

What is an interoperable Public Key Infrastructure ?



Presentation Objectives

- 1 Review current work conducted by ATA DSWG on interoperability
- 2 Discuss two airline business use cases where PKI Interoperability is essential

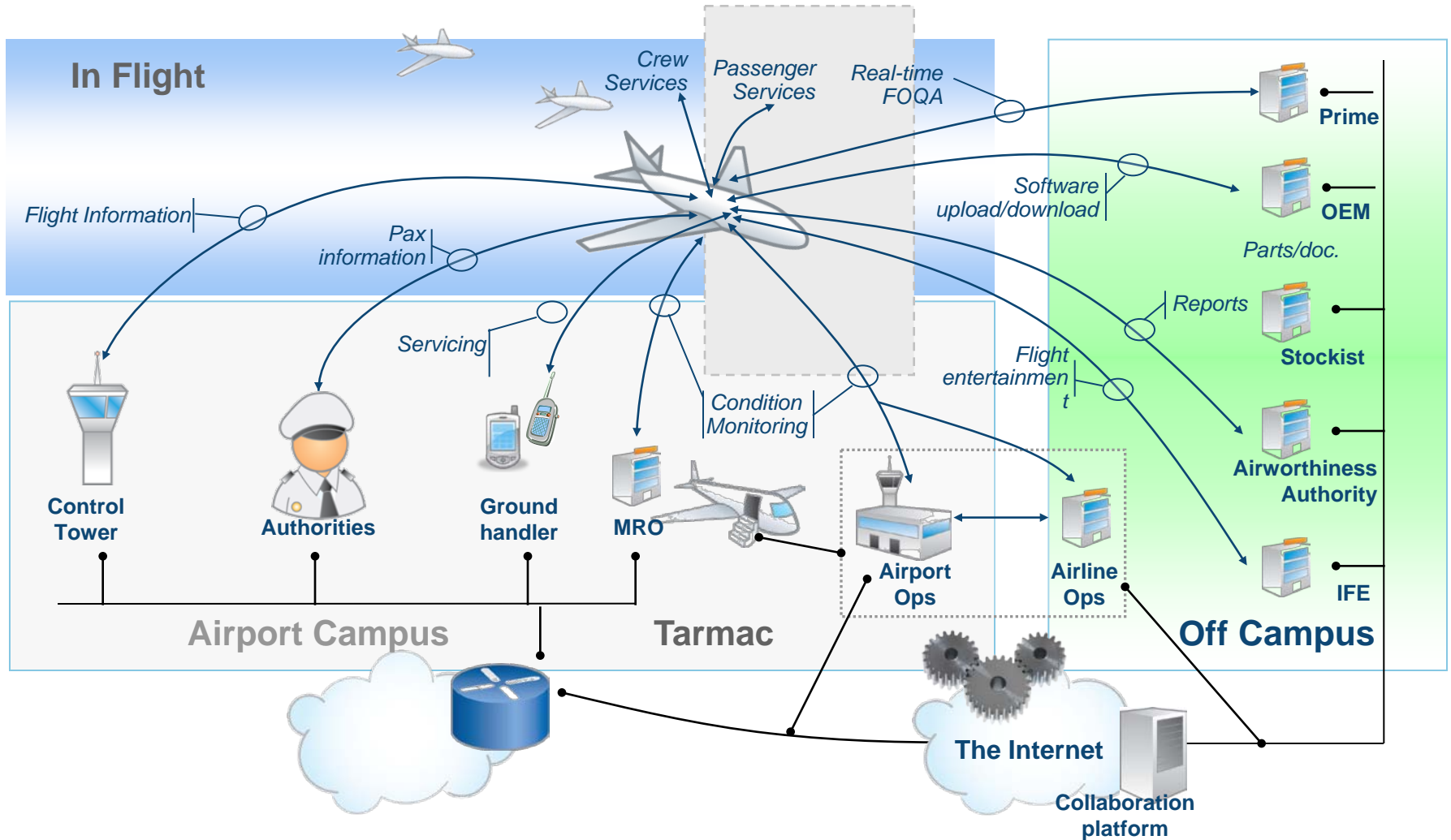
Agenda

- 1 Some definitions and history
- 2 Still facing PKI Interoperability issues, here some examples
- 3 Trust Model for the Industry
- 4 Migration from SHA-1 to SHA-2
- 5 Digital Signature Interoperability

