Identity Management & Aviation White Paper

Reinventing Airport ID Pass Management

HUMAN RECOGNITION SYSTEMS

RIGHT PERSON | RIGHT SKILLS | RIGHT PLACE

Contents

Introduction

If you've ever applied for an Airport ID Pass, you know what a painful process it can be. All staff working either airside or landside (be it permanently or temporary) at an airport are required to have a valid ID Pass issued by the Airport they are working in. Whilst the rules underpinned by regulation have evolved or rather been added to, extended and further complicated, over 25 years, all except one of the UK's Airports still use the same paper based processes.

This paper will examine the issues facing the current pass process and how new technology can help remove these issues ensuring a better process for all stakeholders.

The Problem

It is a confusing process for the companies applying for passes for their staff. Application rejection rates for permanent ID Pass applications of between 15% and 80% at Airports we work with confirm this. When the minutiae of rules (even to the extent of acceptability of certain letterheads or the colour of the ink used) differs from site to site this creates a further administrative effort for companies whose staff work at multiple sites.

This detracts from the serious security process at hand, focusing energy on the administrative overhead, rather than mitigating an ever present insider threat.

For Authorised Signatories

Companies have to appoint an "authorised signatory" to legally undertake the Airport ID pass application process within their business. This person is then responsible for ensuring that relevant and correct information about ID pass-holders or applicants is passed to the Airport ID Centre and is kept up to date. For new applications they have a responsibility for obtaining references and other documents e.g. criminal record checks, which in themselves are only valid on the day they are printed. They are also responsible for verifying aspects of each application. In practice the process is undertaken by existing roles within the organisation (Security, HR, Line Managers etc.), but increasingly it is outsourced at some cost to avoid the complexity.

The application process is not only complicated, it is slow. The end to end average lead time to obtain an Airport ID pass can be up to 9 weeks; costing the UK Aviation industry in excess of £2 million per annum in lost productivity alone.

Despite all this, on-airport companies can be afraid to complain. Identity Centres at UK Airports are professional and have to balance security and customer service at the front line. Nevertheless, they are the gateway to the Airports and therefore making a complaint is seen by some as too high a risk.

With the paper process being siloed, Authorised Signatories also felt they were operating alone and are lacking a sense of community that they can call on to help drive any change.

For Airport ID Centres

However this isn't one sided. The Airports too suffer from the process. One of the UK's largest and most respected Airports rejected between 20-25% of initial applications due to administrative errors by the applicants and authorised signatories and we've had reports as high as eighty per cent in other leading Airports.

The lack of visibility for each pass application leads to more calls to the ID Centre, further taking their time away from their true job – to vet pass applications and ensure security at the airport.

This waste, for the airport and on-airport companies is at the heart for the need to change…

Why hasn't this changed?

There are a number of reasons why the process has not changed. Firstly there is no single owner. It is a federated process i.e. a distributed process where the different parts of the process are controlled by different people. This means that pass processes have evolved differently at different Airports creating a lack of standardisation across the industry.

Secondly, due to the federated process, costs are hidden and distributed across all stakeholders. No-one organisation be it an airport or an on-airport company has a full handle on the costs across the whole process. And as most of the costs are associated to waste and inefficiencies within the process, they become difficult to quantify.

The Solution

Is Automation the answer?

Technology has moved on – look at tax self-assessment. Even in this most rigorous, rule driven, government process taxpayers expect to submit their tax returns on line, ensuring more accurate returns, fewer errors and for any administrative errors to be spotted and corrected before the return is submitted.

Whilst the existing process is confusing for the applicants, frustrating for the Airports and feels overly complex for both, products currently in the marketplace to help improve the process are primarily aimed at just semi-automating the existing vetting process through proprietary software - normally to lock customers into specific vetting companies.

Re-engineering not just automating

The semi-automation of the vetting process, however, is only one element of the end to end process. This approach doesn't really embrace the overall waste in the existing Background Checking, Vetting, Verification and Airport ID Pass Application and Management processes.

Automation of a poor existing process does not make the process better. The process can only be improved through end-to-end change and re-engineering.

Cloud-Based Software as a Service

By creating an online, cloud-based SaaS solution to handle the application, vetting and issuance of Airport ID passes, Airports open a raft of potential benefits.

