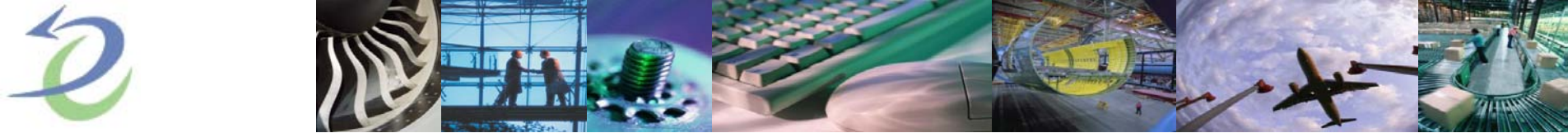


■ Developing your corporate PKI Strategy

- Gil Mulin, Airbus
- Julien Holstein, Aerospace Vision on behalf of Airbus



Prologue

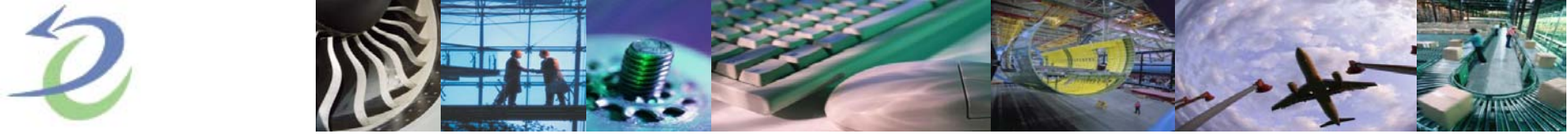
With cyber security as one of the top priorities of the President, the federal government has initiated a significant overhaul of its information security standards, guidance, and risk management activities.

The National Institute of Standards and Technology (NIST) in partnership with the Department of Defense and the Intelligence Community, is developing a unified information security and risk management framework for federal agencies and their support contractors including those organizations in the A&D industries.

Many state and local governments as well as private sector entities are adopting the security standards and guidelines on a voluntary basis.

Applying information security best practices and effectively managing risk associated with the operation and use of information systems will help ensure that the operations, assets, and individuals within the United States critical infrastructure are well protected against an increasingly sophisticated and dangerous set of cyber threats.

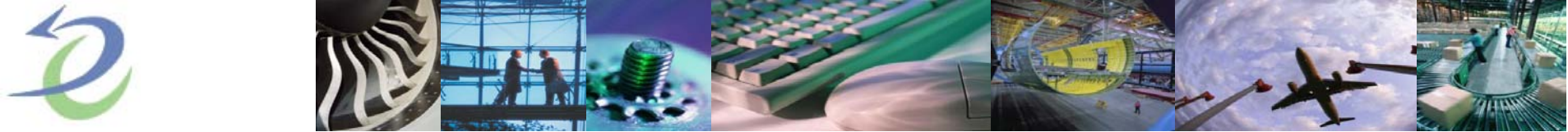
Dr. Ronald Ross, Project Lead for FISMA Implementation Project, National Institute of Standards and Technology (NIST)



Agenda

- 1 Introduction**
- 2 A reminder**
- 3 Companies' needs**
- 4 Possible implementations**
- 5 Conclusion**





1 - Introduction

→ Information security is a key topic in the industry

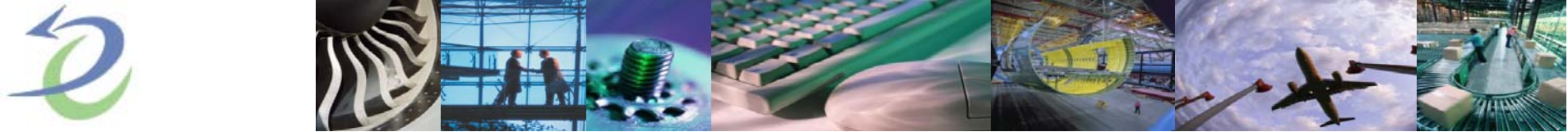
- Deals with confidentiality, integrity (and non repudiation) and availability of data
- Data digital security is widely handled with digital certificates

→ Aeronautical actors have to implement information security all over their activities

- In domains where aircrafts are impacted
- In all their other domains (finance, strategy, HR, technical design...)

→ DSWG sets the standard concerning the usage of digital certificates around the aircrafts

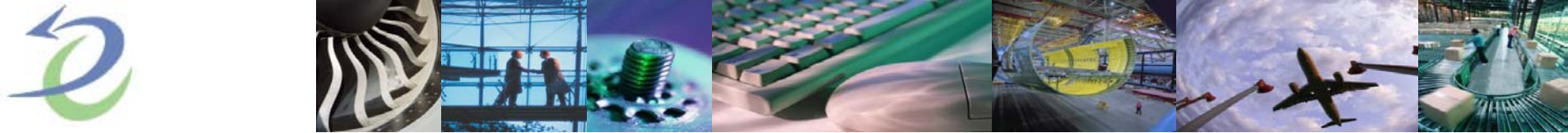
- Impact various contributors (manufacturers, system providers, airlines, airports...)
- Defines processes and technical requirements around digital certificates in order to provide a good level of trust



Agenda

- 1 Introduction
- 2 Reminders
- 3 Companies' needs
- 4 Possible implementation
- 5 Conclusion





2 - Reminders

→ What are digital certificates ?