Agenda

- 1 Some definitions and history
- 2 Still facing PKI Interoperability issues, here some examples
- 3 Trust Model for the Industry
- 4 Migration from SHA-1 to SHA-2
- 5 Digital Signature Interoperability

Increased usage of digital certificates within the ATI



Let's start with a definition of 'interoperability'

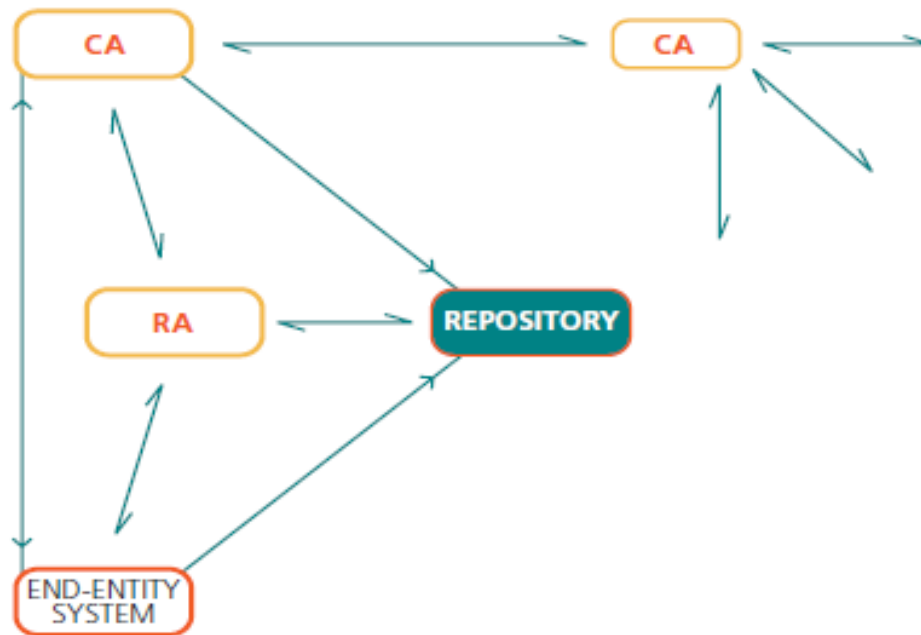
PKI Interoperability



The capability of a PKI component or system – whose interfaces are fully disclosed – to interact and function with other products or systems, without any access or implementation restrictions

PKI Interoperability Framework

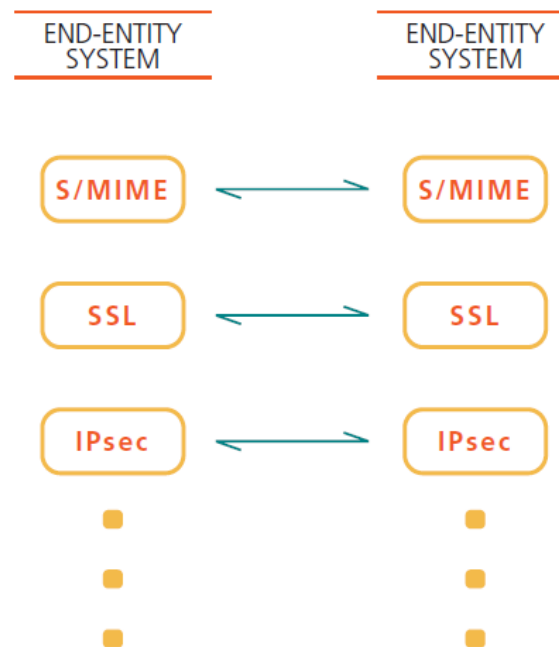
- Introduced by Tim Polk of NIST at 1st PKI Forum in 2000
- Three major interoperability areas identified :
 - Component-level Interoperability



