



- 
- Public Key Infrastructure (PKI)
  - Obstacles to implementation

Julien Holstein  
[julien.holstein@aerospace-vision.com](mailto:julien.holstein@aerospace-vision.com)

Dave Coombs  
[dcoombs@carillon.ca](mailto:dcoombs@carillon.ca)



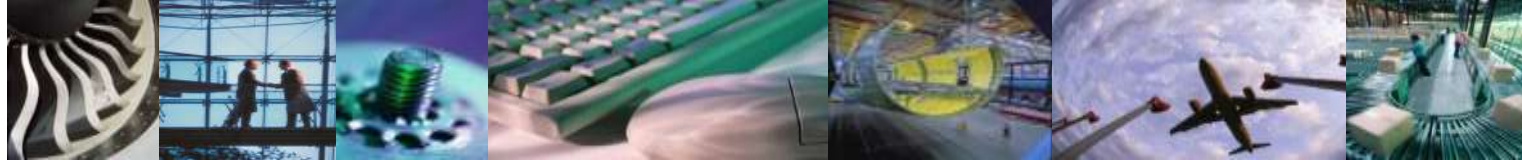
- 
- This presentation is composed of two parts:
    1. A description of the principal obstacles to the implementation of digital signature / PKI
    2. An explanation of the ways in which these obstacles may be overcome



---

- Part One

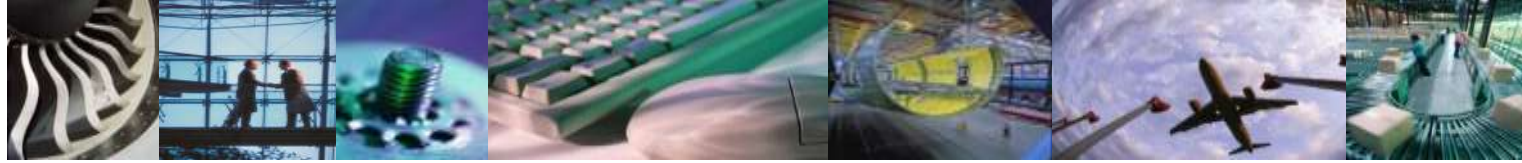
1. Security is not mandated
2. Standards are not complete
3. Standards are not known
4. Implementation processes are not defined
5. The requirements are not clearly understood



# 1. Security is not mandated

---

- Is this true... largely yes.  
Where do we find elements of mandating?  
In requirements for continued airworthiness, in type certification certainly but there is no overarching mandating of the use of PKI as yet.
- The Advisory Circular allowing electronic 8130-3 / EASA FORM 1 mandates PKI, and in order to limit liability airlines would be wise to consider PKI for operations such as software data loading, but this has not been seen as sufficient motivation for airlines to go for a comprehensive use of PKI.
  - Of course the exception here is the requirements of the A380 and B787



## 2. Standards are not complete

---

- Is this true... largely no.  
Standards for interoperable PKI have been developed. These have been developed by the ATA DSWG and the operational trust fabric developed by CertiPath and the aerospace and defense community.  
Some precision is still to be developed:
  - Time-stamping standards
  - Archiving of PKI artifacts
- We are aiming to release a revision in October which includes them.



## 3. Standards are not known

---

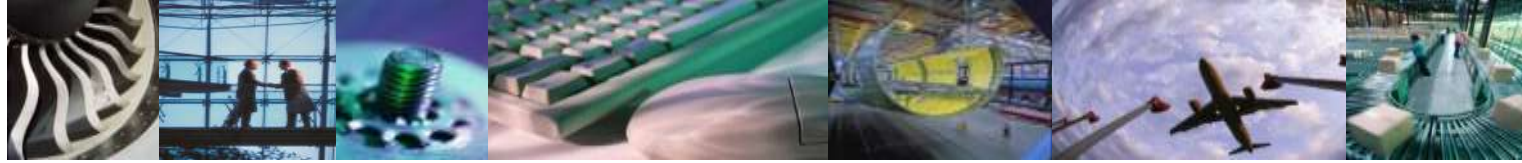
- The ATA is a well known organization, central to the continuous, harmonious operation of commercial aviation.
- The contribution of the ATA members to the creation of Spec 42 however has been quite restrained, and apart from the webinar that was produced this is the way in which knowledge Spec 42 is propagated.
- There is a substantial number of large, medium and small organizations who do not participate in industry activities and who perhaps do not even consider that there is anything to learn.



## 4. Implementation processes are not defined

---

- There is some truth in this statement.
- One of the problems in defining precise implementation processes is the fact that the infrastructure of many airlines is quite individual.
- ATA Spec 42 can identify generic processes but it could be that this doesn't reflect the reality in a given airline.



## 5. Requirements are not clearly understood

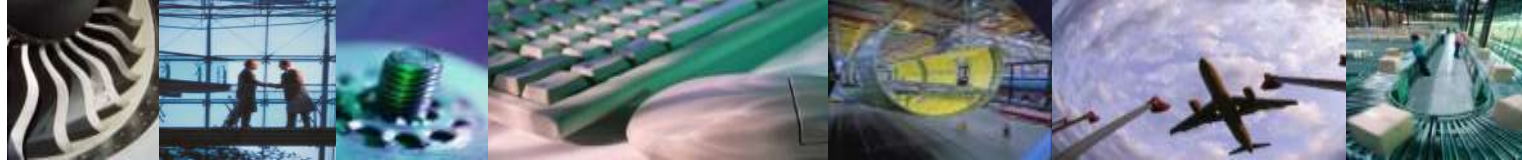
---

- This means that at every attempt to implement there is a tsunami of protest... the result of the implementation is inefficient, bureaucratic, heavy, expensive, ridiculous. Why this reaction?
  - aviation has existed 100 years without it
  - evolution is seen as gradual not dramatic
  - typically avionics engineers do not understand IT security guys and vice-versa
  - investment in security is seen as pushing out investment in facilities which produce an obvious financial return.



