



Securing Your Data – ATA Spec 42

Regan Brossard - The Boeing Company
June 2017

Agenda

- PKI - Use in the Aviation Industry and why is it necessary
- Guidance for Transitioning to Connected Airplanes
- Choosing an Appropriate Level of Assurance
- Current DSWG and Related Industry Activities



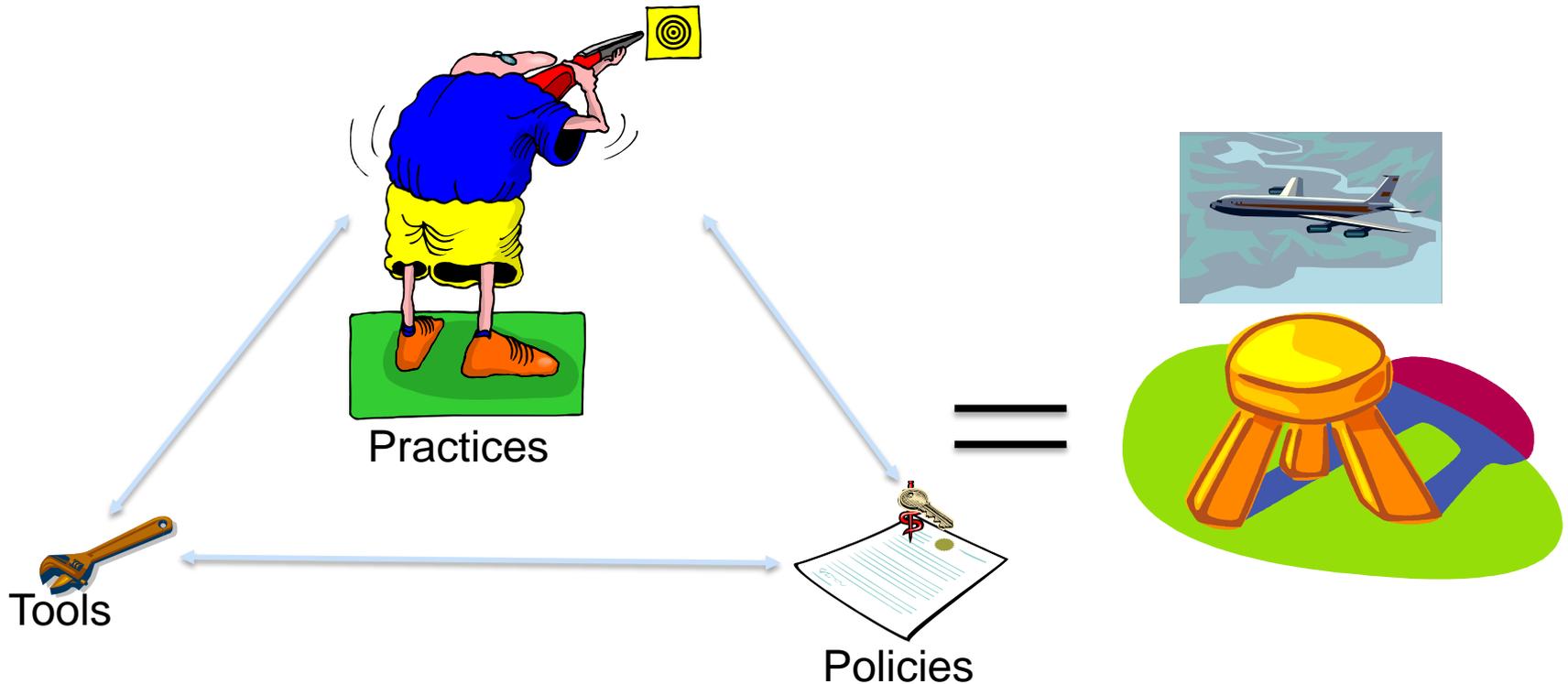
Department of Defense – Cyber Strategy

- We are all vulnerable in this wired world. Today our reliance on the confidentiality, availability, and integrity of data stands in stark contrast to the inadequacy of our cybersecurity.
- The Internet was not originally designed with security in mind, but as an open system to allow scientists and researchers to send data to one another quickly.
- Without strong investments in cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack.
- Malicious actors use cyberspace to steal data and intellectual property for their own economic or political goals.
- An actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems.

DOD Cyber Strategy, April 2015

What is PKI?

Public Key Infrastructure (PKI) is a set of tools, policies and practices for protecting digital assets.