Source: PKI Forum

PKI Interoperability Framework

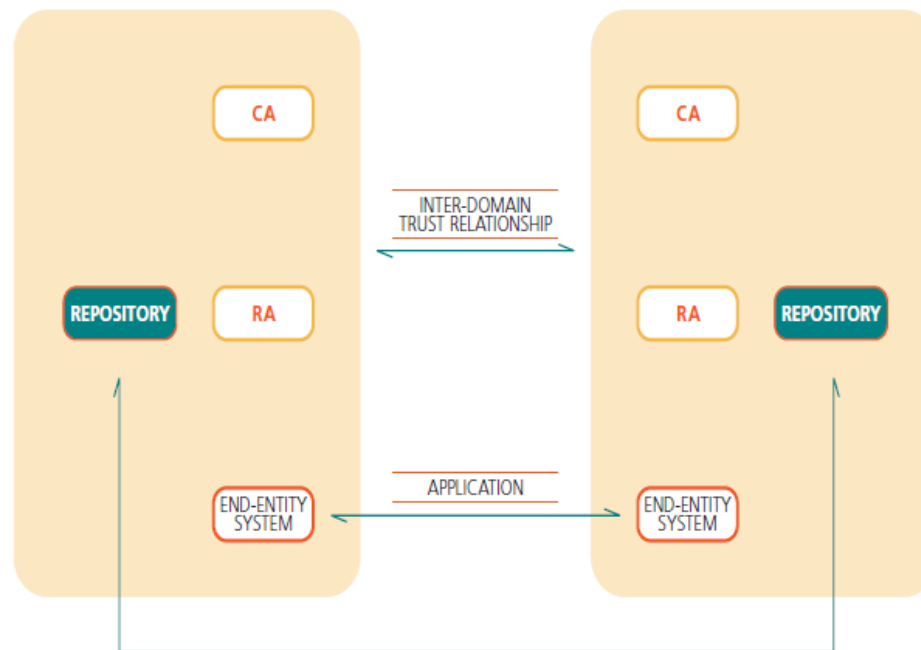
- Introduced by Tim Polk of NIST at 1st PKI Forum in 2000
- Three major interoperability areas identified :
 - Application-level Interoperability



Source: PKI Forum

PKI Interoperability Framework

- Introduced by Tim Polk of NIST at 1st PKI Forum in 2000
- Three major interoperability areas identified :
 - Inter-domain Interoperability



Source: PKI Forum

Significant progress achieved with PKI Interoperability since 1976

- Several PKI interoperability projects conducted in various regions of the world in early 2000. As a result, several recommendations were issued and implemented
 - Example: pki-challenge @ www.eema.org
- Several Air Transport Industry standards help achieve a greater chance for interoperability
 - ATA Spec. 42 ‘Aviation Industry Standards for Digital Information Security’
 - Defining a reference certificate policy for the ATI
 - AEEC, Doc. 822, Aircraft / Ground IP Communication, Doc. 822
 - Defining digital certificate profile for Gatelink
 - ATA Spec. 2000 ‘Electronic Product and Part Regulatory Documentation’
 - Defining structure for XML digital signature

Agenda

- 1 Some definitions and history
- 2 **Still facing PKI Interoperability issues, here some examples**
- 3 Trust Model for the Industry
- 4 Migration from SHA-1 to SHA-2
- 5 Digital Signature Interoperability

Certificate Management Integration

- Problem Encountered
 - Various applications (firewalls, Radius servers, PDAs, web servers) have different approaches (integrated or not) often supported by poorly-written documentation on the PKI topic
 - Lack of support for revocation checking, trust fabric resolution, path discovery, policy/name constraints, etc.
- Fix Applied
 - Knowledge of classical tools (openSSL, Keyman, Keytool..)
 - Use of plug-ins (Pathfinder, Entrust, Webcullis, etc.) to enhance capabilities of existing products, to choose products that do support these PKI-related functions, to require correct implementation of RFC5280 to vendors and specification writers
- How ATA Spec 42 recommendations help avoid such issue
 - Section 3.2.2. ‘Key Generation for Devices that Cannot Generate Their Own Keys’

Certificate Lifecycle Management for Devices

- Problem Encountered
 - How is the device supporting digital certificate renewal ?
 - How is the device acting as the relying party handling revocation ?
 - Can the device check for certificate status using regular OCSP (or alternatively SCVP or CRL) ?
 - Can the device access the CA environment directly for digital certificate validation ?
 - Issue is that device often cannot reach the asserting party CA environment
- Fix Applied
 - Internal replication of CA directory on a server reachable by the end entity
 - Leverage IETF-based protocols such as Simple Certificate Enrollment Protocol (SCEP), Certificate Management Protocol (CMP), and XML Key Management Specification (XKMS) for renewal and re-key
- How ATA Spec 42 recommendations help avoid such issue
 - Section 2.3.1.4 'Certificate Lifecycle Operational Requirements'
 - Section 3.6.2.3 'Revocation Status'

