Overview of the Aircraft Security Process

Securing an Aircraft Information System

Bertrand LECONTE
8 January 2019

AIRBUS

- Aircraft technologies
- Security bricks
- Security measures
- Aircraft security principles

- **Aircraft technologies**
- Security bricks
- Security measures
- Aircraft security principles

A320 & A330 Avionics

- **Avionics**: Aviation Electronics
  - Set of controls, sensors, computers, actuators

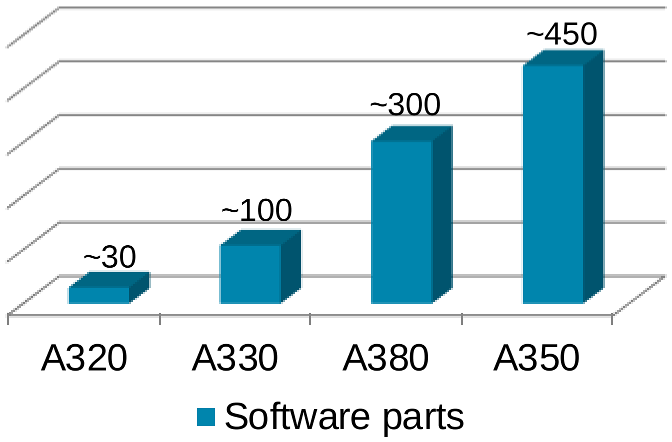
- 25+ ATA chapters
- Systems are mainly **independent**
- ARINC 429 bus
  - **Unidirectional**, point to multi-point
  - 32bit at a time: 8bit label and 19bit data
    - Single value per label: speed, altitude…
  - Quite low speed: 100Kbps

Some ATA chapters			
21	Air conditioning	**32**	Landing gear
22	Auto flight	**34**	Navigation
23	Communications	**42**	Integrated Modular Avionics
24	Electrical power	**44**	Cabin systems
27	Flight controls	**45**	Maintenance system
28	Fuel	**46**	Information systems

ARINC (in this context) – Standardization body

A380 & A350 Avionics

- Avionics Full DupleX – AFDX
  - Deterministic Ethernet
  - Based on **Virtual Links**
    - Unidirectional, point to multi-point
  - Switches are enforcing Virtual Links
  - Bi-directional communication needs two VL
- Integrated Modular Avionics
  - ARINC 653 API
  - Space and Time partitioning
  - Incremental certification
- Open World



VL – Virtual Links
API – Application Programmable Interface

AIRBUS

Security considerations

Security by obscurity **does not work**

- Confidentiality of specifications & designs is very hard to manage
- Think **insider attacks**
  - Wikileak
  - Edward Snowden…
- Think **leaks**
  - Shadow Brokers…

- **Reverse engineering**
  - It works well
  - It is not so hard
  - It is not necessarily expensive

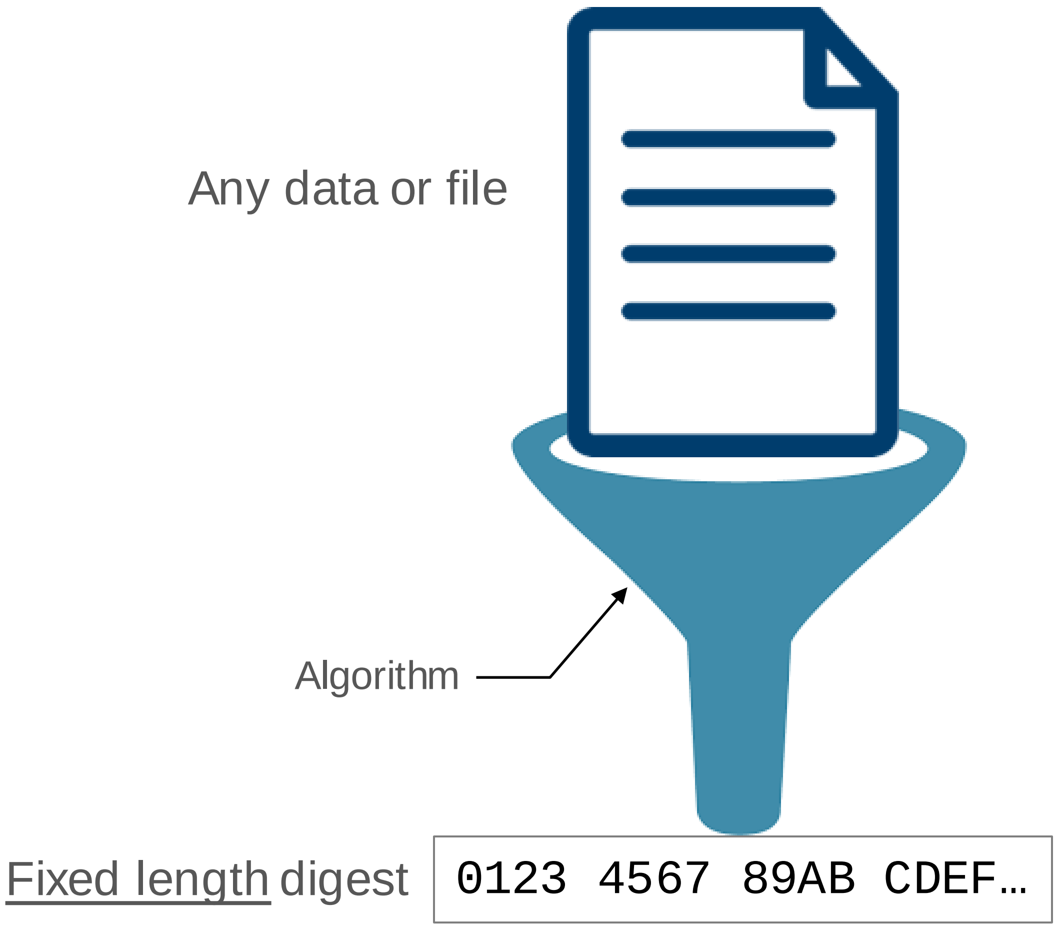
- Aircraft technologies
- **Security bricks**
- Security measures
- Aircraft security principles