Software as a Service (SaaS) is defined as software that is deployed over the internet. With SaaS, a provider (such as Human Recognition Systems) licenses an application (for example, MTrust) to customers as a service on demand, through a subscription, in a "pay-as-you-go" model.

Flexibility and Scalability

SaaS and Cloud solutions offer true flexibility and scalability and should give you confidence that the solution will be able to meet both your airport's current and future demands. For example, during an airport's busy summer or Christmas periods or large construction works that increase volumes for a period of time, a SaaS/Cloud solution such as MTrust requires no changes to the core system. It is simply scaled up to cope with the additional demand.
In fact, this flexibility is so crucial that 65% of businesses stated that it was an important reason to move to the cloud[1].

Automatic software updates, with improved support and maintenance

With SaaS solutions new functionality is available on demand and can be automatically updated with no intervention by the end user, nor any need to update servers, saving on average 18 man days[2] a year. This minimises any potential disruption to an airport.

Additionally software Support teams have instant access to your airport's installation enabling faster resolution to cases and less downtime.

Disaster recovery

When Airports move to the cloud, they no longer need complex IT disaster recovery plans. Cloud providers take care of most issues, and they do it faster, meaning one less job for an IT department and a cost saving for the airport.

SaaS solutions provide enterprise level redundancy rather than reliance on tape backups and on average resolve failures 4 times faster[3] than non-SaaS solutions.

Cap-Ex Free

With SaaS solutions, there is no upfront investment in software licensing as services, such as MTrust, are typically pay as you go, so there's no need for capital expenditure at all. As cloud and SaaS solutions are much faster to deploy, Airports have minimal project start-up costs, with predictable ongoing operating costs.

Work from anywhere

All of our solutions are available from anywhere with an internet connection, enabling employees to complete an application for an airport ID pass whilst on the move. As long as employees have internet access, they can work from anywhere. This in turn leads to higher adoption rates amongst end users.

Security

With SaaS, no data is stored client side. Some 800,000 laptops are lost per year in Airports alone[4], but when everything is stored in the cloud, data can still be accessed no matter what happens to a machine. This security is extended to the cloud servers, with the level of data encryption provided by systems such as MTrust means that even if a server or disk is stolen, the data cannot be accessed.

The importance of such security should not be underestimated. In July 2014, the ICO (information Commissioner's Office) fined the NHS, £325,000 after after hospital hard drives containing sensitive patient data were sold on eBay.

Over and above the direct financial implications of fines, the reputational damage of a security breach can have a significant detrimental impact to a company, especially in today's social media society

Copying with growing demand

As Airports continue to grow in size and take on more staff, it is clear that the existing paper based processes will not be able to cope with the extra demand. This will lead to delays in staff getting on to the airport and further disruption to on-airport works and a decline in customer service.

Systems hosted in the cloud have the ability to be scaled up or down based on demand. And coupled with the pay as you go element, Airports can benefit from significant savings by using this scaling flexibility.

Combatting the Insider Threat

Amid concerns about terrorists training in Syria and then returning to Europe or the United States, airport security officials remain focused on threats posed by "insiders" i.e. airport employees who could use their access to airport facilities to carry out a terrorist attack. This threat could come from any airline or airport employee with access to restricted or airside areas within the airfield, but what can Airports do to mitigate against insider threats?

The CPNI Insider Data Collection Study[5] looked into the personality types, behaviours and organisational settings associated with insider activity. The CNPI believe there is a “clear link between an insider act taking place and exploitable weaknesses in an employer’s protective security and management processes.”

We believe that Airport ID Pass management systems, whilst not offering an all-encompassing panacea for solving the insider threat, can help Airports addresses the key weaknesses identified by the CNPI:

1 Poor management practices and a lack of awareness of people risk at a senior level/Inadequate corporate governance

With the best of breed processes embedded, Airport Pass Management Systems overcome any existing poor practice. Employing these systems allows a cultural shift in how we manage insider threat to aviation, from the top down.

2 Poor use of auditing functions

The new systems offer traceability and auditing at their heart. For example, a User Audit that tracks every action performed by all users in detail.