Digital Certificate Validation

- Problem Encountered
 - Security policies often not in place by Corporate IT preventing end-users to add root certificates in their browser store, such as Microsoft Update location
 - Some devices, such as authentication servers, often cannot support multiple root certificates, or multi-level CAs?
 - Can application / device support bridge model and perform certificate path discovery and validation ?
- Fix Applied
 - IT security policies to address PKI issues
 - Interoperability testing is required prior to massive deployments
 - PKI-enable applications to include PDVAL tools
- How ATA Spec 42 recommendations help avoid such issue
 - Section 3.8 'Trust Anchor Management'

Digital Certificate Enrollment Process

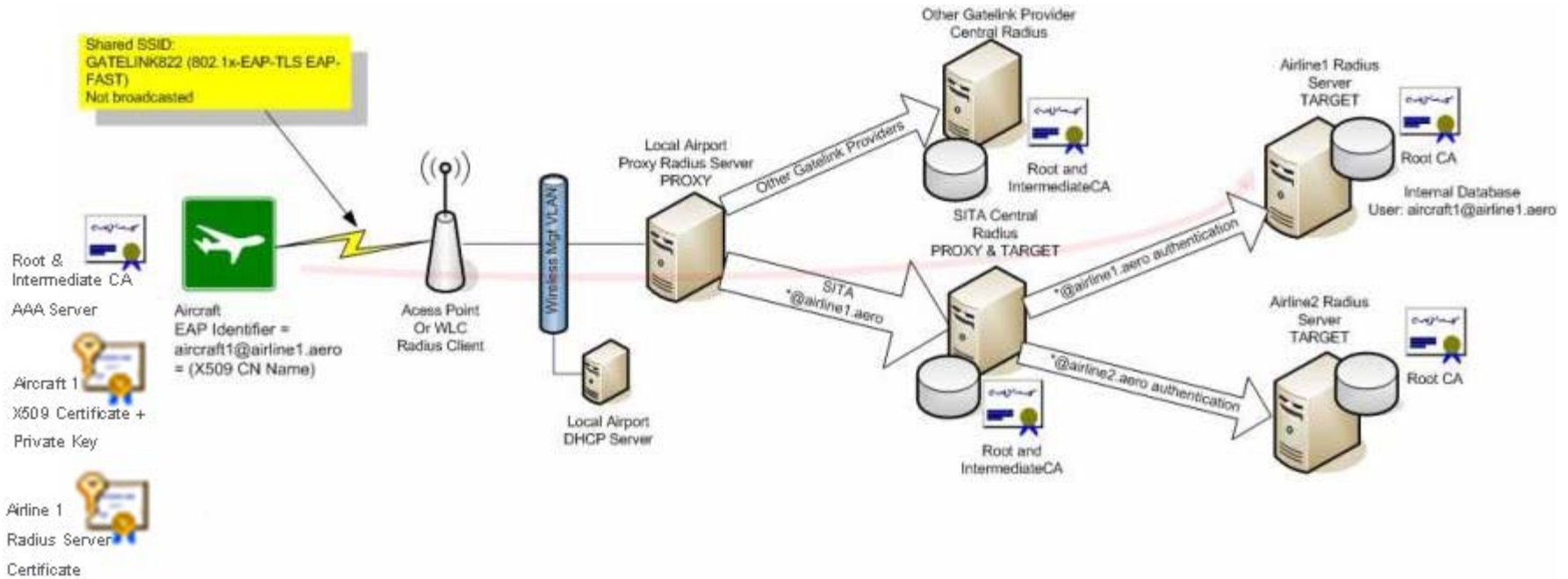
- Problem Encountered
 - Variability in identification document standards and guidelines
 - Legal issues
- Fix Applied
 - Identity proofing standards should be of highest priority
 - Standards should define a hierarchy of preferred documentation
 - Recognized state-issued passports
 - Source documents which may be used to obtain a passport (likely a country-by-country definition)
 - Work eligibility documents (requiring a country-by-country definition)
- How ATA Spec 42 recommendations mitigate this issue
 - Section 3.2 ‘Identity Proofing and Vetting’