Cryptography
Hash algorithms

- Transform any file (or byte flow) to a unique fixed length value
  - SHA-1: 160 bit
  - SHA-2 256: 256 bit

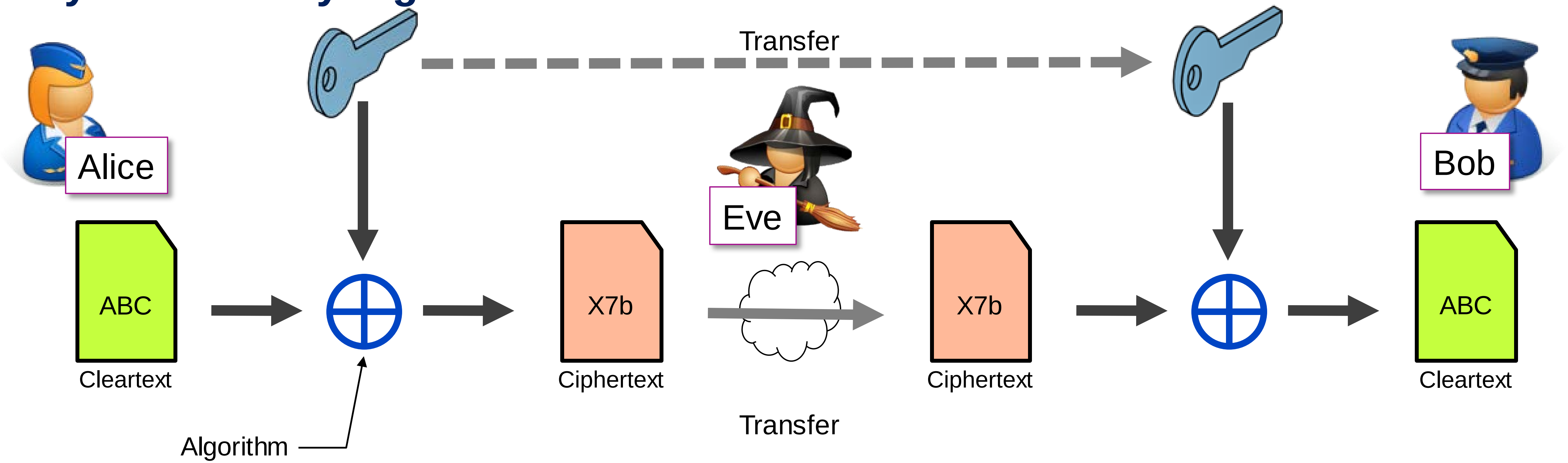
- Properties
  - **One way** function: function which is infeasible to invert (except by brute force)
  - **Small change** to message should change digest a lot
  - Infeasible to find two different messages with **same digest**
  - **Deterministic**: same message always results same digest
  - **Quick** to compute

