

# ATA Spec 42

Cybersecurity Working Group  
2025 overview

# All about Spec 42

- Purpose for the specification
- History
- What does it provide?
- Standards
- Compliance
- Future work

# Why Spec 42?

- Secure operation of the “connected aircraft” has made it necessary to leverage Public Key Cryptography, and the supporting Public Key Infrastructure (PKI), to ensure digital security within the airline and aircraft infrastructure. This technology enables security controls that provide authentication, integrity and data confidentiality
- Use of industry standards and guidance, such as ATA Spec 42 and multiple ARINC documents (e.g. ARINC 842-3, 835, 827 645-1) are essential in helping reduce risks of compromise associated with ***misguided deployments***.
- As more and more “connected” use cases emerge, having a single, secure way to implement reduces costs and complexity of deployments
- Success requires the right tools, policies and practices to be followed – ***it’s not just about the technology***.
  - 90% of the effort is in the policies, procedures, practices and training
  - 10% of the effort is in the technology
  - 100% of the value is in the first 90%

# History

- AFG Digital Certification Working Group (DCWG) launched in 1998
  - SITA / Equant built the first “Aerospace PKI” which was operational in 2000
  - First CP based off of Canadian Government PKI
    - The GoC PKI CP was later used by many others as well, so the Aerospace Industry alignment with other relevant PKI policies has been there from the start.
- DCWG joined ATA e-Business Program in 2002
- Recast as ATA Digital Security Working Group (DSWG) in 2005
- Initial issue of Spec 42 in 2008
- Rebranded as ATA Cybersecurity Working Group (CSWG) in 2025
- Most recent issue 2025.1

# What does Spec 42 provide?

- Builds on open, established standards and technologies – Public Key Infrastructure (PKI), Digital Signatures, Digital Identity, etc.
- Establishes **industry-standard** policies for issuance, usage and management of digital certificates
- Provides guidance for deployment of identity management solutions based on regulatory guidance such as FAA AC 120-78A Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals
- Guidance on application of both PKI and non-PKI solutions to provide security of digital resources

# Which Guidance?

- Identity and Access Management
  - Common design and operational guidelines to be followed by organizations that desire to use credentials (PKI-based or otherwise)
  - Covers both the credential issuer, as well the engineering guidance to use the credentials
- Digital Signing of Data
  - Digital signature use cases
  - PKI (asymmetric keys) and non-PKI (symmetric keys) signature guidance
- Time Stamping and Archiving
  - Timestamp use and guidance
  - Digital Archiving Considerations

# Provides Reference Policies

- ATA Spec 42 Reference Certificate Policy
  - A Certificate issued in accordance with this Certificate Policy (CP) conveys a low or medium level of identity assurance, using either software or hardware storage for private keys.
- Time-stamp Authority Policy
  - Time-stamp Authority Policy (TSP) is presented as a template to organizations interested in becoming Time-stamp Authorities (TSA) within the civil aviation and aerospace industry
- ATA Spec 42 Reference Digital Signature Policy
  - Template for a policy which specifies the minimum set of rules for application and management of digital signatures for the aerospace community

# Build on Standards, and is the Standard

- **Spec 42 *relies* on many non-aviation industry specifications and guidance. For example:**
  - Federal Information Processing Standards: FIPS140-2, FIPS-197
  - National Institute of Standards and Technology: NIST SP 800-57, NIST SP 800-63, NIST SP 800-122
  - European ETSI standards
  - OASIS W3C
  - Internet Engineering Task Force: RFC3647, RFC5280, RFC 7030, RFC 1994, RFC 2759, RFC 2945, RFC 4210, RFC 5055
  - OMB Memorandums: M-04-04, M-07-16
- **Spec 42 is *referenced as a requirement* within many aviation industry documents for guidance:**
  - ATA Spec 2000 Chapter 16
  - ARINC documents: 645, 667, 823, 827, 835, 842, etc.
  - ICAO ATN-IPS
  - ICAO Trust Framework Panel
- **Spec 42 compliance is *required* in many aircraft OEM programs:**
  - Boeing: *“Implement a Level 4 certificate policy process for airplane software signing certificates, per reference c) ATA Spec 42, chapter 2 or equivalent.”*
  - Airbus: *“In order to generate FLS digital signature, the supplier shall use a digital signature tool and cryptographic elements compliant with Digital Certificates ATA/DSWG Class 4 or Medium Hardware Certificate Policy as described in document ATA/DSWG Spec 42 2012.1.”*

# Compliance

- Increasingly, “ATA Spec 42 Compliant” is becoming a normal thing to see
  - Language such as “Credentials used for signing must be issued at ATA Spec 42 Medium-Hardware Level of Assurance”.
- Can be thought of in two ways:
  - **Component (Avionics, GSE, PDL, etc.) implementors** have guidance in Spec 42 on how to handle validation and use of the PKI and non-PKI Credentials
    - Implementing all of the SHALL requirements related to the consumption, interpretation and validation of the credentials.
  - **Credential Issuers**
    - Issuing Spec 42 compliant credentials means implementing **all** “SHALL” requirements in the Spec 42 Reference Certificate Policy, and passing an annual audit by a third party auditor that proves such compliance.

# Future Work

- Co-Ordinate to ensure that ATA Spec 42 is in alignment with all other relevant PKI Policies that may affect the Industry
  - ICAO Trust Framework Panel
  - US FBPKI / EU Framework on Digital Signatures
- Comprehensive Compliance matrix for both component vendors and credential issuers
- Post Quantum Crypto incorporation to assist in migration in the early 2030s
- Encryption
  - Increasing topic of interest
- Continuing work to ensure alignment with relevant standards and governmental identity policies



# Contact Information

Patrick Patterson  
Chief PKI Architect  
Carillon Information Security Inc.  
[ppatterson@carillon.ca](mailto:ppatterson@carillon.ca)  
tel: +1 514 485-0789 x101  
mobile: +1 514 994-8699  
fax: +1 450 424-9559  
<http://www.carillon.ca>