UNISYS | Securing Your Tomorrow®

HOW AIRPORTS CAN ENHANCE PASSENGER EXPERIENCE AND SECURITY WITH BIOMETRICS

ABOUT THE AUTHOR

Ajay Prabhakar is the Industry Manager and SME for Airports Passenger Facilitation in Unisys Asia-Pacific. He is responsible for developing new solutions for passengers as well as pre-sales and marketing for the Unisys Airports Solutions. He has delivered and implemented products for Airlines and Airports such as Departure Control Systems, self-service technologies such as kiosks, self-bag drops, home printed bag tags etc. He is a member of IATA and various industry groups, a blogger and a thought leader in airports passenger domain.

Contact him at
Ajay.Prabhakar@in.unisys.com
Or connect with him on LinkedIn.

Air transport is the fastest way to get from Point A to Point B. No wonder, millions of people pass through airports across the globe each day to board flights to their destinations. But moving through the airport itself, from the curbside to the plane, is far from swift. Air travelers must navigate through various airport zones and undergo multiple physical and document checks before they can finally board their aircraft and set off for their destination. One of the biggest difficulties passengers face within the airport is security.

Of course, the importance of passenger security measures in airports is impossible to overstate. By virtue of their role in facilitating domestic and international travel, airports are potential gateways for illegal activities and unlawful entry into foreign countries. Incidents such as the 9/11 attacks demonstrate how the wrong people on-board can impact not only the safety of other passengers, but also the nation as a whole. In the age of fake identities, forged documents and insider threats, it is vital for airports to ensure that people are who they claim to be and that their presence at the airport and on an airplane poses no security risks.

Multiple cases of fake ticketing and documents, impersonation, unlawful immigration and collusion with airport staff to carry out terrorist attacks have come to light in recent years. Consider the case of a 32-year-old man detained at New Delhi's Indira Gandhi International Airport as he prepared to board a flight to the United States using the identity of someone more than 50 years his senior[1]. Two other travelers were apprehended in separate incidents for allegedly using fake tickets to enter the terminal area for personal purposes[2]. In another instance, a non-Indian was arrested at Delhi airport with a fake Indian passport and documents[3]. Clearly, airports need infallible methods to establish the identity of travelers and prevent their unwarranted and illegal movements.

Failsafe Security

Today, passengers undergo long, painful security checks. While airports have embraced technology for many aspects of airport operations, security continues to rely heavily on manual procedures and identity checks. Moves to tighten passenger security have only added more checkpoints in the process. Long queues and slow screening together with repeated document checks inconvenience passengers and cause considerable anxiety. Long screening backlogs cause passengers to miss flights and lead to misplaced baggage or even flight delays. Such issues can potentially snowball into airline or industrywide problems. Disgruntled passengers may become unruly, affecting the safety of other passengers and airport staff alike. Ultimately, passengers suffer, airports get bad press and the airline bears financial, legal and reputational costs.

[1] https://7news.com.au/travel/man-disguised-as-senior-citizen-tries-sneaking-onto-flight-to-us-at-indian-airport-c-449446

[2] https://www.indiatoday.in/india/story/british-2-held-delhi-airport-fake-ticket-entry-1596956-2019-09-08

[3] https://www.hindustantimes.com/delhi-news/rohingya-man-arrested-at-delhi-airport-with-fake-indian-passport/story-N7xLRXAJK8ckDcStTz0gYK.html

Manual security checks will not remain viable. Airports need solutions to move passengers more quickly and efficiently while accommodating evolving security requirements. Biometric security looks like an obvious choice.

Biometrics offers a solution for ensuring a positive passenger experience without compromising security. Biometric security is based on the premise that every individual can be accurately identified by intrinsic physical or behavioral traits. Biometric data is difficult to steal or fake and changes little over an individual's lifetime. Convenience is another bonus, as biometrics demands no passwords, tokens or documents. An individual gains access to restricted areas simply by being himself! Border control, healthcare and law enforcement are some of the industries that have adopted biometric identification. Airports across the globe have implemented or are currently running trials or small-scale biometrics based passenger identification and processing programs, be for it one touchpoint like the boarding gate or multiple checkpoints from curb to boarding gate.