---

So what can be done?



# 1. Security is not mandated

---

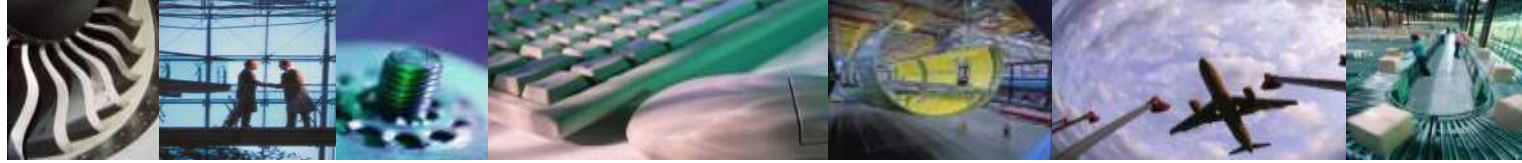
- Chicken / egg?
- Regulators don't want to mandate security with PKI until operators are equipped to deal with it.
- To some extent this will take care of itself as new aircraft do mandate PKI for various systems.
  - Then, operators who do this, and develop the infrastructure and the internal processes, may \*choose\* to retrofit older aircraft with PKI applications/systems to realize long-term cost savings and increase benefit from their investment.
- Expect regulators to mandate security more once airlines and MROs are more used to it and service providers are better established.



## 2. Standards are not complete

---

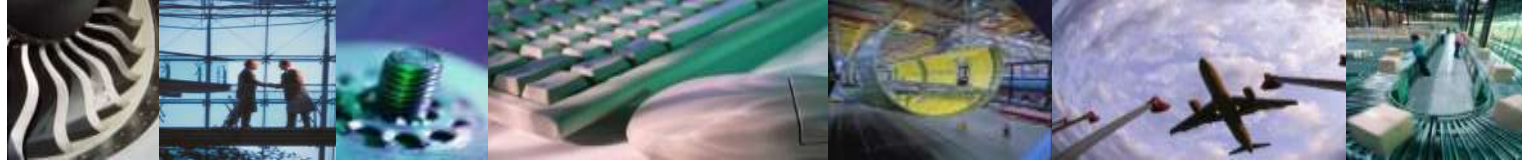
- Mostly not true, as Julien said.
- PKI is not new. Methods and standards developed and refined over 40 years.
- PKI standards for commercial aviation (what became Spec 42) developed over 10 years.
  - Updated annually to reflect ongoing best practices.
  - Includes implementation guidance section.
- Industry trust fabric “bridge” operational since 2006.



## 2b. Standards in use!

---

- Electronic ARC (e8130, EASA FORM 1)
  - Orders reference Spec 2000 chapter 16, which says PKI shall be done the Spec 42 way.
- Every Airbus A380 has PKI certificates on board, compliant with Spec 42 policy.
- Boeing 787 requires PKI certificates compliant with Spec 42 as well.
- Gatelink (ARINC 822 references Spec 42)
- Software/data loading
- EFB
- Secure ACARS



## 3. Standards are not known

---

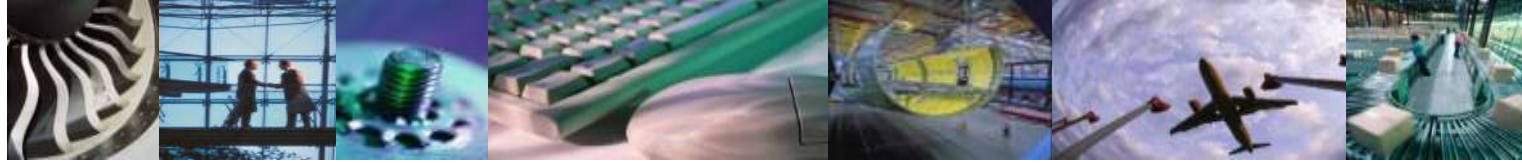
- Spec 42 written by DSWG members: mostly manufacturers, vendors, and suppliers.
  - Airline participation has been “inconsistent”.
- Launching new aircraft will be smoother for airlines with exposure to the standard and an understanding of the requirements.
- Airlines can also take advantage of PKI solution providers and service providers to help bridge this knowledge gap.
  - But best is to get involved and share airline perspective with the DSWG!



## 4. Implementation processes are not defined

---

- Related to the previous point... Standards may not reflect airline reality given limited airline input.
  - And every airline is different anyway!
- PKI service providers understand how to implement Spec 42.
  - Missing piece: integrating with existing airline business, maintenance, and management processes.
- As more airlines do launch new PKI-enabled aircraft, please share your experiences to help DSWG improve the standard.



## 5. Requirements are not clearly understood

---

- Eventually, digital security for connected aircraft will be a necessary component of airline business, regardless of inertia and protest.
- In the nearer term, this can only be addressed by explanations in forums such as this, and by the increased participation of the airlines in the aviation security standards organizations, notably the DSWG.
- The business deciders in the industry want to make investments with an attractive ROI. This means not making investments today which have to be thrown away tomorrow morning.
  - The implementation of cross-certified interoperable PKI delivers that.
  - One implementation can be used for many projects, purposes, and facets of business.



---

Thank you.