Agenda

- 1 Some definitions and history
- 2 Still facing PKI Interoperability issues, here some examples
- 3 **Trust Model for the Industry**
- 4 Migration from SHA-1 to SHA-2
- 5 Digital Signature Interoperability

Business Challenge:

Identity Assurance that extends beyond the 4 walls



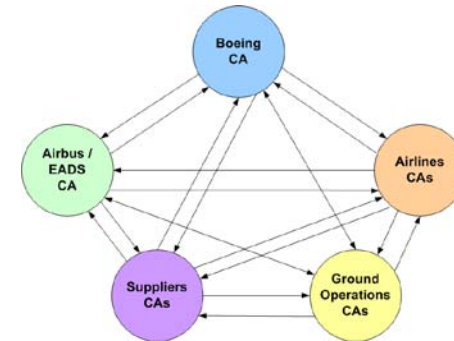
PKI – It's all about trust

What are the various trust models ?

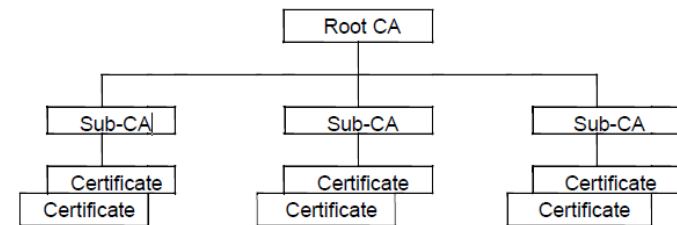
– Trust is derived from the 'level of assurance' which is linked to the CP

– Three trust models are available:

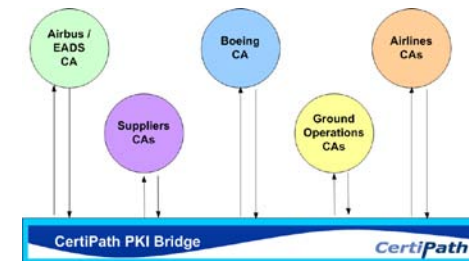
- Bilateral agreements between each parties that need to interact



- Hierarchical model



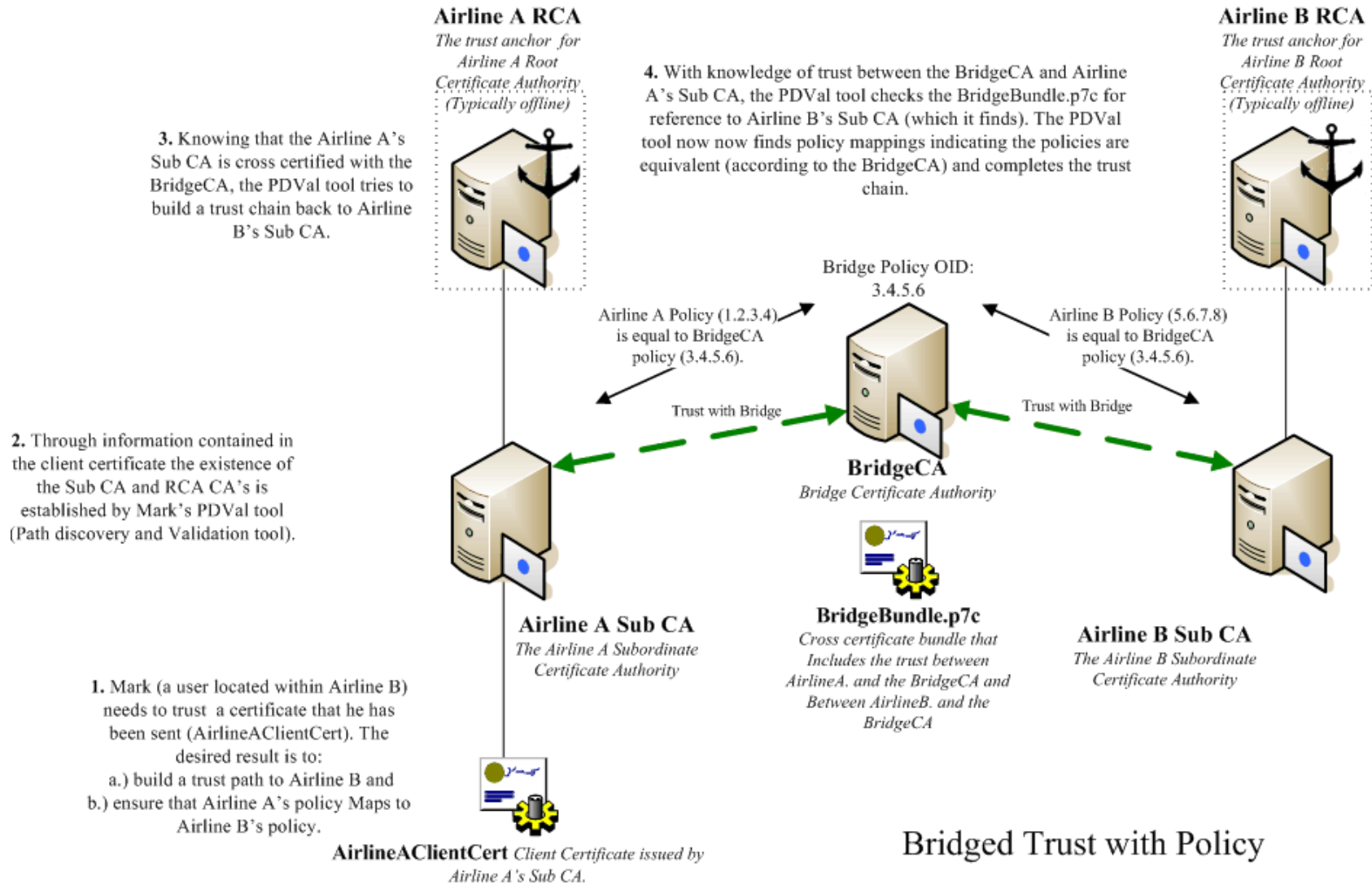
- Bridge (Cross-certified, shared trust) model