Use in the Aviation Industry

Function	Old	New
Distribute airplane software	Media sets using floppy disks or other physical media (small quantity)	Electronically distribute (thousands of parts)
Load Airplane software parts	Data loaders and other maintenance devices	PKI Signed Parts, load via Onboard Networks
Offload of Flight Operations data	Manual transfer via physical connection	Automated transfer over wireless connection
Documenting maintenance records	Paper based and signed by mechanic	Electronic – signed with certificate
Authorized Release Certificate	Paper based form stored in warehouse	Electronic – signed with certificate
Weight and Balance data and calculations	Complex multi-step process	Automated, based on airplane data
Wirelessly Connect to an airplane IP Network	N/A	Authenticate and securely transfer data to/from A/P

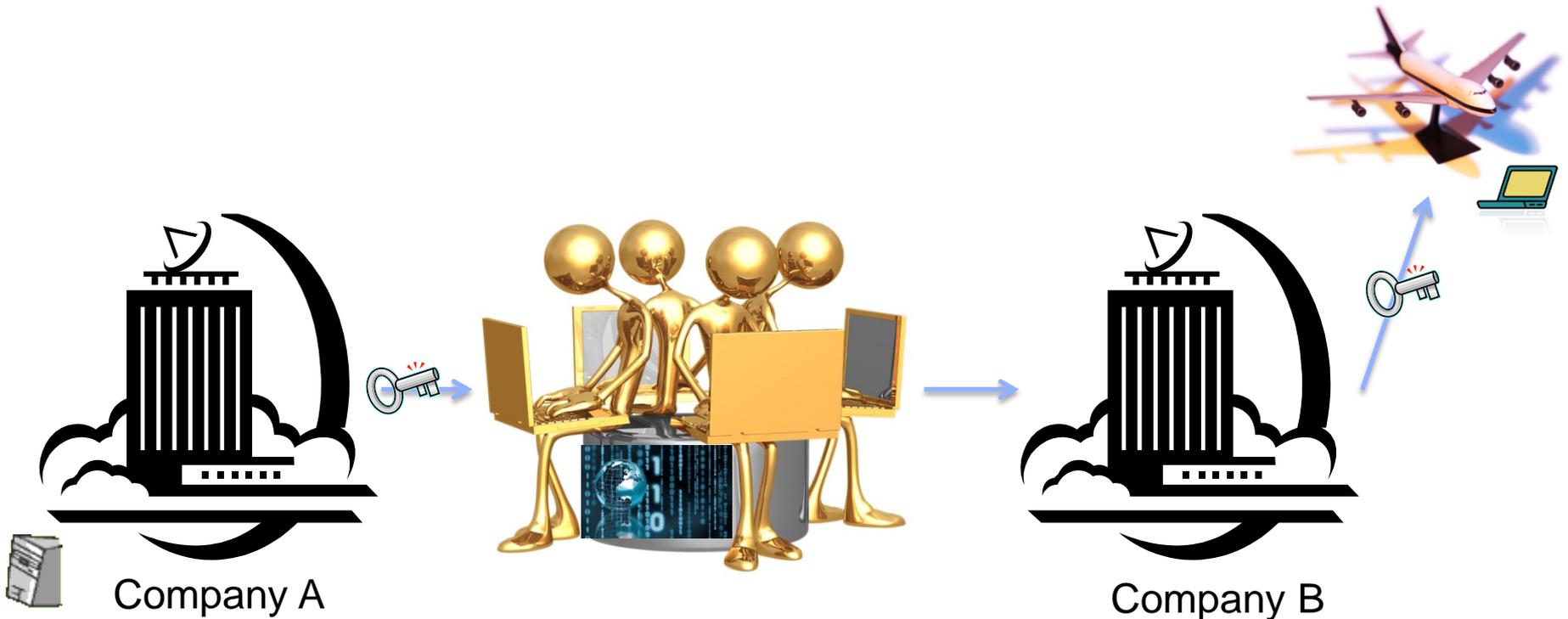
Transitioning to Connected Airplanes

- Strategy is to leverage technology where appropriate to improve maintenance execution, increase data integrity, timely offload and use of airplane flight ops data while minimizing security risks
- Design objective of a PKI solution should be to minimize impact to existing airline operations and maintenance processes
- Connected airplanes require PKI to provide the security necessary to operate