→ Digital certificates are the digital keys which allow to encrypt data (protect the confidentiality) and to digitally sign data (provide assurance on integrity, identity and non repudiation). They are provided by Certificates Authorities (CA)

Mr Blue signs a document with his certificate



And send it to Mr Green




Mr Blue encrypt a document for Mr green



And send it to Mr Green




Mr Green recognizes Mr Blue signature



This provides assurance on :

- The identity of the sender
- The integrity of the data since it has been signed
- The fact the message has been sent (non repudiation)

Mr Green decrypt the document with his certificate



This provides assurance on :

- The confidentiality of the data

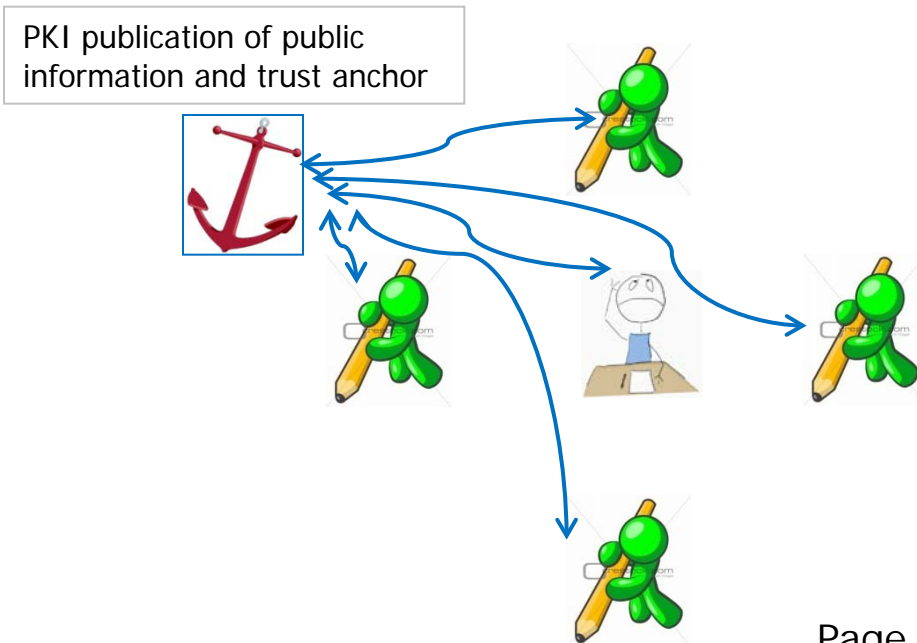
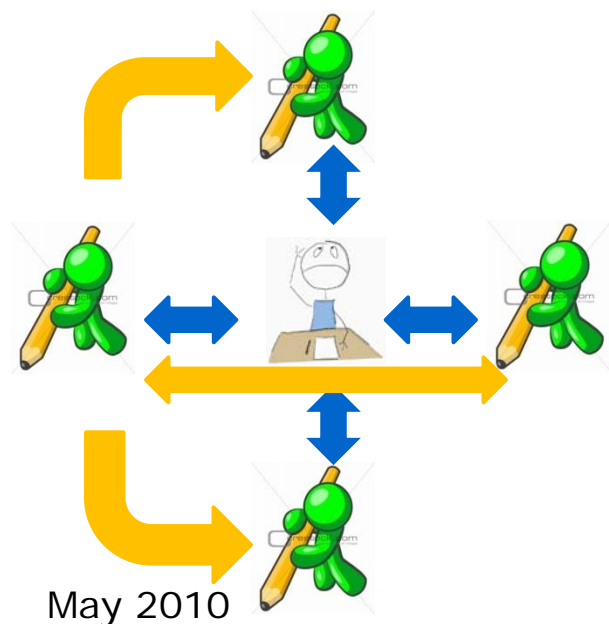


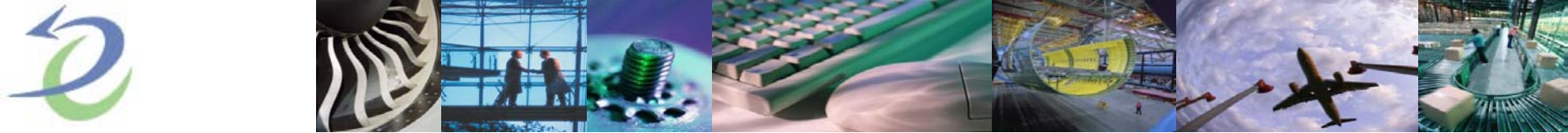
2 - Reminders

→ What is a Public Key Infrastructure (PKI) ?

→ A PKI is the addition of physical Information System means (servers, specialized software,...) and processes in order to manage digital certificates lifecycle (certificates generation, revocation, renewal, user registration, revocation lists managements, public information publication, trust anchor...)

→ It is important to notice that a PKI is split in 20% of technology and 80% of processes and management