Advantages of a bridge model

- Agreeing to meet common standards and policies for identity assurance
 - Each organization can trust the assertions of others that are part of the community
- Certified once, trusted everywhere
 - Hub model is more cost-effective than 1-on-1 mapping with all of your partners
- Single strong authentication that is leveraged with all partners
 - By becoming cross-certified to a bridge, companies establish interoperable trusted identity credentials
- Avoids the issues related to managing large trust lists
 - Trust Level Assurance
 - Revocation

How Bridge Trust works



Bridged Trust with Policy

Source: ATA Spec. 42

Bridge CA Interoperability testing - an example

- Examination of all CA certificates, including self-signed root and cross certificate for compliance with the bridge Certificate Policy
- Examination of one sample of each type of certificates issued by each CA
- Examination of PKCS#10 cross certificate request
- Examination of one sample of each type of CRL issued by each CA
- Examination of all OCSP Responder certificates
- Examination of one sample OCSP request and response from each OCSP Responder
- Examination of all pointers in the certificates and CRLs such as CRL Distribution Point and CA Issuers field in Authority Information Access
- Obtaining status response of certificates from the OCSP Responders

Agenda

- 1 Some definitions and history
- 2 Still facing PKI Interoperability issues, here some examples
- 3 Trust Model for the Industry
- 4 Migration from SHA-1 to SHA-2**
- 5 Digital Signature Interoperability

What is SHA and why the migration to SHA-2 ?

- Secure Hash Algorithm (SHA) is a one-way hash function developed by NIST and defined in FIPS 180
- Most digital signatures generated today make use of SHA-1
- NIST SP 800-131 calls for digital signatures to be generated with a longer hash value by the beginning of 2011
- SHA-2 is the more secure successor to the SHA-1 digest algorithm
 - SHA1 produces a 160 bit digest value and is well paired with 1024 bit RSA public key certificates
 - SHA2 produces larger digest values that are well paired with 2048 bit and larger RSA public key certificates
 - Available algorithms: SHA-224, SHA-256, SHA-384, and SHA-512

Transition Timeline ?

- NIST 800-131 (draft) has recommended that 1024 bit RSA be eliminated from use by Dec 31, 2010
 - By Jan 1, 2011, in use RSA keys should be 2048 or better and the SHA2 family should be used for hashing / digest
 - This means ...
 - Certificates issued today that will survive beyond Dec 31 2010 should be 2048 bit or better
 - Conforming CAs must begin using SHA2 by 2011
 - SHA1 no longer considered safe to use
- Transitioning of some avionics systems may take longer because of airworthiness certification process
 - Decision to delay transition should be supported by adequate risk assessment

What issues may this transition cause ?

