Fortanix®

Case Study


# Global Aerospace Leader Achieves Aviation Data Security Controls and Standards

## Customer Profile

A world leader in aerospace. The company is a leading manufacturer of comercial jetliners, defense, space, and security systems.

## Data security challenges with the new generation of 'connected, digital aircrafts'

### The new generation of aircraft systems

Over the last decade, the commercial aviation industry has been going through a major transition towards the 'digital and connected aircraft'. These changes have been propelled by the increasing need to improve overall efficiency within the aviation space and reduce the cost of operations. This has led to the installation of several onboard systems on commercial airplanes to improve the overall efficiency and maintenance. Aircrafts today increasingly interact with external systems and applications, including the internal avionics systems communicating with the ground station or even a passenger accessing a service using internet. Some of these systems are also used for air-ground communications and transfer of data collected onboard to the back office.

### Why data security is so critical

With dozens of connected systems and data points, there are increasing incidents and risks of cyber-attacks and the current suppliers in aviation have not been able to implement broad data security controls. This has led to issuance of specific standards within the aviation space to ensure security of data and connected systems. And that's why data security is of critical importance for airlines.

### Spec 42 of Aviation Industry Standards for Digital Information Security

provides the appropriate standards and measures required to achieve the appropriate level of security for an aircraft application that primarily relies on digital identities. It's also a framework to transition from an existing manual process to an automated digital identity-based solution. One of the most important mandates stipulated by Spec 42 requires all aircrafts to use a FIPS compliant device to store the private keys for aircraft parts and implement an effective code signing operation for all parts within the aircraft. Today's connected airplanes are required to implement a PKI based security to operate.

## What Were They Looking For?

The customers' primary use case was parts signing to meet the Spec 42: Aviation Industry Standards for Digital Information Security. The customer had partnered with Microsoft to transition its commercial aviation applications into the Microsoft Azure Cloud and made use of Azure IoT suite, Bifrost SD/ fleet link services. To enhance the security of their applications and data, the customer was specifically looking for-

- HSM functionality through the Azure Cloud to Bifrost and SDM/Fleet Link services, infrastructure, and applications
- Secure cryptographic key management utilizing HSM technologies that meet or exceed the FIPS 140-2 standard
- Scalable code signing operations.
- Platform reliability and uptime was also a critical requirement.

There was an increasing need for a PKI based signing solution to help enhance security and improve trust across day-to-day operations such as electronic boarding, package distribution and signing of flight paths.

## What was offered? - Fortanix Solution

Customer had prioritized on the code signing project but was not able to zero in on a vendor that could offer a scalable solution with minimized impact on airplane operations. The project was literally months behind schedule. The customer approached Fortanix for a POC. The solution was offered as a quick to deploy and easy to use SaaS. After a successful POC, the project was fully implemented for their operations in one key geographic region. The design architecture included-

- The Fortanix cloud based FIPS 140-2 Level 3 HSM utilizing Intel® SGX: Software Guard Extensions.
- All HSMs provided by the service were fully redundant, and no action was required (by humans or external applications) to access a "redundant node" in the event that a "primary node" becomes unavailable.
- The SaaS user interface was accessible via two-factor authentication. Applications and APIs communicate with the HSM "nodes" through authenticated API mechanisms. Authorized, and authenticated users use the GUI to establish "groups" of HSMs and generate required keys within the HSMs.
- Certificate Signing Requests (CSRs) are then generated through the service GUI or via customer applications.
- Keys are always maintained within the HSMs as well as all cryptographic processes (signing, authentication, etc.).

This HSM infrastructure was used to manage the following keys and processes:

**All authentication keys and cryptographic authentication processes.**

**Bifrost API-based key signing and all cryptographic signing operations.**

## Why Fortanix?

While evaluating different vendors, they were specifically looking for a solution that was easy to configure and provided reliability and uptime. Fortanix delivered its Data Security Manager as a SaaS which offered the following differentiators

SaaS based solution was quick to deploy and easy to use with a user-friendly centralized console to monitor all data security operations of the aircraft.

Fortanix offered a state-of-the-art code signing solution that included a FIPS 140-2 level 3 assurance for private key protection and advanced capabilities like strict role-based access controls, quorum-based approval workflows, automation, and audit logs for all code signing operations.

Supported all types of asymmetric keys, signing, and hashing algorithms used for code signing

Secure storage of sensitive objects/keys during the signing and verification processes.

| Required Digital Solution as per Spec 42 – Compliant PKI Solution | Why Fortanix |
|---|---|
| Associate signer with credentials using a medium level of assurance | State-of-the-art signing solution with FIPS 140-2 level 3 assurance for private key protection |
| Credentials of signer valid and not compromised and known across companies | Strict role-based access controls, Secure storage of keys and Quorum-based approvals |
| Transferable historical record of protected content and knowledge of who signed, identify when record was generated using timestamp, as appropriate | Tamper-proof audit logging capabilities |
| Industry best practice of ensuring data integrity | Intel SGX powered technology to protect data across its lifecycle |
| Positively identify characteristics of and associate what was signed with signee | Quorum approval workflows |

## The Impact

The practical applicability of the solution to enhance the data security controls within the aircraft and fleet operations has made a considerable impact on the overall operational efficiency and trust.

### Help build trust across day-to-day airplane operations

Day- to-day operations such as ability to do the signing of packages before the packages are distributed and uploaded to planes, signing of flight paths, etc. are now done through a robust PKI-based signing backed by FIPS 140-2 level 3 Certified HSM enhancing the overall security and help build a trust-based operational model.

### Meet Aviation compliance standards

With most standards in Aviation requiring a PKI based signing solution backed by a FIPS validated HSM to enhance data security controls for airline operations, Fortanix implementation has helped meet these requirements.