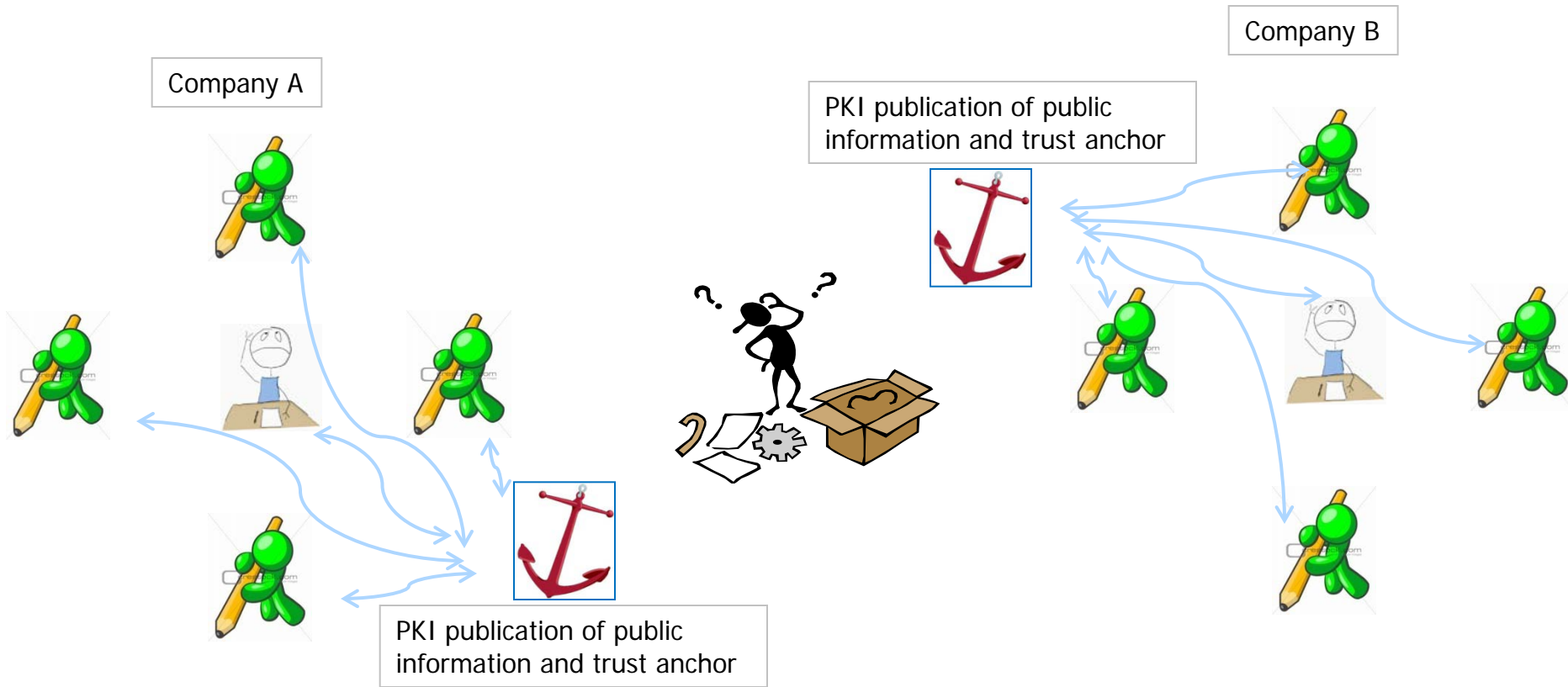


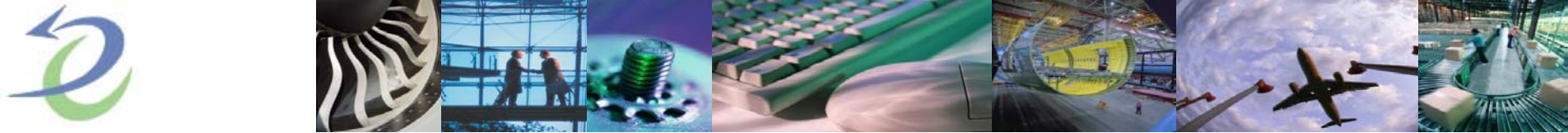


2 - Reminders

→ What is a cross certification bridge ?

→ A cross certification bridge is a set of rules PKI can fulfill to enlarge their circle of trust. All the PKI cross certified toward the same bridge trust and are trusted by all the others

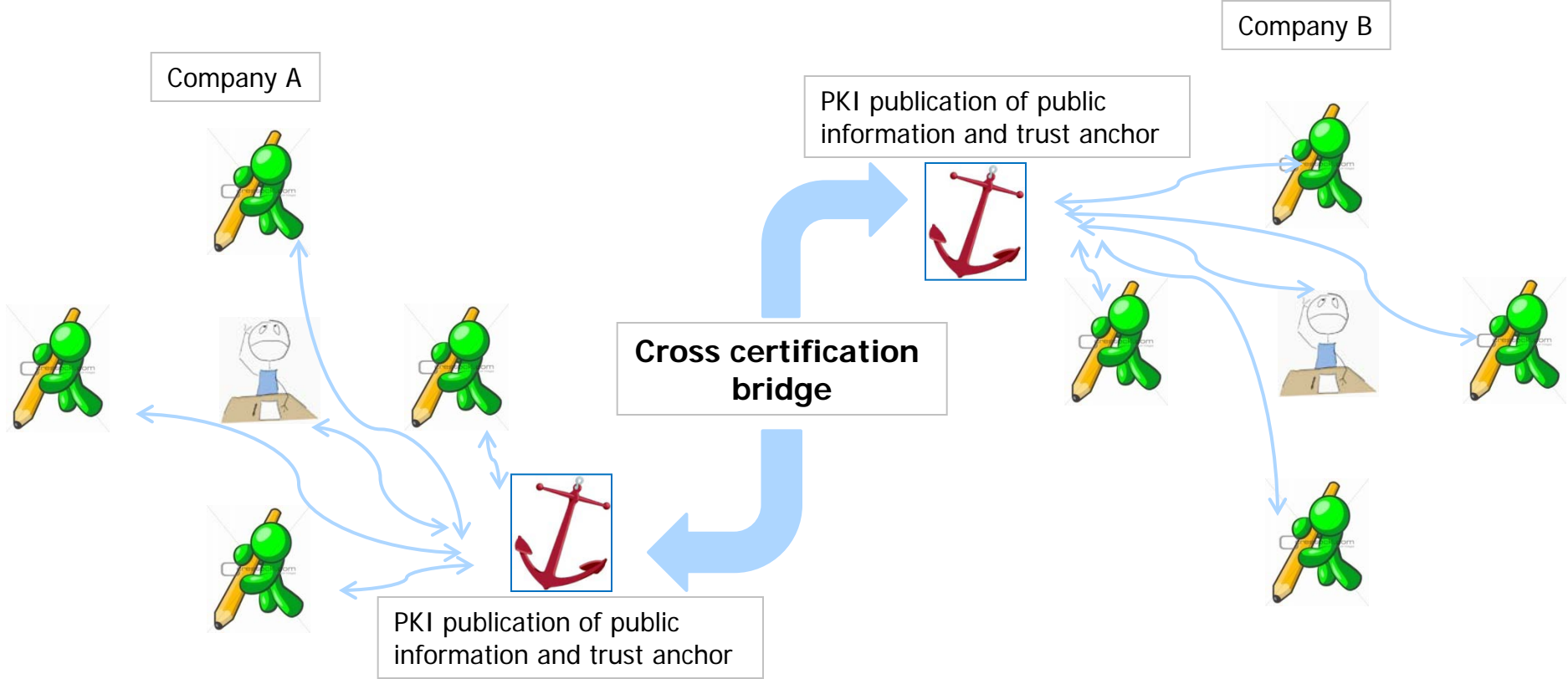




2 - Reminders

→ What is a cross certification bridge ?

