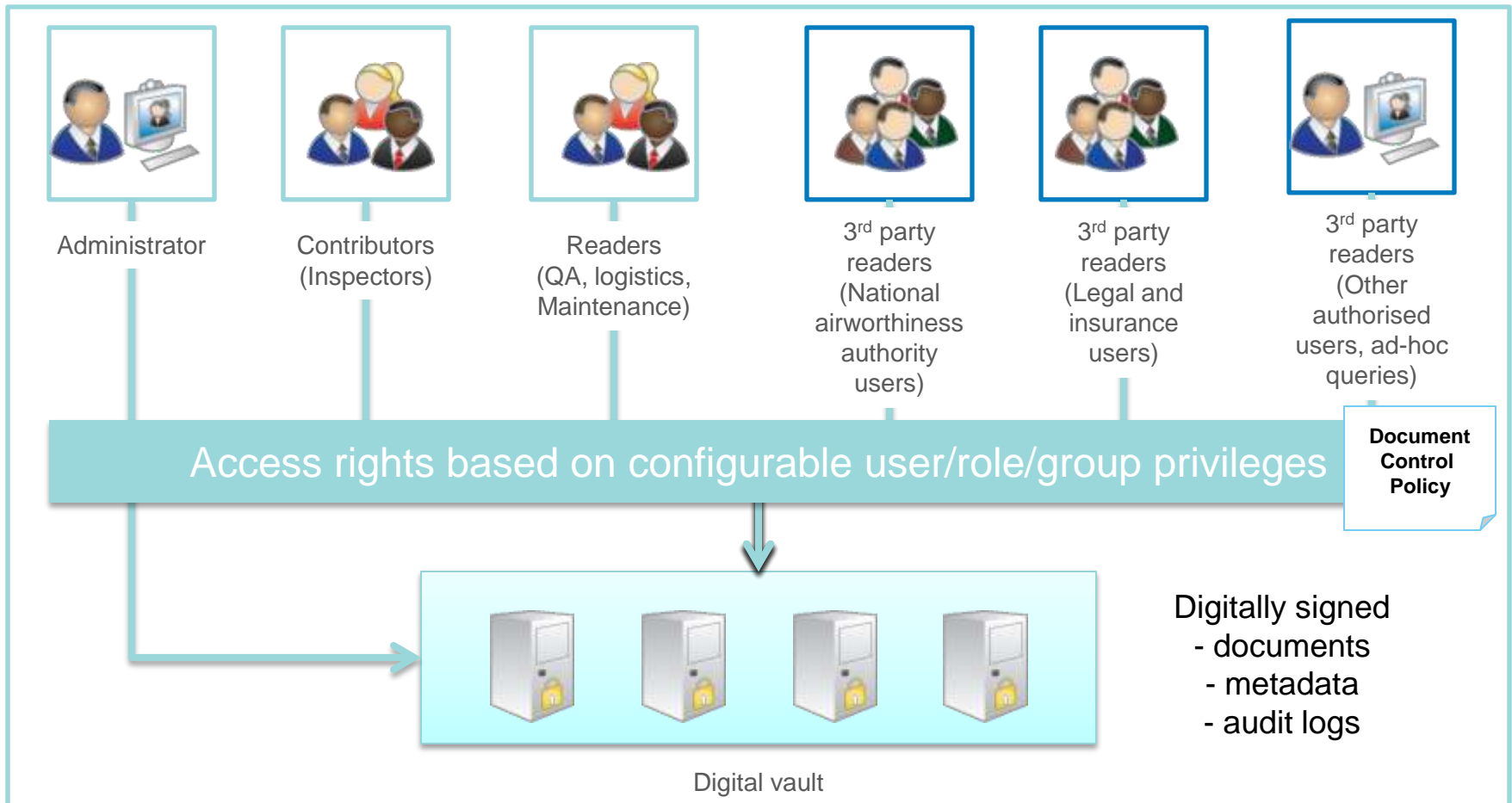
Legal signing

Signature validation

Reliable delivery

Secure archiving

e-ARC "as-a-service"