- Workhorse of cryptography



Cryptography

Symmetric-key algorithms

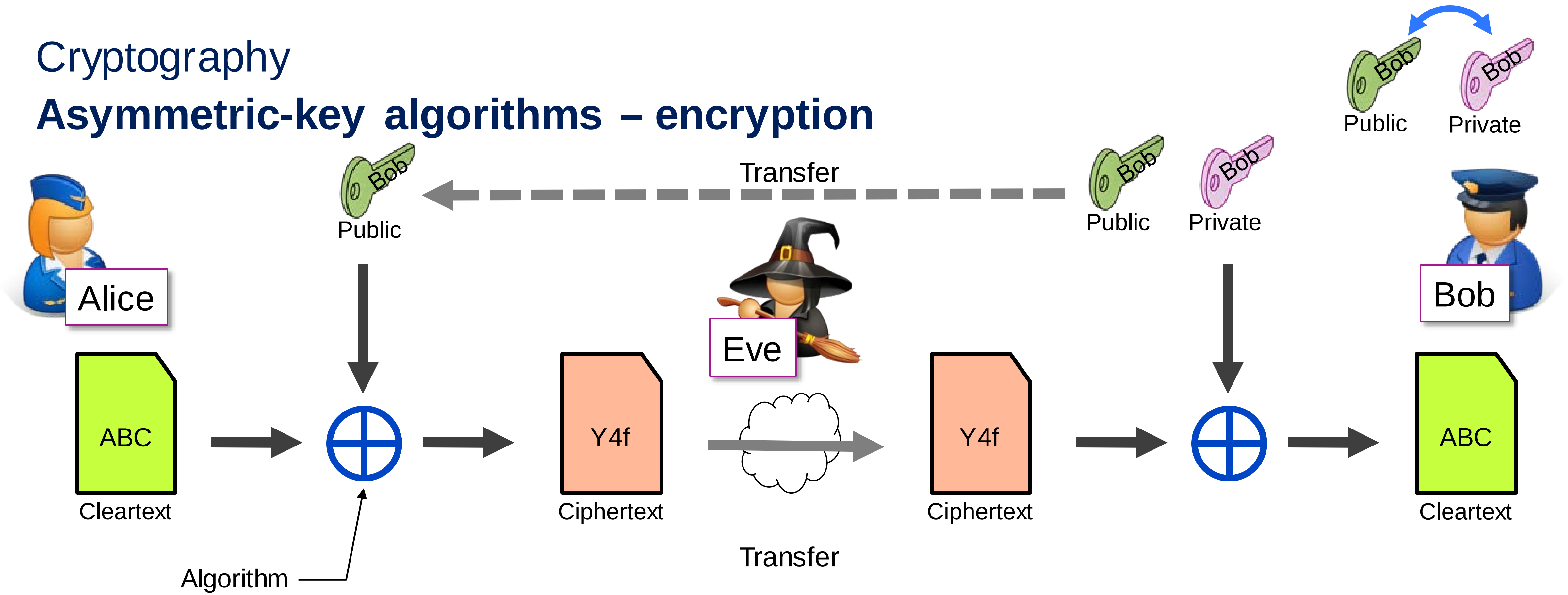


- Used for **encryption** – confidentiality protection
- Algorithm examples: DES, 3DES, **AES**
- **Fast** algorithms, can be implemented in hardware
- Ciphertext is undistinguishable from **random text**

- Key length should be at least 128bit, preferably 256bit
- Exportation, importation, usage are **locally regulated**
- Message is only **as secure as the key**
- **Key distribution** is the issue

Cryptography

Asymmetric-key algorithms – encryption

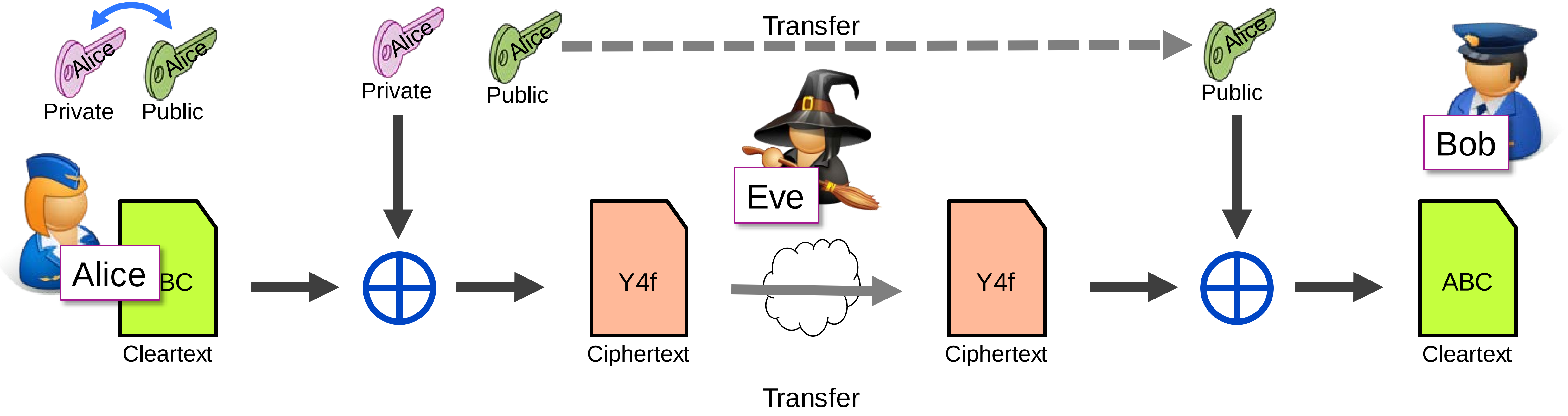


- Public key and private key are related
- It's not possible to find private key from public key
- What is encrypted with **public** key is decrypted only by **private** key
- What is encrypted with **private** key is decrypted only by **public** key

- Message is only as secure as the **private key**
- Ciphertext is undistinguishable from random text
- Algorithm examples: RSA, Elliptic Curves