→ A cross certification bridge is a set of rules PKI can fulfill to enlarge their circle of trust. All the PKI cross certified toward the same bridge trust and are trusted by all the others





2 - Reminders

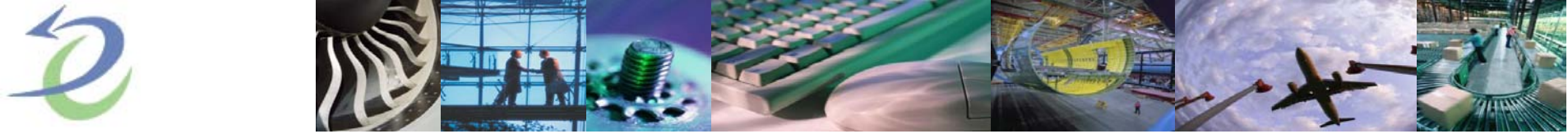
→ What is a cross certification bridge ?

→ A cross certification bridge is a set of rules PKI can fulfill to enlarge their circle of trust. All the PKI cross certified toward the same bridge trust and are trusted by all the others

→ A cross certification bridge requires a Trust anchor. A Trust anchor is the foundation upon which the trust chain rests. A trust anchor is an unequivocal authority, usually governmental.

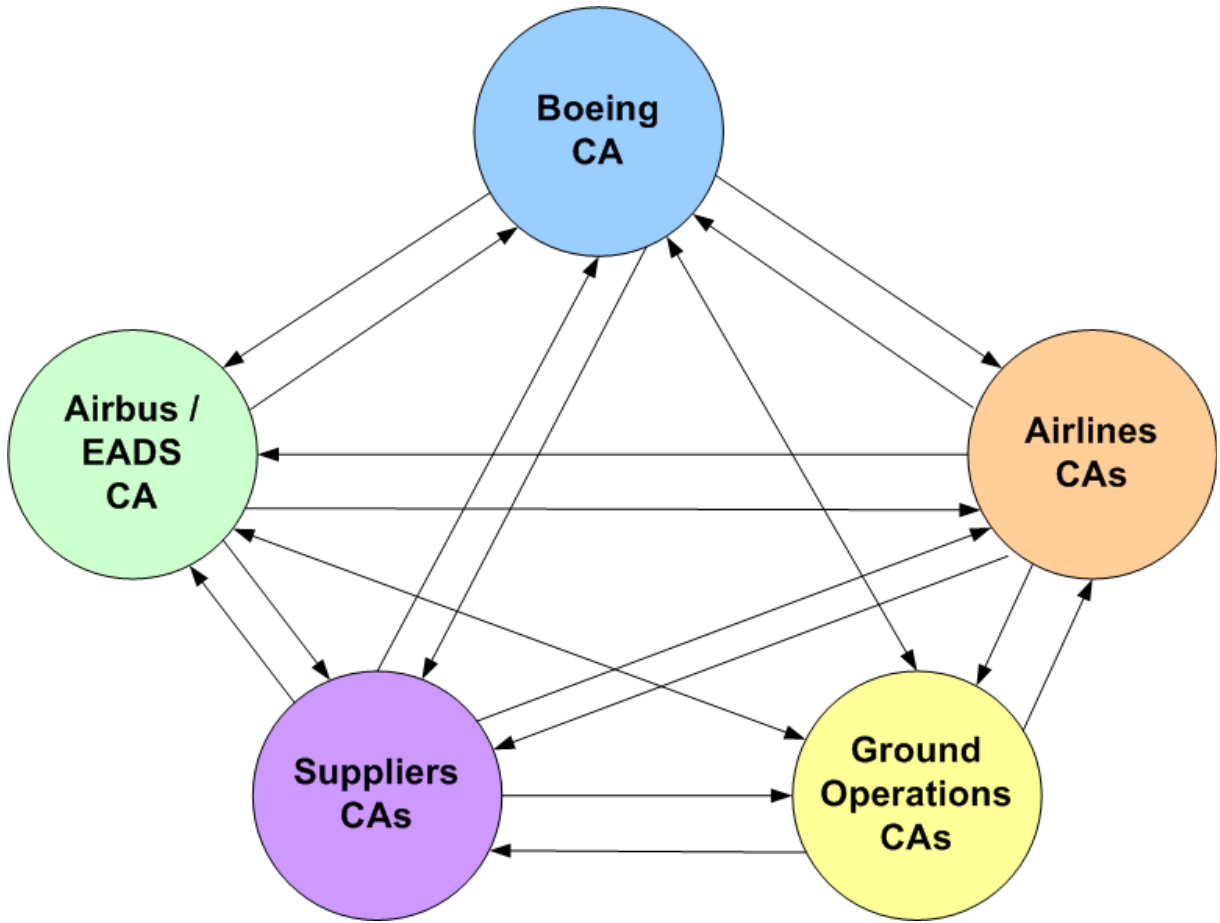
→ For example , in the case of Certipath (jointly owned by ARINC,SITA and Exostar) the trust anchor is the U.S Federal PKI Authority.

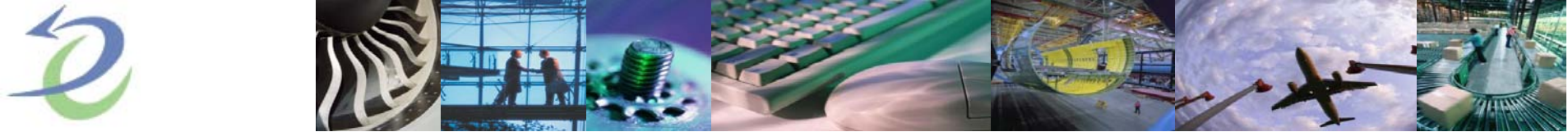
→ The trust anchor determines the criteria for cross-certification as well as the governance regime.



