CASE STUDY

IMPLEMENTATION OF PUBLIC KEY INFRASTRUCTURE (PKI) WITH HSM FOR VISTARA

About The Company

Vistara is a joint venture of Tata Sons Private Limited and Singapore Airlines Limited (SIA). The company is registered as TATA SIA Airlines Limited wherein Tata Sons holds 51% stake in partnership and Singapore Airlines owns 49% stake. The carrier commenced operations on 9 January 2015 with its inaugural flight between Delhi and Mumbai. The airline had carried more than two million passengers by June 2016 and as of 2019, has a 4% share of the domestic carrier market, making it the 7th largest domestic airline. Vistara was the first airline to introduce premium economy seats on domestic routes in India.

The common goal of the joint venture is to redefine air travel in India to provide Indian travelers a seamless and personalized flying experience that blends Tata’s and SIA’s service excellence and legendary hospitality. As it aims to transform the flying experience of travelers in India, Vistara christens its brand tagline as 'fly the new feeling'. In a short span of time, Vistara has rapidly expanded its footprint, both in terms of network and service proposition. Vistara now serves 36 destinations with over 200 flights daily and has already flown more than 20 million happy customers since starting operations.

FLEET

- **Airbus A320**
- **Boeing 787-9 Dreamliner**
- **Boeing 737-800NG**
- **Airbus A321neo**

[Link: www.tataadvancedsystems.com]
E-Enabling Aviation

The general trend towards omnipresent networking has reached the realm of the aviation sector. Commercial aviation is at the threshold of the era of the e-Enabled airplane, thanks to the convergence of world-wide data communication systems, network-centric information processing and commoditized lightweight computational hardware. e-Enabled airplanes with wired and wireless offer a wide spectrum of network applications such as Electronic Distribution of Software (EDS), and onboard collection and offboard retrieval of airplane health reports are bound to revolutionize the current air transportation system. Such airplanes provide many benefits to operators in terms of operational efficiency, passenger comfort, and maintenance, repair, and overhaul.

The aerospace industry is witnessing a revolutionary trend, seeking technological and process innovations in aircraft design, manufacturing, operation, maintenance, and traffic management. The next generation air transportation systems such as FAA-led Next-Gen in the USA and SESAR in Europe will employ technologies and processes for enhancing airspace capacity and aircraft operation and in these future systems, the e-enabled aircraft is envisioned to play a key role with its advanced sensing, computing, and communications features. A well-designed information system provides a robust foundation for e-Enabling. This systems architecture enables the airline to efficiently implement and maintain integrated business systems.

What are EFBs?

Apart from the technological advancements in the areas of aircraft engines and airframes, significant modernization of the avionic equipment is being witnessed. There was a time when classic analogue dials were once an essential part of any cockpit; nowadays they are more likely a relic and their function is being taken over by multifunctional displays (glass cockpit) that we can find in many general aviation airplanes. The paper documentation necessary for flight operations and management meets the similar fate. To increase efficiency, be more eco-friendly, and take advantage of technology, the aviation industry is gradually drifting towards the paperless cockpit.

According to Federal Aviation Administration’s Advisory Circular 120-76D, dated 27 October 2017, “An EFB is any device, or combination of devices, actively displaying EFB applications. An EFB hosts various applications, which are generally replacing conventional paper products and tools, traditionally carried in the pilot's flight bag. EFB applications include natural extensions of traditional flight bag contents, such as replacing paper copies of weather with access to near-real-time weather information.”
Business Challenge

Being a technology-focused organization, Vistara continually looks to optimize its IT resources and infrastructure to keep pace with rapid growth in its own network and the aviation industry at large. The Airline’s documentation and the processes and regulations surrounding it are quickly evolving. Accountability, consistency and integrity are of utmost importance for flight safety, work efficiency, regulatory compliance, and to maintain sustainable profit margins in order to survive competition. The Electronic Flight Bag is a modular, integrated hardware and software package and is a major step toward e-enabling the entire air transport system. In addition to this, the EFB provides communications interfaces and data management capability between the EFB and the airline operational control. These modernizations, although highly efficient, timely and accurate, can also be easier targets of “spoofing” or interception of communication paths. Essential data that is communicated in the open is susceptible to multitude of attacks which could jeopardize system integrity and availability. There must be a method where the operator can verify the integrity of the information being transmitted and the signing validity of the source, in order to maintain aircraft and passenger safety.

Solution: Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. PKI has been deemed by leading aircraft manufacturers as the best suited security solution for various aircraft-related applications. It is the most secure and flexible authentication method used today within the aerospace community as it can ensure a much stronger identity assurance to minimize or prevent operator error, and greatly reduce security risks. The reason being that digital certificates issued from the private branded CA provide a robust foundation for secure document exchange, collaborative engineering, secure e-mail, digital signatures and transaction security between systems. Not just this, to validate communication devices, device authentication can be carried out through X.509 Public Key Infrastructure (PKI) certificates.
Components of PKI

- Certificate Revocation List (CRL)
- Certificate Authorities
- SCEP/NDES
- Certificates
- Hardware Security Modules (HSMs)
- Authority Information Access (AIA)
- CAPolicy.inf
- Certificate Templates

Benefits

One of the advancements that brings in e-Enablement of aircrafts are the Electronic Flight Bags that facilitates a neat, paper less cockpit and other benefits such as quick and efficient access to charts, logbooks, operations documents, enhanced taxi safety awareness, video surveillance, and reduced fuel and maintenance costs amongst others. However, to address the cyber security aspects, utmost care must be considered to identify the EFBs before the relevant data is loaded into them from ground systems. Not just this, all the data that leaves/enters the ground systems must remain confidential and be passed through strict authentication and integrity checks. The Public Key Infrastructure (PKI) is technology based on cryptography that addresses these aspects in the most efficient manners. The afore described PKI architecture serves as a flexible authentication method that helps to circumvent multitude of security risks and facilitates safe exchanges of sensitive data. Functioning as a trusted service that supports a variety of platforms and integrates seamlessly with other information security solutions such as the Mobile Device Management (MDM), it can be leveraged to serve as a single management and technical methodology to satisfy several business needs and enforces the principles of confidentiality, integrity, availability, non-repudiation and authenticity.
“Vistara strives to enhance passengers' comfort and experience. With the acquisition of e-Enabled airplanes such as Boeing 787-9 Dreamliner and implementation of EFBs, and to circumvent network-induced security threats, it required a solution to ensure safe distribution of business-critical airplane software. Public key infrastructure (PKI) was the legitimate solution to help us achieve this.”

“With concerted due-diligence, we selected the Public Key Infrastructure with Gemalto HSM to build assertive, coordinated, and effective technology to defend our aviation’s networks, infrastructure and business, especially for long-haul aircraft journeys as against traditional way of building PKI solution. We are proud to build a key differentiator having one of the first Wi-Fi-enabled aircraft combining PKI & E-Enabling security utilizing tamperproof, FIPS capable HSM.”

Subhash Kumar Mishra
Head IT Enterprise, TATA SIA Airlines Limited – Vistara