Cryptography

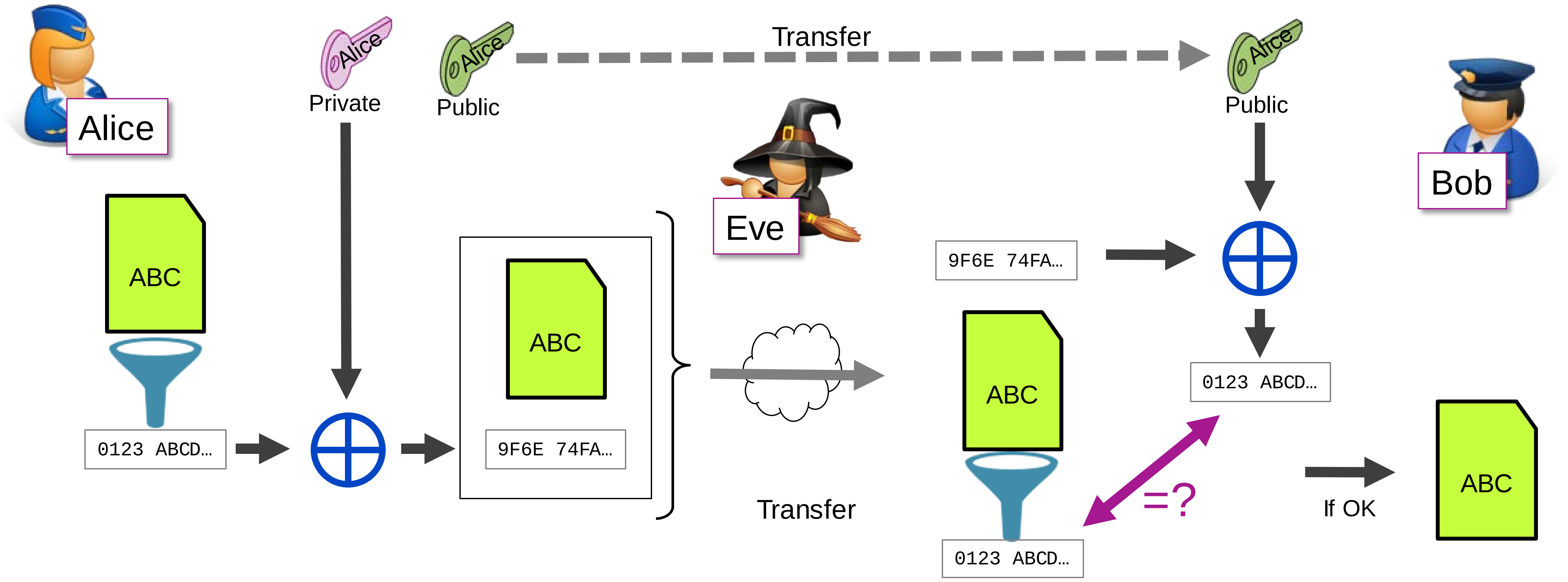
Asymmetric-key algorithms – proof of origin



- Asymmetric-key algorithm are used for **many functions**
  - Encryption
  - Authentication
  - Integrity
- Exportation, importation, and usage are **locally regulated**
- How to distribute keys?
- Asymmetric algorithm are **slow**

Cryptography

Asymmetric-key algorithms – digital signature

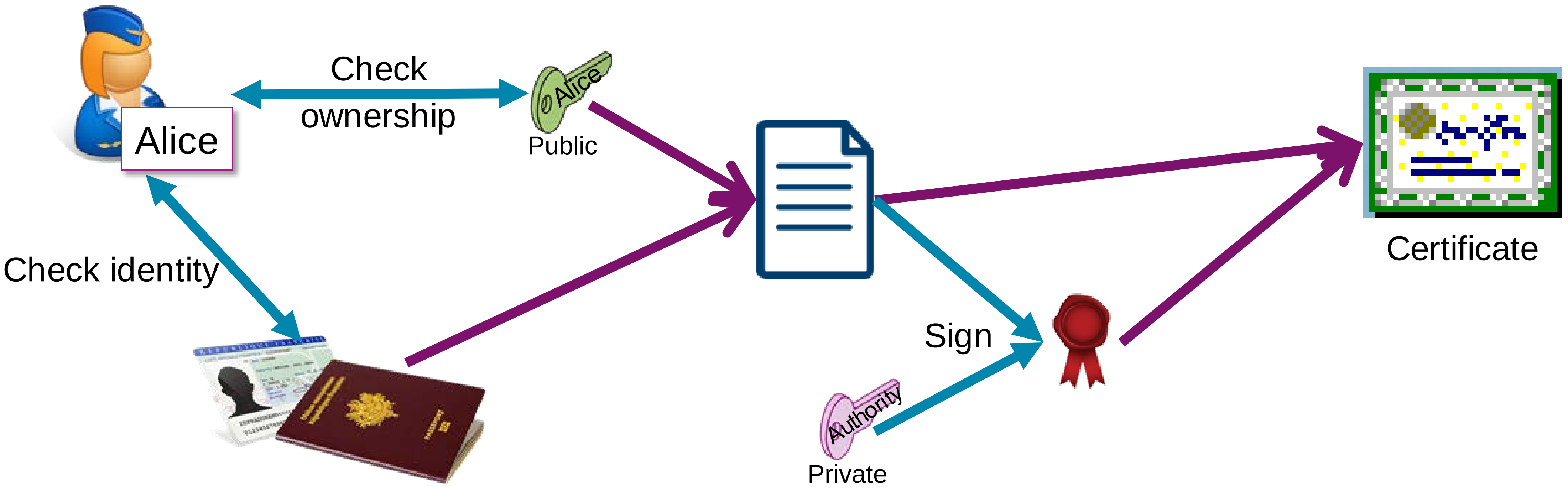


Asymmetric-key distribution

Certificates and Public Key Infrastructure

Problem: how to get confidence in a **given public key**, how to link it to the **real world user identity**?