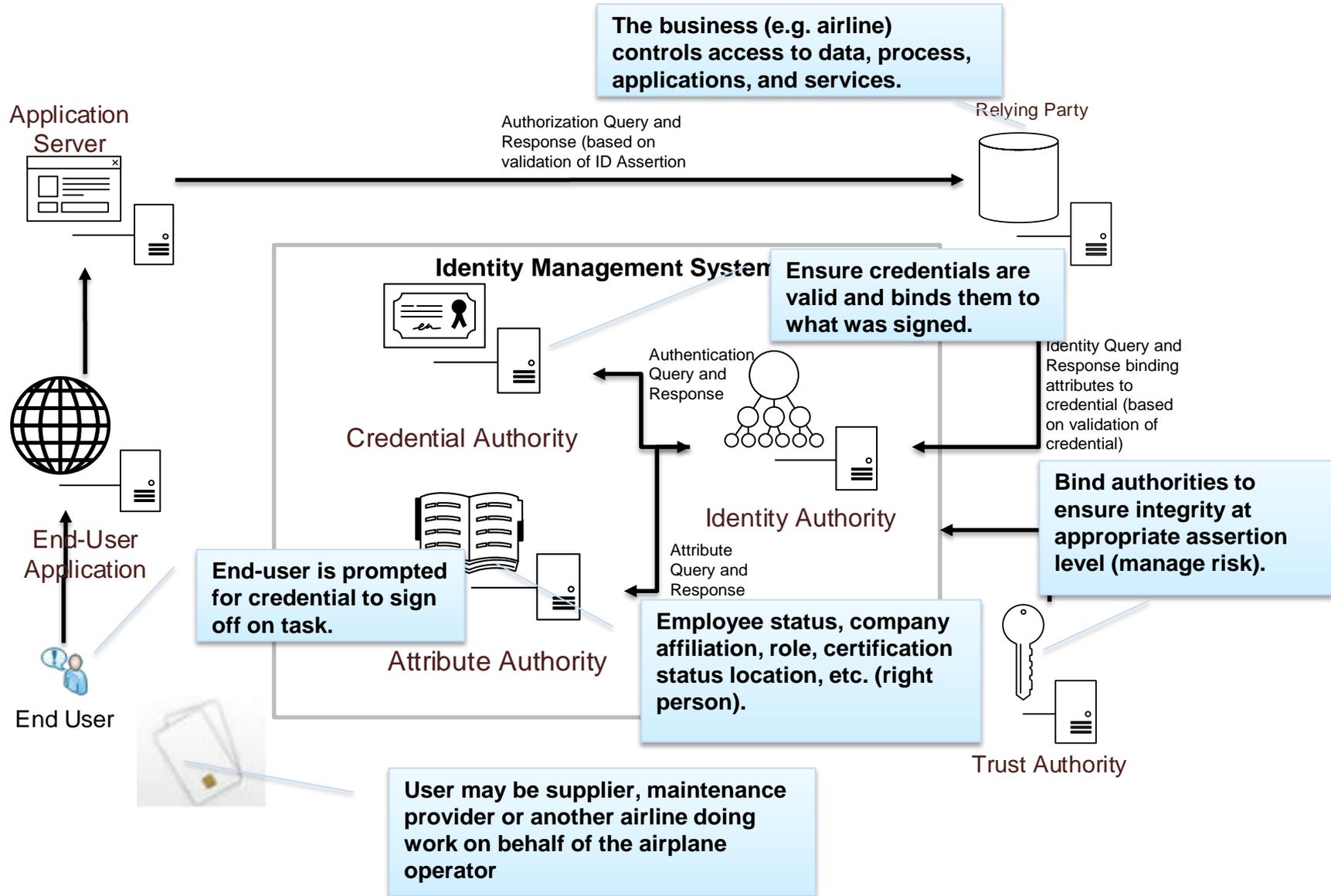


Why PKI?

The primary purposes of PKI are to protect assets that travel through or are exposed to untrusted, external environments such as the public internet and to protect the exchange of information between companies.



Using PKI - Key Objectives



Appropriate Level of Assurance

In the context of Digital Security, Assurance Level, refers to the confidence that a certificate was used to perform some action and that it was done with knowledge of the identity of the individual or entity associated that with certificate.

Spec42 defines a number of assurance levels and the requirements to achieve those levels.

Understanding the requirements to achieve these levels of assurance are critical aspects of ensuring the integrity of your data.

Determining the right level of assurance requires a risk analysis to be performed. Asserting unnecessarily high levels of assurance adds complexity and cost.

