

Industry Requirements for Digital Security



JULIEN HOLSTEIN
AEROSPACE VISION

Our Industry , your Industry has gone from very simple to very complex in a comparatively short time.

Your world is changing at an increasing rate , every year the paraphernalia of life becomes more sophisticated

My object today is to persuade you that our industry needs digital security and to motivate you to embrace it.

We need your support to achieve the goal of securing our industry.

You are the key.

This includes engineers in flight operations , in maintenance, the flight crew themselves, support services, airport operators, airline management,

Original equipment manufacturers- including engine manufacturers, not just the airframe manufacturers.

It includes manufacturers of UAVs or drones , helicopters and also the defense establishments. It needs the help and support of the regulators.

Lastly ,but not least , it needs the national and international security standards organizations to work closely together so that the standards work across the face of the globe.

AUDIENCE

How many of you know what we mean by the connected aircraft?

How many think that this challenges the security community?

Thank You

Lets look together at what this means.

Integrated Digitalization

increased proximity of civil and defense operations



- **BEFORE**
- Civil
- Limited to specific corridors
- **AFTER**
- Sharing a common sky
- Increasing use of convertible defense equipment

- **BEFORE**
- Defense
- Limited to specific zones unless operational requirements dominate
- **AFTER**
- Sharing a common sky
- Increasing use of sub-contracted services
- Increasing use of convertible civil equipment.

But also :

The integration of operational security readiness to ensure the protection of critical national infrastructures

The ability to effectively support humanitarian relief efforts in case of natural disasters, civil unrest, or help to the civil, population resulting from military action.

The consolidation of SPEC 2000 and S1000D is a consequence of this development.

What are the drivers behind this development?

The one sky is part of the attempt to counteract global warming since the indirect routes followed today by commercial aircraft generates unnecessary fuel use.

The increasing pressure on the airline industry to reduce costs supports the one sky approach.

Tighter defense budgets have generated the strategy that tankers can be convertible –when not needed for defense purposes they can be used to carry passengers.

The military now also relies far more on private support services because they are both cheaper and more flexible than the equivalent military establishment

At the extreme even the military themselves are outsourced

Data Sources reach back to the Originators

**Here is an extract of the Industry mind map
that was developed by Jean-Paul Moreaux
within EuroCae 72**



use case starts when the requests to make a Load and Balance Calculation
system prompts for the Aircraft Data
provides the Airfield Data
system prompts for the Cargo Load Distribution
provides the Cargo Load Distribution
system prompts for the Passenger Load Distribution
provides the Passenger Load Distribution
system prompts for the Fuel Load
provides the Fuel Load
system prompts for the Catering Load
provides the Catering Load
system calculates and stores the Load and Balance Information
system displays the Load and Balance Information
use case ends.

This shows a sample of the processing chain that makes up the EFB

use case starts when the requests to make an [Aircraft Performance Calcul...](#)
system prompts for the [Airfield Data](#)
provides the [Airfield Data](#)
system prompts for the [Load and Balance Information](#)
provides the [Load and Balance Information](#)
system prompts for the [Flight Performance Items](#)
provides any [Flight Performance Items](#)
system calculates the [Aircraft Performance Data](#)
system displays the [Aircraft Performance Data](#)
use case ends.

This is another example of the processing chain that makes up the EFB.
Note that these two examples are themselves interdependent.

Compare the A320 and the A380 the prevailing technological environment

A320

- Data loading by floppy disks and then CDs physically loaded.
- Aircraft not connected to extranets
- Diagnostics on aircraft condition on the ground

A380

- Data loading by uploading from data providers secured .by PKI
- Aircraft receiving up to date information throughout the flight
- Diagnostics on aircraft condition during the flight cycle

To summarize the main currents of change

- 1. The increased proximity of the civil and defense sectors**
- 2. The transformation of the aircraft from being independent from data communications during the flight cycle.**
- 3. The transformation of the ATM from voice as primary to data as primary.**
- 4. The triangulation of the aircraft, ATM and the airline itself in the second by second ATM process in NextGen and SESAR.**
- 5. Therefore the need for SAFETY experts and SECURITY experts to work more closely together and**
- 6. The need for the International Security Standards to be constructed for world wide use.**

PKI is our best tool



**BUT UNDER WHAT
CIRCUMSTANCES?**

PKI , or public key infrastructure is a way of protecting data

It can be used to ensure integrity, to allow audit, to prove delivery of data (non-repudiation) , to prove identity and when necessary to ensure confidentiality.

A really useful PKI is one which can be relied upon.

Some of the main actors in the industry have built upon the standards written and promoted by the ATA DSWG to create the industry bridge, CertiPath.

Companies can either create their own PKI Services , cross-certified with Certipath or buy cross-certified certificates.

We are concerned here with unclassified information, not with national defense classifications.

The Current State of Security



- **There is the concern that investment will be too slow. As the new aircraft will be a small proportion of the worlds fleet, what is the incentive to invest.**
- **In operations , where legacy rules, security could be an orphan. This is a major concern. Even if securing the data and the process flows can ensure the survival of the airline, most of the time security is the orphan.**
- **Examples here : baggage handling – the link between passengers and their bags.
: RFID applications – implementation now, maybe security later.**

- **Each organization has its own processes and procedures, implemented over a long period of time and using a number of ways to secure the data.**
- **In order to become more efficient, reducing costs, carrying more passengers for each liter of gallon of jet fuel used, our industry needs to have end to end security with some key functionalities, integrity, non-repudiation, authentication, auditability and sometimes confidentiality.**
- **Before this generation of aircraft the lack of investment in security was limited in its consequences since the processes were uncoupled.**

Of course there have always been some problems.