Solution: have an authority certifying this



- Aircraft technologies
- Security bricks
- **Security measures**
- Aircraft security principles

AIRBUS

Which security measures could be used to protect aircraft information systems?

Firewall

Function or device aimed at

- Looking at network packets
- **Deciding** if they can go on or have to be dropped

For IP communications

- Usually looks at level 3 and level 4 (IP addresses and TCP/UDP ports)

How to express the filtering policy?

- Not an easy job…
- Basic rule: **drop everything**, allow only what you need
- What can do an attacker of what you let go through?
  - No protection for what is allowed
  - Target is exposed without protection…

The firewall is not the protection, the enforced filtering policy is

AIRBUS

Application level gateway

Firewalls are filtering at layers 3 and 4

- **IP addresses**, ports (≈ identification of applications), not looking at payload

Application level gateway aims at **filtering upper layers**

- It must **understand** protocols, **filter** application and protocol values
- Whatever accepted transmission must be **innocuous** for receiving application

Advantages

- Good security level, high confidence in security
- **The real application is protected**

Consequences

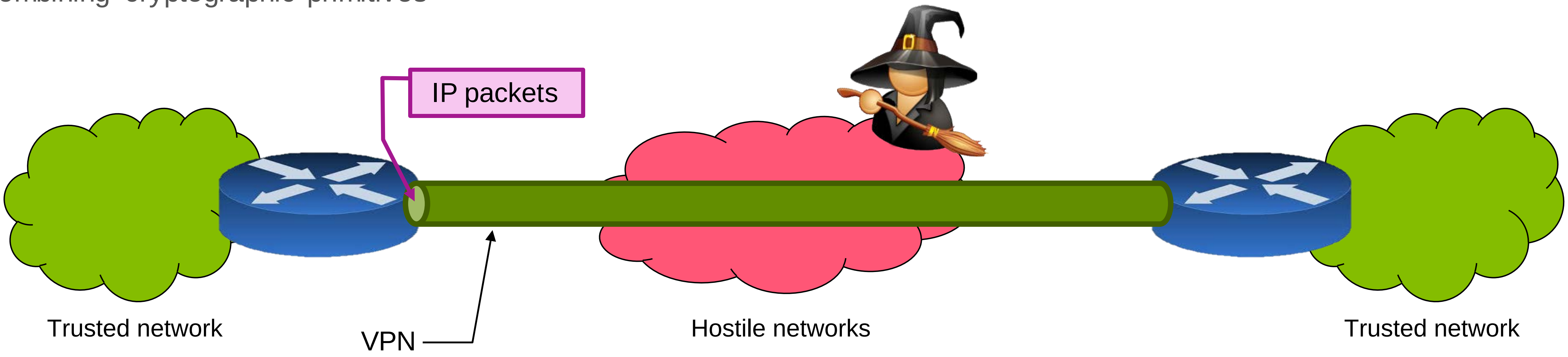
- Costly to develop as **specific** to every application and protocol

AIRBUS

Virtual Private Network

Objective: communicate through an **untrusted network** as if you were on dedicated **private lines**

- Build communication channel with security properties (integrity, authenticity, confidentiality)
- Combining cryptographic primitives