Spec42 provides suggested assurance levels for signing of operational data but requires understanding of the:

- value of the data
- risk data compromise
- consequence to the business of corruption, exposure or loss of data

Automating Paper-based Processes - considerations

1. Approving Civil Aviation Authority/Country: FAA/United States		2. AUTHORIZED RELEASE CERTIFICATE FAA Form 8130-1, AIRWORTHINESS APPROVAL TAG			3. Form Tracking Number: R1030314	
4. Organization Name and Address: Intro Corporation-5121 Industry Drive-Suite 104-Melbourne-FL-32940				5. Work Order/Contract/Invoice Number: 2014-XYZ		
6. Item:	7. Description:	8. Part Number:	9. Quantity:	10. Serial Number:	11. Status/Work:	
1	Connector	MTCPOKTI22PFX	1	N/A	FACTORY NEW	
12. Remarks: These parts are factory new and traceable to the Manufacturer TE Connectivity (Tyco/Raychem) Certificate of Conformance on file.						
13a. Certifies the item identified above were manufactured in accordance with: <input checked="" type="checkbox"/> Approved design data and are in a condition for installation. <input type="checkbox"/> Non-approved design data specified in Block 12.			14a. <input type="checkbox"/> 14 CFR 43.9 Return to Service <input type="checkbox"/> Other regulation specified in Block 12 Certifies that unless otherwise specified in Block 12, the work identified in Block 11 and described in Block 12 was accomplished in accordance with Title 14, Code of Federal Regulations, part 43 and in respect to that work, the items are approved for return to service.			
13b. Authorized Signature: Raymond Howell		13c. Approval/Authorization No.: DARFS11216CA	14b. Authorized Signature: Not Applicable		14c. Approval Certificate No.: Not Applicable	
13d. Name (Typed or Printed): Raymond Howell		13e. Date (dd/mm/yyyy): 3/04/2014	14d. Name (Typed or Printed): Not Applicable		14e. Date (dd/mm/yyyy): Not Applicable	
User/Installer Responsibilities						
It is important to understand that the existence of this document alone does not automatically constitute authority to install the aircraft engine/propeller/article. 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 his/her airworthiness authority accepts aircraft engine(s)/propeller(s)/article(s) from the airworthiness authority of the country specified in Block 1. Statements in Blocks 13a and 14a 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 8130-1 (02-14) NSN: 9812-00-012-9805						

Who signed this form?

What credentials were used to sign?

Were those credentials valid?

What do you know about that person?

Was that person authorized to sign?

When did they sign it?

Can someone outside my organization sign?

Can data coming from an outside source be validated?

Was there a problem with those credentials before or after it was signed?

Has it been altered since it was signed?

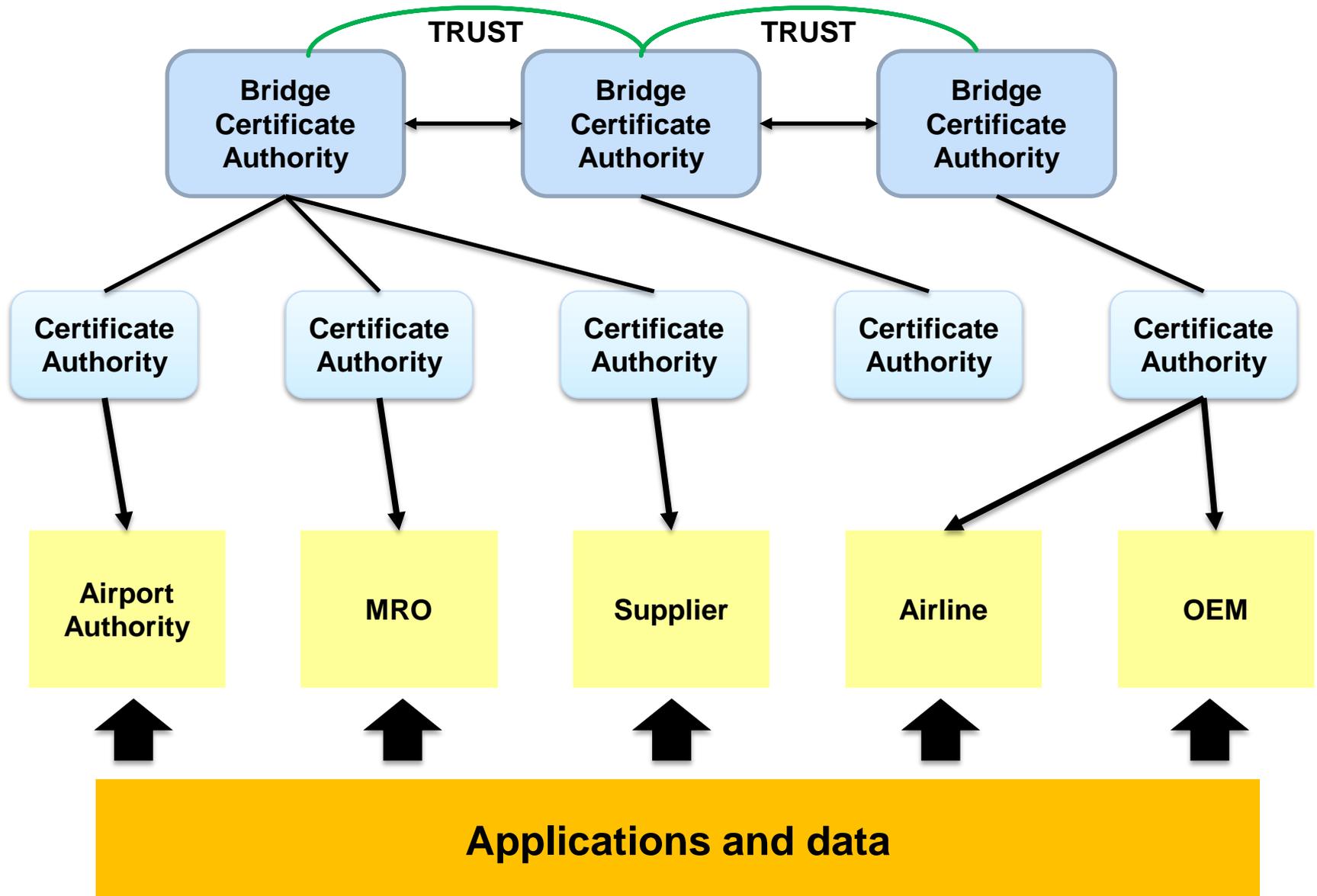
What are the consequences of...