AEROSPACE KNOW-HOW

Legal signing

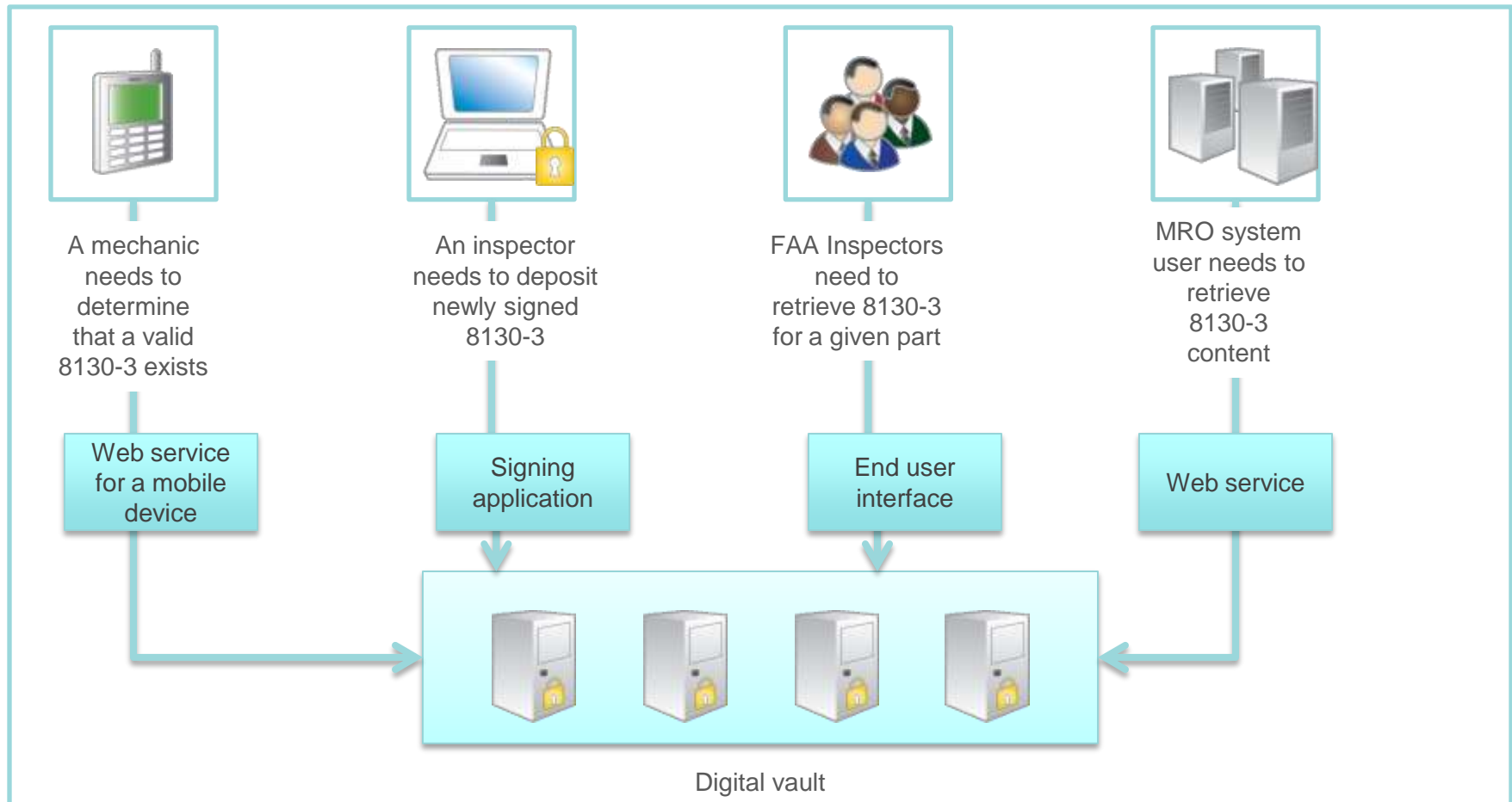
Signature validation

Reliable delivery

Secure archiving

e-ARC "as-a-service"

# Secure archiving: sample use cases



# Secure archiving: what should it do ?

## Digital vault for full control of digital documents

- Authentication upon deposit, deposit proof
- Full data encryption
- Granular access control
- Complete audit trail (such as deposit, retrieval, requests for copies, ...)
- Signature and encryption lifecycle management (re-signature, trans-encryption)
- Guaranteed integrity of documents
- Traceability of actions
- Confidentiality of stored documents
- Long term validity
- Access through user interface or 3<sup>rd</sup> party applications (e.g. ERP)

# Overall solution components

Form Issuer's ICT infrastructure

Identity & access control

PKI infrastructure

Back office (e.g. ERP)