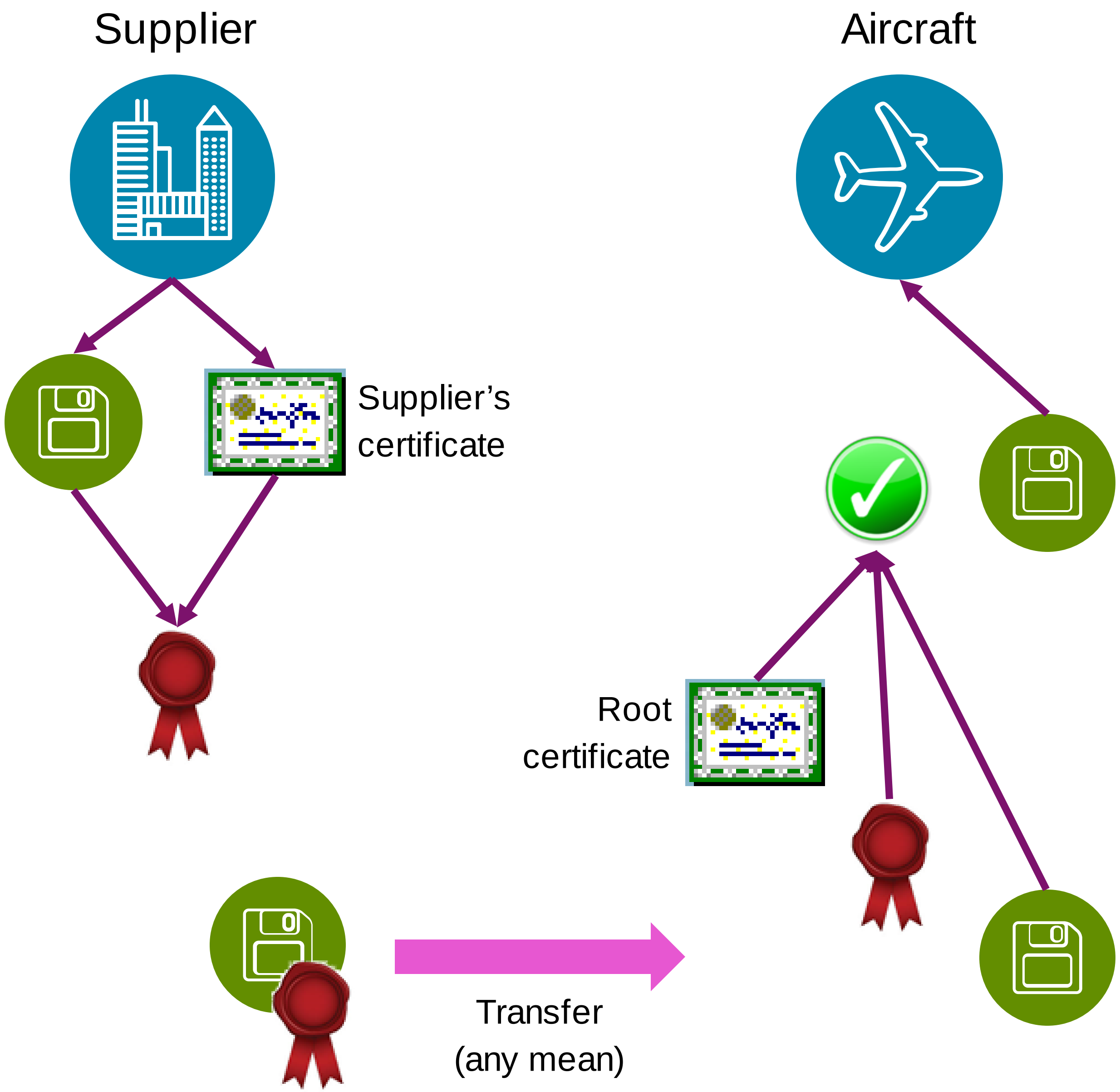
- Brings you confidence someone **external to the communication** will not read, modify or inject packets
- Does not protect you if attacker is **at the other side**…

AIRBUS

Aircraft Protection Principles

Digital signature of software

- Field Loadable Software (FLS)
  - *Field:* not in supplier's premises, can be done on aircraft
  - *Loadable:* can be changed or updated without specific tooling, without opening the box
  - *Software:* Executables, configuration and customization files, databases
- Need to ensure
  - **Origin**: FLS had been produced by an authorized supplier
  - **Integrity**: FLS had not been modified since production by the supplier



Basic principles

Asymmetry

- An **attacker** only has to find **one vulnerability** to exploit in order to start an attack, whereas a **defender** must guard against an attack on **any and every** service

Security in depth

- Perfect protection is not possible
- Objective is to slow down the attackers
- Discourage them by raising the technical problem

Global vision

- Security studies need a global vision of architecture and systems
- It's the only way to **prevent bypass**

Limit **attack surface**

Do not imagine what attackers want to do, they will be more creative!

- Aircraft technologies
- Security bricks
- Security measures
- **Aircraft security principles**

AIRBUS

Environment and assumptions

Environment identifies **threat source** profile to be considered

- **Trust** environment has to be defined
- Without any trust, nothing is possible, impossible to protect from everything and everyone

Airline people are by default **trusted**

- Flight crews
- Cabin crews
- Maintainers

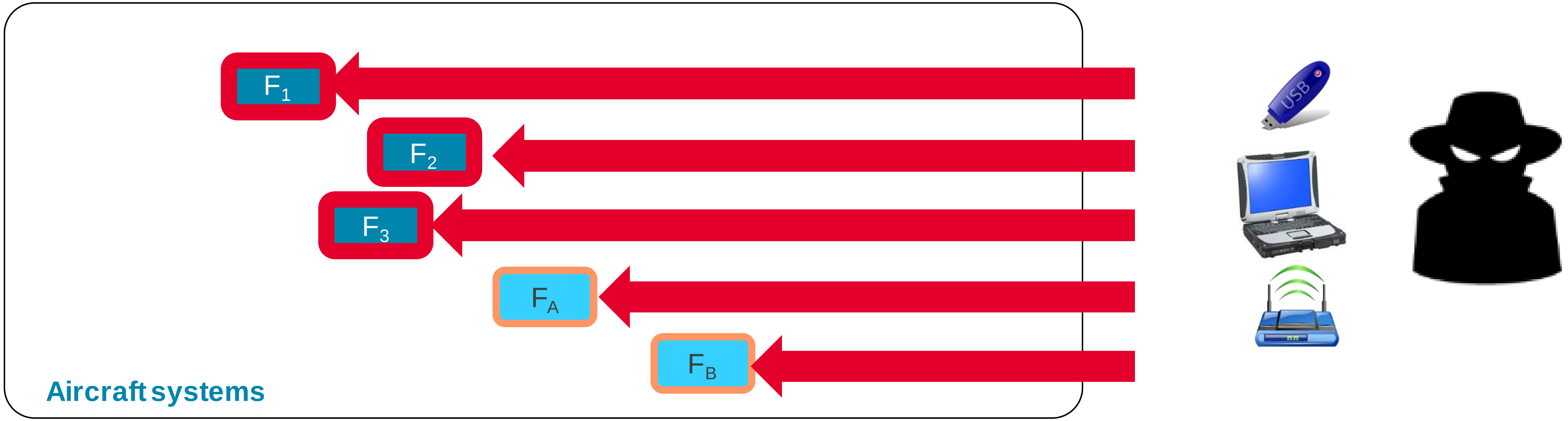
Nevertheless, by default the e-tools they use are **not trusted**