How important is the integrity of the data?

Required Digital Solutions – Key Features

	Spec 42 Compliant PKI-Based Solution
Associate signer with credentials using an medium level of assurance	<input checked="" type="checkbox"/>
Credentials of signer valid and not compromised and known across companies	<input checked="" type="checkbox"/>
Transferable historical record of protected content and knowledge of who signed	<input checked="" type="checkbox"/>
Positively identify when record was generated using timestamp, as appropriate	<input checked="" type="checkbox"/>
Industry best practice of ensuring data integrity	<input checked="" type="checkbox"/>
Positively identify characteristics of and associate what was signed with signee.	<input checked="" type="checkbox"/>

Bridge Trust Model - Federation



Spec 42 – Guidance for use of Digital Security in Commercial Aviation

- Spec 42 provides guidance on common processes, tools and practices for **securely** transmitting, storing and exchanging commercial aviation data.
 - Considerations for protecting data from corruption or manipulation of while in state or during transmission between an airplane and system.
 - Methods of positively identify a person or device electronically using digital security
 - Guidance on continuous operations both from an airlines operator and system designer perspective.

Digital Security Working Group Activities - 2017

2017-1 Spec revision highlights:

- Updated guidance on time-stamping including signer certificate validation, and advanced time-stamp requests and responses
- Expanded guidance on maintenance of digital signatures including preferred format for archives
- Updated guidance for preservation of signed and archived documents
- New section on managing obsolescence of cryptographic algorithms
- New section on PKI compromise management
- New appendix on exchange of credential information between parties

Related Industry Standards - Recent Activity

- Spec2000 Chapter 17 – Maintenance Execution (2016) 
- ARINC Spec 842 (update) – companion document to Spec 42 (in work)
- ARINC 848 – Secure Broadband IP based Air Ground Interface (in work)
- ARINC 852 – Security Event Logging (2017) 
- ARINC 822-A Ground Wireless Communications (2016)
- NIST 800-152 US Federal Cryptographic Key Management (2015)
- NIST 800-172 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (2015)
- ETSI 319-401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016)
- Open Group – Protecting Information: Steps for a Secure Data Future (2014)

Summary

- The connected airplane has made it necessary to leverage Public Key Infrastructure to operate the airline business.
- This technology is already being widely used and will continue to be designed into a number of aspects of the airline and airplane infrastructure.
- Use of standards such as ATA Spec 42 is paramount and will help reduce risks of compromise associated with misguided deployments.
- Success requires the right tools, policies and practices to be followed – it's not just about the technology.
- To ensure the guidance in Spec 42 meets the industry's requirements, we also need your participation.

Questions ?

Contact: Regan Brossard - Boeing

206-276-7803 or

Regan.K.Brossard@Boeing.com