Standards Organisations and their work



Work group	Objective of the workgroup	Industry Expectations
DSWG	<p>Development of civil PKI standards</p> <p>Oversight of all ATA projects</p> <p>Define Identity and Risk Management specifications for Air Transport Industry</p>	<p>standards recognized are</p> <p>those used by airframe manufacturers and supply chain</p>
AEEC	Development of risk assessment 811	Fully recognize DSWG
811	Data loading	
822	Create definition for “Gatelink”	
823	Secure ACARS	
666/667	Create definition for software loading	
EUROCAE 72	<p>Development of new certification requirements for connected aircraft</p> <p>including security</p>	<p>that they are completed</p> <p>Ensure necessary expertise used</p> <p>Covers groundworthiness & the aircraft</p> <p>Close collaboration with WG 71 and 73</p>

Joint Co-ordination group - This is the group charged with ensuring no overlaps in the creation of international security standards. The goal is a coherent set of security standards , accepted by all.

UK CPNI	UK Government accept the industry security strategy
CertiPath PMA	Governance of the Cross-certification Definition of the Management of Device Certificates
TSCP GB/EAG+/BDG	Definition of Industry secure collaboration methodology
CertiPath Audit WG	Definition of the audit regime Management of the audit regime
4 Bridges WG	Coherence of Bridge Management
DOD Interface WG	Acceptance of external cross-certified PKIs
US Federal PKI	Acceptance of external cross-certified

EUROCONTROL SET ATM Security **The manner in which ATM is implemented is aligned with ATA/AEEC/ICAO**

ICAO WG I **UN Organisation which is the final regulator**
Create definition for Next Generation ATN **Fully recognize DSWG**

RTCA SC 216 **US based development of new certification requirements for connected aircraft**
match EuroCAE view where applicable merging security and safety
FAA issues guidelines to the industry closely related to SC-218 **Fully recognize DSWG**

FAA - CertiPath Co-ordination

Encouraging FAA to use Federal bridge certificates **e.g secure e-mail**

What is the Strategy?



**CONVERGENCE OF SECURITY TOOLS
AROUND PKI**

CONVERGENCE OF CIVIL AND DEFENSE

CONVERGENCE OF SAFETY AND SECURITY

On the
ground

In the air

Civil

In the
office

On the
products

On the
ground

In the air

DEFENSE

In the
office

On the
products

Identification



PEOPLE

ASSETS



People

In the U.S there is HSPD 12 and following that FIPS 201

This imposes in the Federal Government identity vetting and management to a very high level.

Security , after all, is a marriage between good man management and robust technical implementations

In Europe the same approach exists but law limits some of the checks that are available in the U.S .

The checks concerned are ;

- good neighbor
- credit checks
- direct criminal checks

Assets

There are several aspects that have to be resolved;

1. How to consistently manage device certificates ,
that is , certificates
that are issued to a sponsor who themselves has
been through a thorough identity management and
vetting process.
2. How to uniquely identify flying objects.

Digital identity of aircraft



- Aircraft in flight are identified to ATC by a number of different means:
 - ✦ Flight number
 - ✦ An 'ICAO' 24 bit address
 - ✦ Mode S address
- These aircraft identities are not secured, and can fail.
- With the advent of SESAR and NextGEN, and the 'connected aircraft' and more automation, there is a need for aircraft to be **Digitally Identified**. See ATA/AEEC white paper.
- This Digital Identity must be appropriately secured, and be capable of surviving failures.
- We have proposed that this Digital Identity:
 - ✦ Should be an industry standard 'Vehicle Identification Number' (VIN)
 - ✦ The VIN is to be 'burnt into' the aircraft for its life (as cars)
 - ✦ Alternatively there is an ISO standard 15459 which needs to be examined.
- Some benefits seen are:
 - ✦ Essential to automate ATC and communication systems securely
 - ✦ Minimize the number of digital certificates on an aircraft
 - ✦ Become a central reference of aircraft identity for all systems that need this
- Using the same logic, we also consider that Digital identity will be required for Air Navigation Service Providers, airports, general aviation, business aviation, UAVs, navigation beacons, etc....

Simulation



**HOW CAN WE PROVE
THAT DATA FLOWS ARE
APPROPRIATE
BEFOREHAND?**

Proposal for a AES



EXPLANATION

CONCLUSION



1. THERE ARE NOT MANY OPTIONS OPEN TO THE AEROSPACE AND DEFENCE COMMUNITY

2. THIS STRATEGY IS LARGELY AVAILABLE FOR IMPLEMENTATION TODAY

3. THE OBSTACLES ARE CULTURE, FINANCE, THE SCALE OF THE IMPLEMENTATION, TIME, LACK OF UNDERSTANDING OF OUR COMMON RESPONSIBILITY.

4. BUT WE HAVE TO SUCCEED