- Many PKI-enabled applications already have full support for SHA-2, as stated by S/W vendors
 - Applications based on OpenSSL (Apache, WebSphere, SAP Web Server, etc.) or Java
 - Applications based on MacOSX, Microsoft Vista, Win7, Win2008 server

- Some PKI-enabled applications may not support SHA-256
 - Applications that sit on Microsoft Windows XP (WinXP) Service Pack 3 make use of CAPI each need to be modified to make use of SHA-256
 - Microsoft has no plans to update the WinXP versions of these applications

=> Need to build inventory of PKI-enabled applications and ensure that they will support SHA-256

- CAs to be updated
 - Interoperability testing using SHA-256 to be done prior to 1-Jan-11
 - 1-Jan-11: Exclusive use of 2048-bit keys in any NEW CA & end-entity certificates issued under its public root

Agenda

- 1 Some definitions and history
- 2 Still facing PKI Interoperability issues, here some examples
- 3 Trust Model for the Industry
- 4 Migration from SHA-1 to SHA-2
- 5 Digital Signature Interoperability**

What is a Digital Signature & What is it used for ?

- **Electronic Signature**
 - An electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign
- **Digital Signature**
 - Cryptographically-generated signature based on public-private key technology
 - Data appended to a cryptographic transformation of a data unit, that allows a recipient of the data unit to prove the source of a data unit and protect against forgery [ISO 7498-2]
- **4 basic functions of digital signatures**
 - Identification signatures
 - Authentication signatures
 - Signatures as declaration of knowledge
 - Signature as declaration of will

What is an interoperable digital signature ?

- Legal frameworks are common across borders
 - Legal framework for electronic signatures has reached a stage of maturity in some areas of the world¹
 - Legal framework should not be based on concepts that are unique to a specific country
 - Legal framework should not contain requirements that cannot be met by foreign solutions
- Technical interoperability in terms of:
 - Signature solutions have a cross-border perspective
 - Digital certification attributes
 - Signature validation method
 - Signature format
 - Signature algorithm

¹ Source: <http://ec.europa.eu/idabc/servlets/Doc?id=32436>

What are recommended steps to create a digital signature ?

- Intended signatory obtains a digital signature key pair that is generated as specified for the appropriate digital signature algorithm (DSA, RSA, ECDSA)
- Intended signatory obtains assurance of
 - Validity of the public key
 - Possession of the associated private key
- Message digests are generated on the message using approved hash functions
- Using the signature algorithm, the signature private key, message digests and other information required by the digital signature process, a digital signature is generated
- Signatory may optionally verify the digital signature using the signature verification process and the associated public key

Work in Progress

What are recommended steps to validate a digital signature ?

- Digital signature was created during the validity period of a valid certificate by the private key corresponding to the public key listed in the certificate
 - Check the certificate signature by a trusted CA
 - Check for certificate path validity up to CA Trust Anchor (leveraging PDVAL tools)
 - Check certificate validity
 - Check certificate revocation status
 - Check name chaining
 - Check certificate
 - Check name c
- Message / document to the digital signature has not been altered since its digital signature was created
 - Signed content integrity check
- May want to leverage server-based Certificate Validation protocol (RFC 5055)

Work in Progress

Conclusion

- PKI technology increasingly used for Air Transport Industry use cases
 - AEEC 822 ‘Gatelink’
 - AEEC 655 ‘Loadable S/W Standards’ / 827 ‘Electronic Distribution of Software’
 - FAA Order 8130.F / ATA Spec. 2000, ch.16 ‘Electronic Product and Part Regulatory Doc.’
 - ICAO Doc. 9880, ‘Technical Specifications for the Aeronautical Telecommunication Network (ATN)’
- PKI technology is highly configurable thus allowing technology to be re-used for multiple business use cases
- Wrong PKI configurations could lead to interoperability problems
- Lot’s of good work already done to minimize interoperability issues
 - ATA Spec. 42 is a good starting point
- ATA Digital Security Workgroup actively working on minimizing such issues
 - In process of developing a new appendix on digital signature interoperability
- We seek your active participation to ATA DSWG



Thank you

For additional information, please contact
Mansour.Rezaei-Mazinani@sit.aero