Digital signature & timestamp

Secure digital archive

Reliable delivery

Validation & integrity

Form Receiver's ICT infrastructure

Identity & access control

Back office systems (ERP, MRO, A/C records)

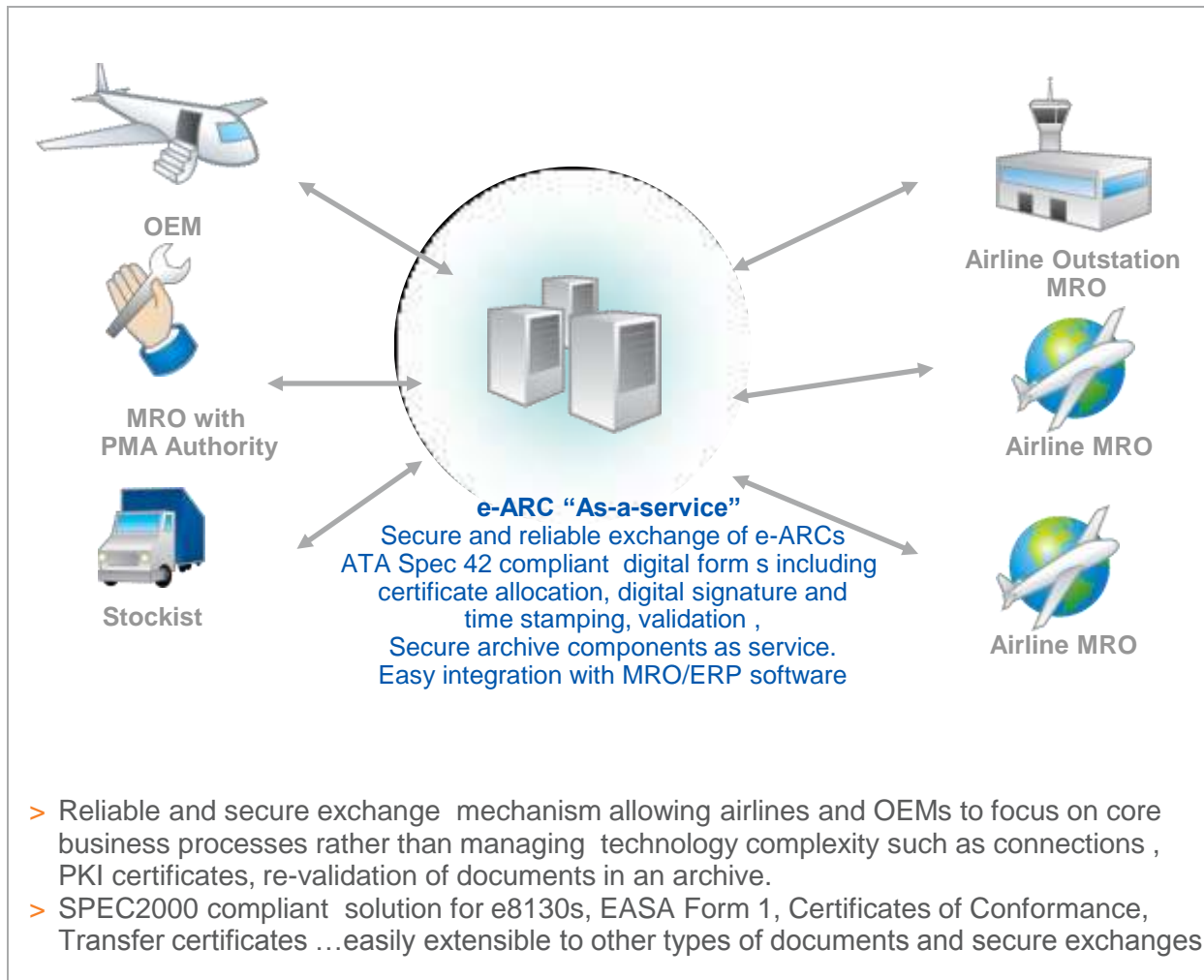
Secure digital archive

Global ICT infrastructure

Industry PKI standards & infrastructure

Industry messaging and communications standards and infrastructure

# e-ARC Service Concept



**Automated integration of data in systems increases speed and reduces errors**

**Consistency and timeliness of data**

**Facilitates data search and retrieval**

**Reduced costs for record retention**

**Difficult to forge because originals can be traced directly to source**

**Pedigree easily available**

# Thank You

[Mansour.rezaei-mazinani@sit.aero](mailto:Mansour.rezaei-mazinani@sit.aero)