2 - Reminders

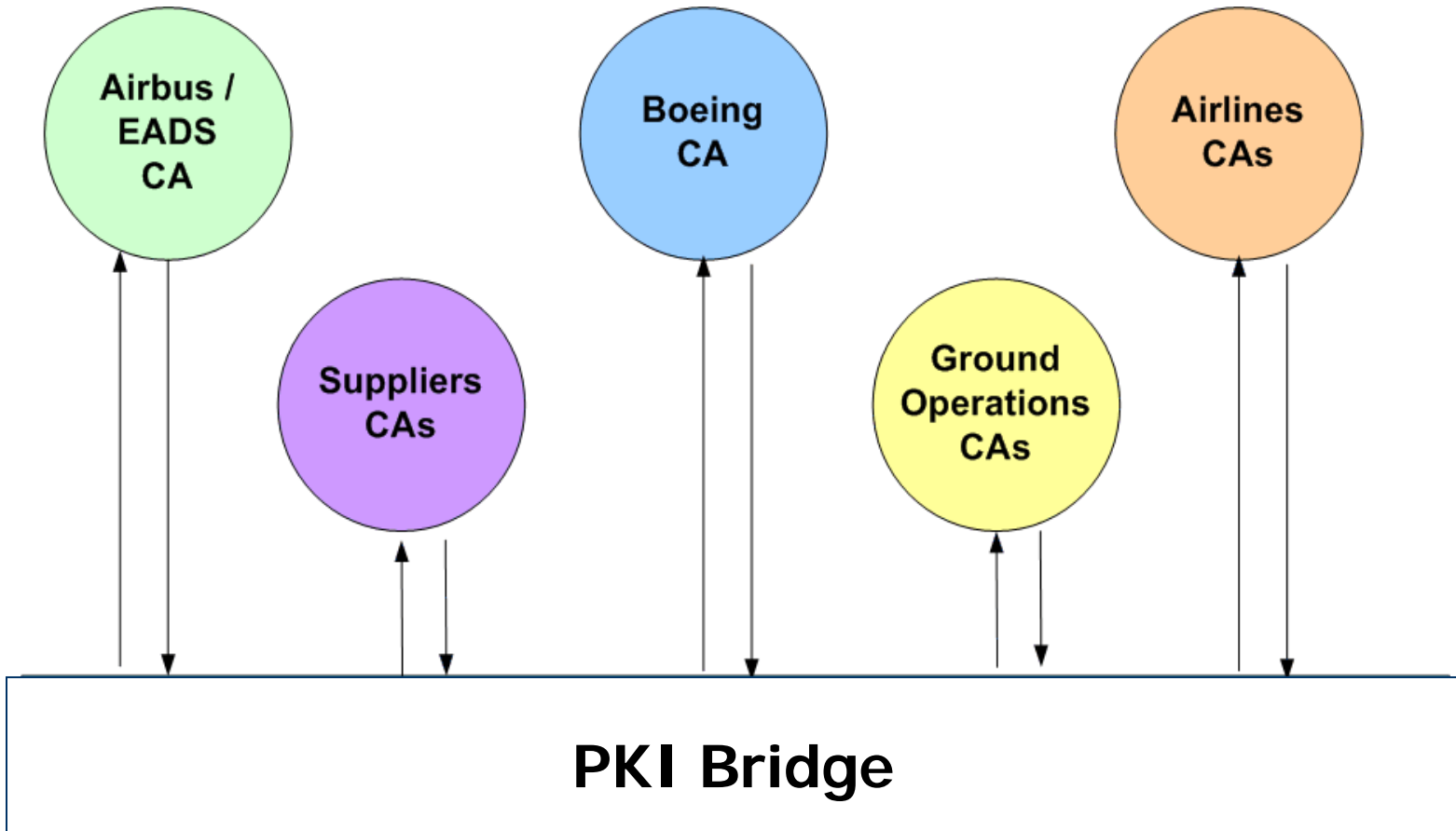
→ What collaboration WITHOUT a cross certification bridge looks like