3 Poor security culture

The new way of issuing an Airport ID Pass alleviates attention to administrative functions in the ID pass process. The old paper based processes bogged down vetting agents in the paperwork. Removing this means agents concentrate on security and identifying risks, rather than typos!

4 Lack of adequate, role-based, personnel security, risk assessment

Systems hosted in the cloud allow a better classification of roles. Allowing different users to perform different actions, based on their roles.

5 Poor pre-employment screening

An online system can ensure that Airport ID Passes cannot progress without the required criteria being met e.g.:

- 5 years history must be covered by references
- A valid GSAT certificate has been provided
- A valid Security Clearance reference (e.g. Basic Disclosure, CTC) has been provided

6 Poor communication between business areas

Online systems enable online communications and communities within the system design. This ensures that communication is carried out both within and across organisations involved in countering the threat to aviation to ensure best practices across the industry.

Our Solution: MTrust

MTrust is a revolutionary Airport ID Pass Application vetting and issuance solution, hosted in the Cloud. It provides streamlined Airport ID Pass management with absolute certainty of identity.

MTrust automatically checks all applications before they're submitted, reducing rejections by greater than 90% and allowing your vetting agents to concentrate on the important things. MTrust also gives Authorised Signatories total visibility of application status, allowing your agents to focus on security and not on incoming phone calls.

The key innovation of MTrust is that Airport workers become Members in the system, allowing them to store their profile in perpetuity. When they leave one company to work for another whether at the same or another Airport, they simply resubmit their profile and MTrust automatically completes their Application only alerting them to gaps. This innovation coupled with the ability to allow Authorised Signatories and individual applicants to check the status of their pass at any time brings a new level of customer service into the ID Centre service.

Developed with London Gatwick Airport, MTrust has created a thriving community of airlines, Airports and on-airport companies, including 2,500 Authorised Signatories. As more Airports select MTrust, with London Luton the latest, Authorised Signatories will already be registered, with employee information ready to submit. This will lead to greater information sharing across Airports, standardisation of the ID pass process and through reduced wastage and greater operational efficiencies it will create annual savings to the UK aviation industry of millions of pounds.

CASE STUDY: London Gatwick Airport

Background

As Gatwick look towards 45m passengers and a 2nd runway it's important for them to be ready for growth and a significant increase in the number of staff that will require an airport pass.

The existing system was slow and difficult for both Gatwick and their stakeholders and would struggle to cope with the increase in on-airport personnel. For an airport that processes 86,000 applications per year, any inefficiencies can be costly and time consuming. Gatwick needed to reaffirm their commitment to their key aims of building strong and constructive relationships with their stakeholders, through increasing value and efficiency and developing the best people, processes and technology.

The Challenge

All staff working either airside or landside at an airport (be it permanent or temporary) are required to have a valid ID Pass issued by the Airport they are working in. Whilst the rules underpinned by regulation have evolved over 25 years, UK Airports still use the same paper based processes.

Gatwick suffered from the process, rejecting between twenty and twenty-five per cent of initial applications due to administrative errors by the applicants and authorised signatories. This slowed the process down, increasing both costs and administrative overheads.

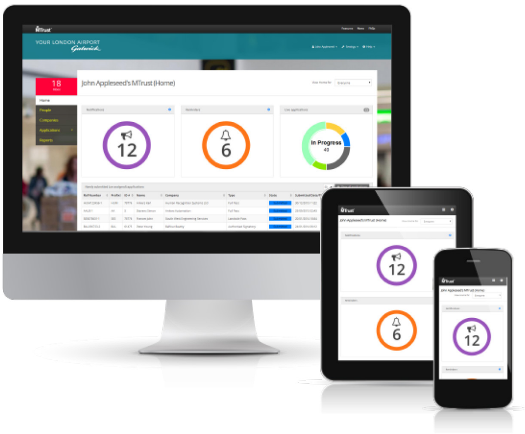
Companies must appoint an “authorised signatory” to legally undertake the Airport ID pass application process within their business. This person is responsible for ensuring relevant information is passed to the Airport ID Centre and is kept up to date. For new applications they must obtain references and supporting documents (e.g. criminal record checks) and verify all information provided for each application. Any new system would have to be easy for Gatwick’s community of 2,500 Authorised Signatories to use, whilst saving time and simplifying the process.