- Laptops, PCs (EFB, PMAT), tablets…
- USB sticks, SD cards…

Communications are by default **not trusted**

EFB – Electronic Fight Bag
PMAT – Portable Maintenance Access Terminal

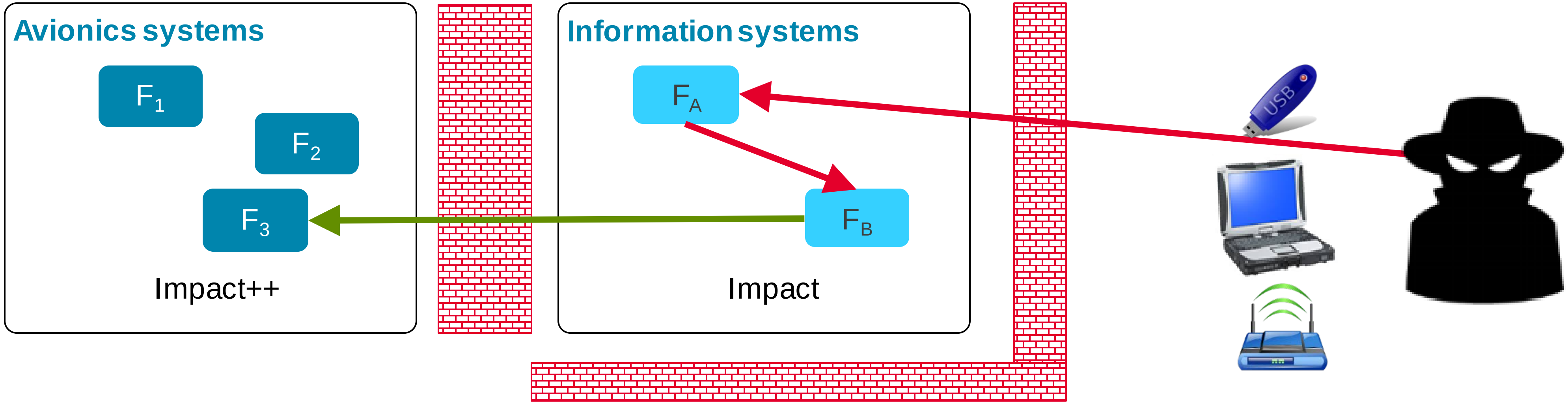
Function protection



- Functions **will be** attacked
  - Many entry points
- Functions are needed for **aircraft safety** and **operations**
  - Security is needed to ensure those functions will be available
- First reflex: **every function is to be protected**
  - Strength of protection depends on impact

AIRBUS

Domain protection

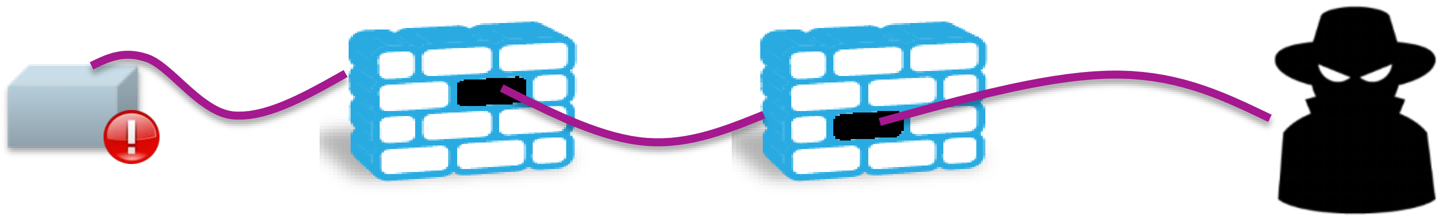


- Reduce cost by creating domains and **mutualizing** security barriers
  - **Layered** protection for most impacting functions
- Every security barrier is sufficient to face considered threat attack path
- Layered protection gives time to correct vulnerabilities
  - If no layered protection → disconnected the system after first vulnerability

- Drawback: rebound attacks
  - Highest impact in the domain has to be taken into account

Aircraft Protection Principles
Layered defense

- Aircraft security architecture must be based upon **layered protection** concept