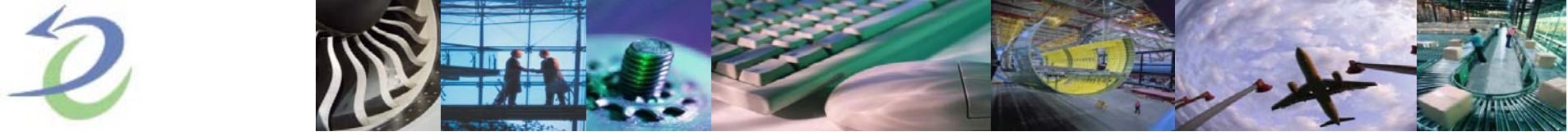




2 - Reminders

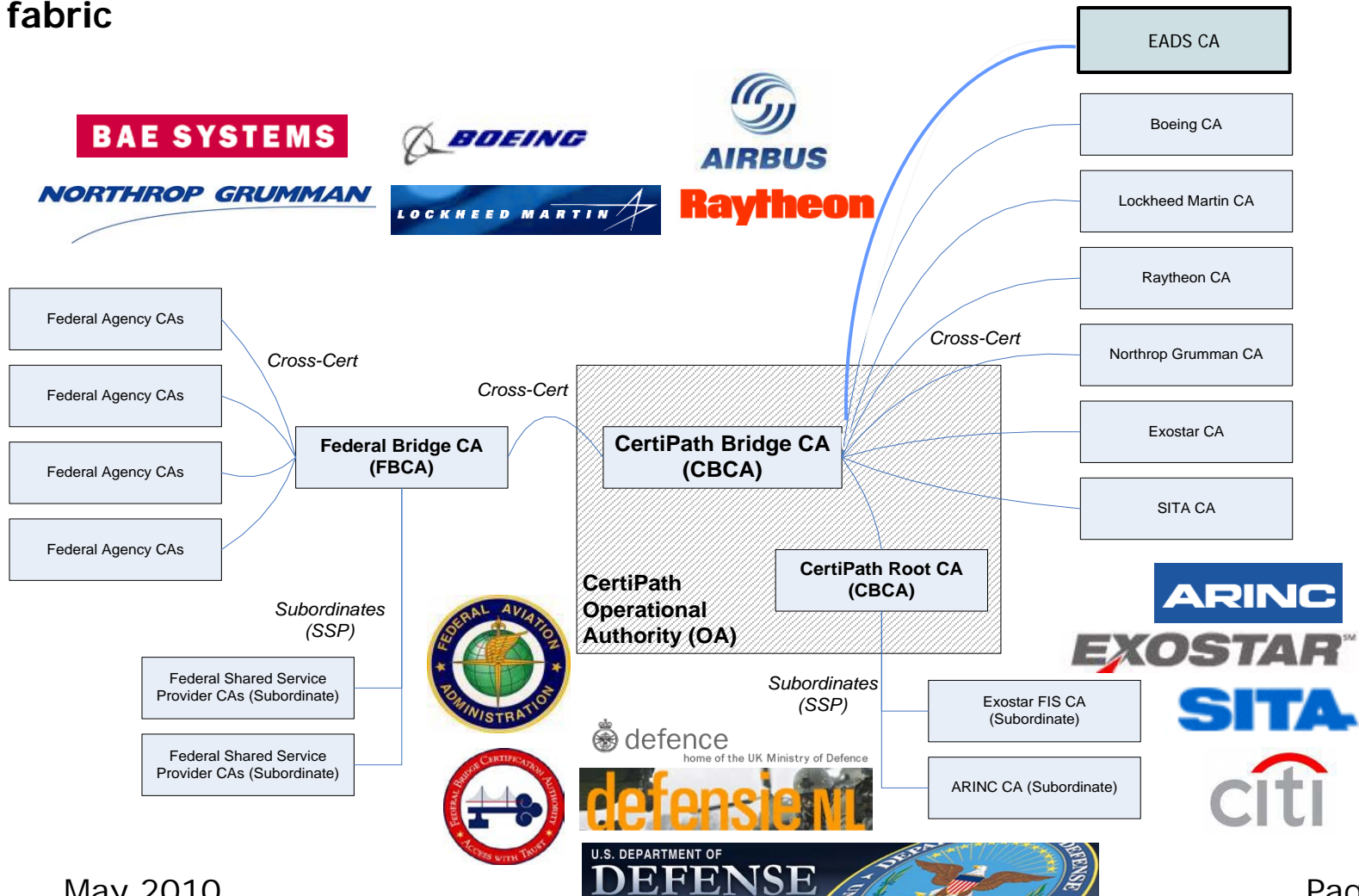
→ What collaboration WITH a cross certification bridge looks like

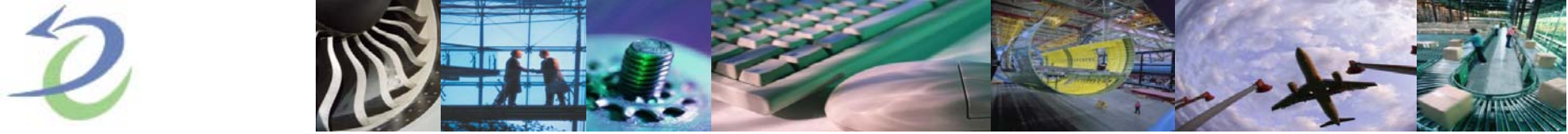




2 - Reminders

→ Trust fabric

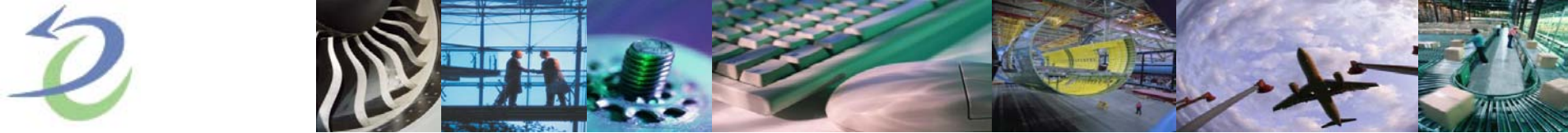




Agenda

- 1 Introduction
- 2 Reminders
- 3 **Companies' needs**
- 4 Possible implementation
- 5 Conclusion





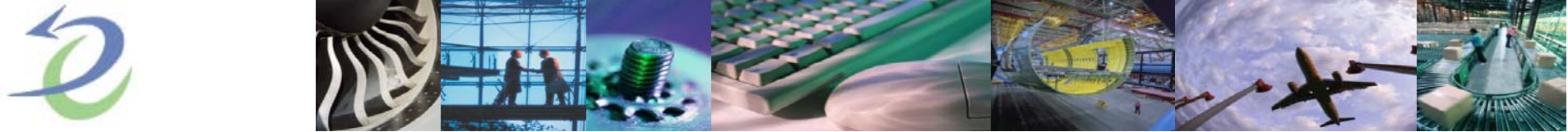
3 – Companies' needs

→ **Aeronautical functional needs**

- Loadable software parts code signing
- FAA form 8130-3 and EASA form1 digital signature
- XML crate digital signature
- ACARS messages encryption

→ **Industrial "ground" functional needs**

- Encryption of sensitive data (files, e-mails, laptops hard drive)
- Digital signature of files and e-mails
- "Qualified" digital signature
- Strong authentication



3 – Companies' needs

→ Interoperability

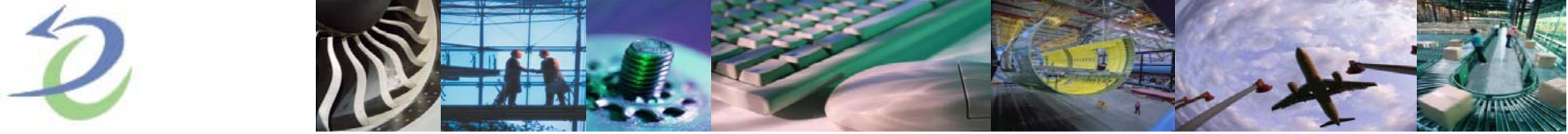
- Maybe I will have to digitally sign a piece of software which will be loaded in an aircraft? (DSWG guidelines)
- Maybe I will have to digitally sign some official documents (DSWG-spec 2000 guidelines)?
- Maybe I will have to implement an "Extended Enterprise" business model which is going to require identity federation? (the foundation of which should rely on PKI)