The Solution

Gatwick appointed HRS to deploy MTrust to transform its ID Centre in 2013.

MTrust is a revolutionary Airport ID Pass Application vetting and issuance solution, hosted in the Cloud. It provides streamlined ID Pass management with absolute certainty of identity and powerful tools to transform the Airport ID Centre performance.

MTrust has provided the ID Centre with a raft of workflow, communication, security and compliance tools to reduce the administrative overhead allowing agents to concentrate on security and the issuing of passes.



MTrust provides a personalised dashboard and inbox for each team member that enables them to see what is happening, right now. The Dashboard provides updates on team bandwidth, application progress and ensures that fast-track passes remain at the top of the team’s lists.

For the Authorised Signatories, MTrust gives complete visibility of an application’s progress and removes the need for calls to the ID Centre. MTrust allows workers to create their own profile prior to submitting a pass application. Upon completion, the Authorised Signatories import this information into the MTrust online pass application forms, ensuring accurate data and applications are correctly completed, first time.

HRS also undertook the training of the Authorised Signatories at the Gatwick ID Centre. Delivered in tailored training sessions to over 800 Authorised Signatories across 6 weeks, split across company and pass type. Training was reinforced by the creation of online Training Videos that are available 24/7 within the MTrust system.

The Results

In January 2015, Gatwick became the first airport to have a paperless process for issuing its Airport ID Passes.

As of February 2015, MTrust has delivered the following results for Gatwick:

- 11,600 applications processed in first two months
- 93% Approved with just 1.4% rejected and the rest in progress.
- All application types have been processed; company, vehicle, people
- 71% of people within MTrust have profiles that can be used again in the future
- Gatwick have been able to reduce their SLA for responding to initial pass applications from 2 days to just 45 minutes

- Happy ID Community - 95% of the 2,500 Authorised Signatories say MTrust will give them better visibility of pass applications, reduce calls to the IDC and enhance security

MTrust has created a community of Airports, Authorised Signatories and Employees who are able to transfer and share information between them for mutual advantage. Over 800 companies have processed a pass application including leading on-airport companies such as British Airways, easyjet, Boots, Costa Coffee, Swissport, NATS and World Duty Free.

MTrust is also TUPE & Transfer Ready. Employees can apply to register their employment at multiple companies simultaneously, facilitating distributed workloads for quick, simple TUPE transfers and eliminating duplication of data where employees work for more than one employer.

Summary

Improving the Airport ID pass process is about more than simply automating the existing process. It's time to re-evaluate the process with 25 year young, not 25 year old eyes, rethink the entire process and improve for all, not just automate. The current paper based administrative overhead can swamp the true intent of the ID pass application process, Security – to assure the identity and suitability of the individual to work in restricted areas.

Systems such as MTrust provide greater visibility to the pass applicants and greater efficiencies to the ID Centre, automating the non-security activities to allow agents to concentrate on the security value add.

Airports, on-airport companies and other stakeholders need a new, community wide, solution that can create:

Improved Security through:

- Greater identity assurance of all applicants
- Cloud-based storage of information leading to greater information sharing across Airports to help standardise the ID pass process
- Personal data protected by class leading technology and managed by the individuals concerned
- Support BS7858:2012 standards for screening of individuals employed in a security environment
- By supporting BS 7858, systems can be extended outside of Airports to other secure critical national infrastructure environments

Improved Customer Service through:

- Ease of Use for applicants
- Significant reduction in time taken to issue a pass
- Complete process transparency for all
- Online and self service facilities

Improved Efficiency through:

- Pay As You Go, Software as a Service
- Significant savings to both the airport and on-airport companies from greater technology utilisation
- Cost savings to customers as a result of reduction in queues and process improvements
- Cost savings from the introduction of automated self service delivery

And that is exactly what we have created with MTrust.

References

1 Time To Think About Cloud Computing - InformationWeek, 22/10/2008
2 UK Companies Spend 18 Days a Month Maintaining On-premise Security Solutions - Webroot, 19/04/2011
3 Aberdeen Group
4 Protect Your Business from Cybercrime - Bloomberg, 05/07/2011
5 CPNI INSIDER DATA COLLECTION STUDY – Centre for the Protection of National Infrastructure, April, 2013