Biometrics Sees Growing Acceptance

So, what do travelers feel about using biometrics for passenger security checks at airports? Findings from the 2019 Unisys Security Index™, a signature research program run by Unisys, point to travelers' increasing willingness to share data from their social media, online purchases, smartphone or wearable devices with airports and airlines to guide their journey through the airport. In the APAC region, 28% of Australians, 38% of New Zealanders, 39% of Filipinos and 47% of Malaysians were open to sharing their data. Across the globe, a whopping 86% of U.S. respondents were willing to give their biometric data at the airport and almost 50% of U.S. respondents were open to facial recognition at airports. In essence, travelers are slowly but surely coming around to the idea of sharing their biometric data for their safety and convenience while traveling. This gives airports ample reason to consider investing in biometric security systems.

In addition, consider the projected rise in air-travel. IATA estimates that passenger numbers could double to 8.2 billion in 2037[4]. Clearly, manual security checks will not remain viable under these circumstances. Airports need solutions to move passengers more quickly and efficiently while accommodating evolving security requirements. Biometric security looks like an obvious choice.

What Airports Need in a Biometric Solution

Before delving into how biometrics helps address the security needs of airports, let us describe the components of a biometric verification system and how it works. A basic biometric device includes a reader or scanner that records the biometric factor being authenticated as well as a biometric engine that converts the scanned data into a digital format. The solution then compares the observed data with stored data in a database to establish or refute an individual's identity. To set up a biometric identification system, airports must invest in a framework that delivers these capabilities while addressing airports' unique requirements.

Because the airport landscape is heterogeneous, comprised of a wide range of systems and devices from different vendors—e.g., enrollment kiosks and entry gates, self check-in kiosks, self bag drops, security checks, immigration and border security and boarding e-gates-the biometric system should work seamlessly with diverse systems, vendor products and integrations with airport and government systems.

The biometrics factor used for establishing identity is another important consideration. Face biometric is the most recommended due to its ease of capture, ease of recognition and versatility. However, as technology and business needs evolve, airports may need to move to a multi-modal approach such as say, Face+Iris. The biometric framework must support this and the evolution of airports as they expand to serve greater numbers of travelers using more systems and devices from multiple vendors, and process more transactions.

[4] https://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx

Airports need a multi-biometric, vendor-agnostic framework that can plug-and-play with multiple biometric engines with minimal or no code changes. The solution should seamlessly connect with multiple airline, airport, passport and immigration systems and devices that process travelers and identify them. Such a biometric solution gives airports the freedom to choose the best technology to suit their needs without worrying about compatibility or a vendor lock-in to a specific system/ technology.

If airports decide to move to a different partner for their biometric engine, the framework should support this as well. Since international travel includes passport and border control checks, the biometric system should integrate with the respective government systems as well as be capable of assessing the risk using local and international watch lists and databases. While biometric validation is definitely more secure than manual security checks, biometric data is highly private and sensitive and is protected by privacy laws. This also makes databases holding biometric data attractive targets for hackers. Securing these databases is a critical aspect of a biometrics engagement.

Airports must also be able to manage exceptions using manual processing. For example, some travelers may not have their biometric data stored in a central database or may be uncomfortable sharing it or may be traveling in groups. Injuries or other mishaps may change some biometric data. Identification failures can also occur due to various environmental factors such as lighting. All these factors require manual intervention and the biometric system in place should accommodate such exceptions or at least simplify some parts of it.

A Plug-And-Play Framework

Airports thus need a multi-biometric, vendor-agnostic framework that can plug-and-play with multiple biometric engines with minimal or no code changes. The solution should seamlessly connect with multiple airline, airport, passport and immigration systems and devices that process travelers and identify them. Such a biometric solution gives airports the freedom to choose the best technology to suit their needs without worrying about compatibility or a vendor lock-in to a specific system/technology.

Implementation of such a system in airports mandates a thorough understanding of the industry, the operational and techno-functional environment of airports and the ability to deliver not only biometrics capabilities, but holistic services including end-to-end implementation, ongoing support and security.

Introducing biometrics technology at airports can certainly enhance passenger experience and airport security, provided airports chose the right technology and an able partner.

For more information on how biometric technology can empower airports to deliver a better passenger experience without compromising security, visit www.unisys.com/smartsecureairports.

For more information visit www.unisys.com

Printed in the United States of America 10/19 19-0586