- Security boundary count is defined by aircraft safety impact of protected asset
  – *Strong* and *Very strong* safety impact requires at least **two barriers** between threat agents and impacted assets

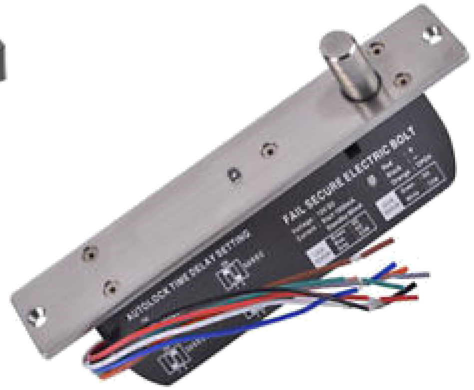
- Security boundaries must be **designed** and **demonstrated** to have **no common vulnerabilities**
  – A single vulnerability must not endanger aircraft security
    - Different technologies: code, system architecture
    - Different COTS
    - Hardware based solution vs software based solution
- At least one security barrier

AIRBUS

Aircraft Protection Principles
Additional properties

- No bypass

- Fail secure
  - If a failure happens, stay secure!
  - Fail Secure vs Fail Safe



AIRBUS

Aircraft Protection Principles
Work Impact

- It's possible to protect something with
  - Technical measures
    - *Example:* firewall, VPN, physical device…
  - **Organisational measures**
    - Procedure, process
    - *Example:* ask maintainer to do a antivirus check on his USB stick before connecting it to the aircraft

- **Technical measures** must be privileged at all times
  - This avoid human errors or omissions
  - This reduce burden for users

Threats to counter
Food for thought for protection

- What can be done with what you functionally allow
  - If you can ask nicely to perform a bad action, why bother doing something else?
- Attacks can be on infrastructure and software too
  - Buffer overflow attacks and others…
- Denial of Services
  - Resource exhaustion
  - Flooding
- Attacks on communication means
  - Spoofing
  - Man in the Middle
  - Jamming
- Degraded & backup modes
  - They are simpler and not necessarily protected

- Monitoring & administration systems
  - They access all systems
  - They are a central point of attack
  - They could allow easy remote control
  - Front face plugs can be a threat too
- Data loading
  - If the attacker can change the software used, why protect…?
  - It's a central point of attack

AIRBUS

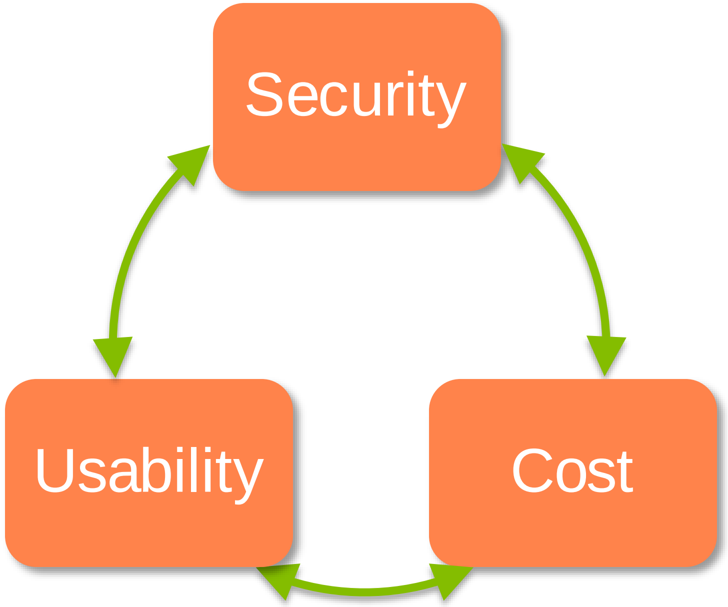
Trade-offs & decisions

Technical feasibility, cost, weight & volume, performance

- Cyber Security **effectiveness**
- Capacity to **demonstrate** to Airworthiness Authorities
- **Industrial constraints**
- **Evolution possibilities** (build modular architecture, use bricks)
- **Infrastructure capacity** to host the security measure

- There is more than one solution!

- Challenge proposed solution with regard to original objective
- Risk management
  - Risk acceptance



General IT security *vs* Aircraft Security
Where are the particular difficulties?

- No on-board security administrator
  - Monitoring cannot be done in real time by humans
- Cycles are different
  - Update cycles cannot be the same
  - Development time are longer
  - Configuration Management is requested by operations and imposes additional work
  - Systems are designed for the lifetime of an aircraft – 25 to 50 years
- Diversity & multiplicity of interconnected systems
  - E.g. ATM systems are different from one country to another during the same flight
- Certification
  - Certification process is long and costly
  - Need to convince Authorities
- Taking into account existing architectures
- Consequences are usually bigger
  - Safety
  - Liability
- Communications
  - Cost
  - Roaming
  - Intermittence

ATM – Air Traffic Management

AIRBUS

Security engineering

- Requirement Based Engineering
- Writing security specification is a nightmare
  - This is not enough!

➔ Need for other activities

Thank you

AIRBUS