→ Practical Operations

- Minimal variation
- Fit within existing responsibilities
- Predictable
- Re-usable

→ Economy

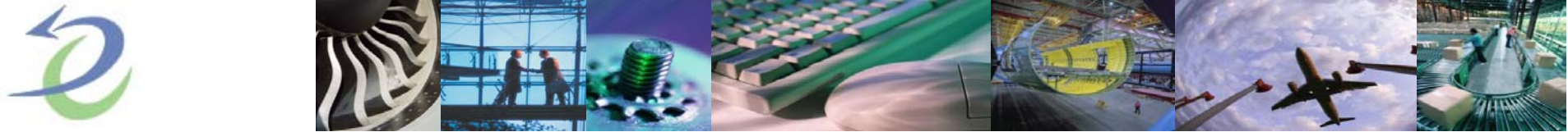
- Minimum new investment as operations evolve



Agenda

- 1 Introduction
- 2 Reminders
- 3 Companies' needs
- 4 **Possible implementation**
- 5 Conclusion





4 - Possible implementation

→ What are your choices in terms of use?

→ To consolidate on as few digital certificates as possible, all issued from a single PKI or to use different digital certificates for each activity, possibly issued by different PKI

→ What are your choices in terms of implementation?

→ You can choose to buy your certificates

→ Why would you choose to buy your certificates?

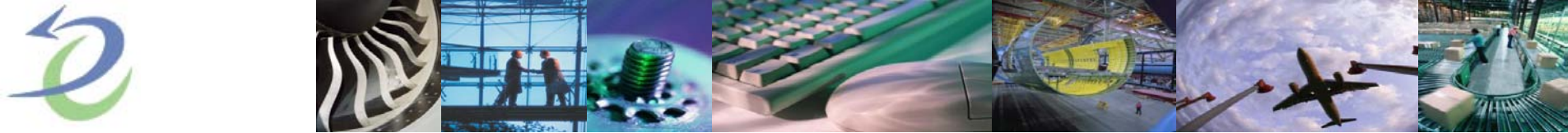
→ You have a choice of providers

→ You can choose to implement your own PKI

→ You will need external expertise to provide specialist knowledge

→ Why would you choose to implement your own PKI?

→ Why would you want to have certificates that are cross-certified?



4 - Possible implementation

→What are your drivers?

→Cost (implementing your own PKI is very expensive)

→Economies of scale

→Availability of resources

→Management focus

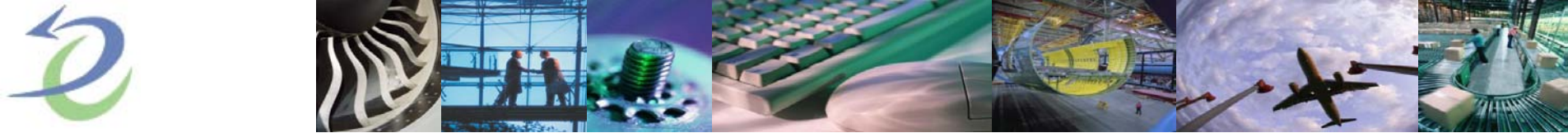
→Strategy : do you want to wait for regulation to enforce you or do you want to or to anticipate the best you can?

→Why would you wait for regulation? Why would you anticipate?

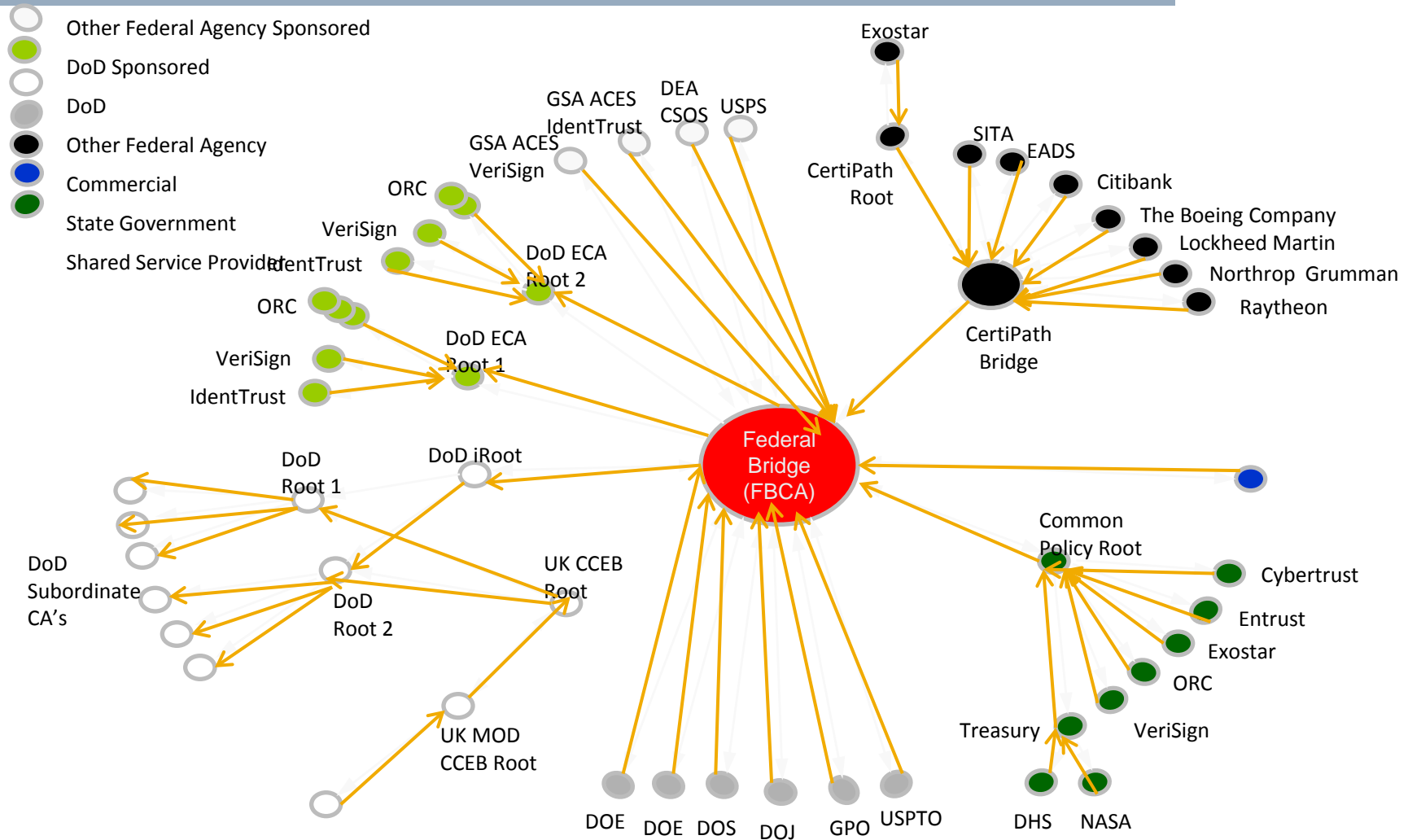
→In either case (make or buy)

→it is fundamental that the company has processes in place that provide a unique identity for each employee together with the respective vetting actions which the law of the country allows. (for example is should be based on FIPS 201 /HSPD 12 in the US)

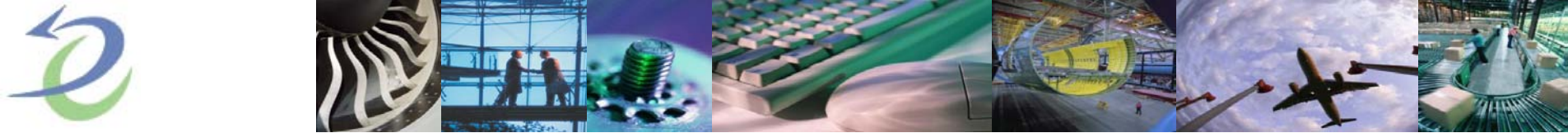
→There are certain roles that have to be created e.g. the Registration Authorities. These RAs register the future subscriber. There are also the Trusted Agents. They are responsible for issuing the certificates and therefore for ensuring the binding of the identity of the subscriber to the certificate itself



4 - Possible implementation



May 2010



Epilogue

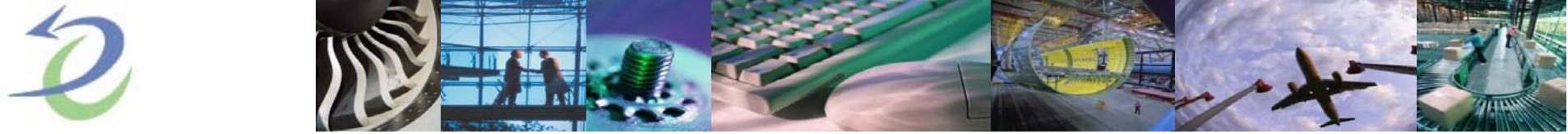
With cyber security as one of the top priorities of the President, the federal government has initiated a significant overhaul of its information security standards, guidance, and risk management activities.

The National Institute of Standards and Technology (NIST) in partnership with the Department of Defense and the Intelligence Community, is developing a unified information security and risk management framework for federal agencies and their support contractors including those organizations in the A&D industries.

Many state and local governments as well as private sector entities are adopting the security standards and guidelines on a voluntary basis.

Applying information security best practices and effectively managing risk associated with the operation and use of information systems will help ensure that the operations, assets, and individuals within the United States critical infrastructure are well protected against an increasingly sophisticated and dangerous set of cyber threats.

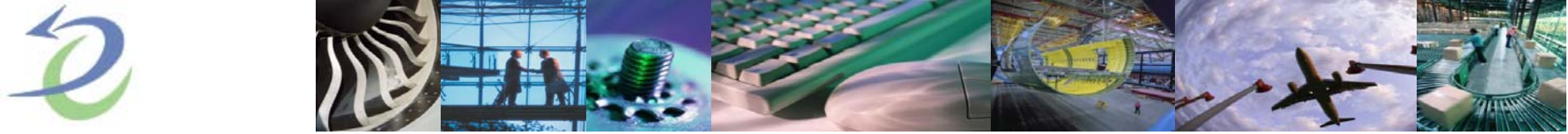
Dr. Ronald Ross, Project Lead for FISMA Implementation Project, National Institute of Standards and Technology (NIST)



Agenda

- 1 Introduction
- 2 Reminders
- 3 Companies' needs
- 4 Possible implementation
- 5 **Conclusion**

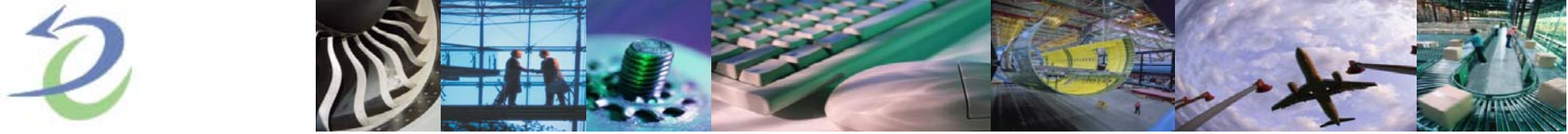




5 - Conclusion

- What do I need to implement?
- Should I make or should I buy?

- In order to help you in front of those two questions, we advise you have a clear vision on your immediate and midterm needs through several axis :
 - Identity and non repudiation, integrity and confidentiality needs
 - Regulated needs versus “free” corporate needs
 - Pure internal needs versus shared needs with partners/customers/suppliers
 - Strategy of my company towards the Extended Enterprise model
 - The **interoperability** you expect between all these needs
 - The agility you expect your solution to have



5 - Conclusion

Any questions?

→ **Gil Mulin, Airbus**

gil.mulin@airbus.com

→ **Julien Holstein, Aerospace Vision on behalf of Airbus**

julien.holstein@aerospace-vision.com