Innovative cloud-based passport issuance system

A cost-effective, secure approach for small and developing states

by Shelley Bryen and Steven Grant

In May of 2015, the very first cloud-based, Software-as-a-Service (SaaS) passport issuance system was deployed to six British Overseas Territories in the Caribbean. Will this be a one-off orphan system, or is it the first of many in a growing trend? In this article, Shelley Bryen and Steven Grant will examine the characteristics and components of a passport issuance system and their suitability for cloud/SaaS deployments as a way to make state-of-the-art technologies accessible for small and developing states.

Scattered around the Caribbean Sea and the North Atlantic Ocean are a group of six British Overseas Territories: Anguilla, Bermuda, Cayman Islands, Montserrat, Turks and Caicos Islands and the British Virgin Islands (see Figure 1). These self-governing Territories are under the jurisdiction and sovereignty of the British Crown. The Governor, usually a British Foreign Office Diplomat, exercises minimal power over local affairs and is more concerned with foreign affairs, defence and trade. The territories issue their own variant of the British Passport to British Overseas Territories Citizens.

Until very recently, these six British Overseas Territories issued their own, British Overseas Territories Citizen (BOTC), machine readable passports from local passport offices in each territory. Following consultations with the United Kingdom's Her Majesty's Passport Office (HMPO), it was decided that the Territories would introduce their own BOTC electronic passports in full compliance with the standards laid down in Document 9303 of the International Civil Aviation Organization (ICAO).[1] In the new process, the Territories continue to receive and process the passport applications and complete the entitlement and authorisation processes. However, in a significant change from past practices, the e-Passports are now being personalised by HMPO in the United Kingdom for both security and cost-effectiveness benefits. The personalised passports are then returned to the local passport office for delivery to the applicant.

This article will look at some of the technical details of the system deployed to these six Territories, and also consider if this type of solution could be deployed to other countries facing similar challenges, such as smaller volumes while wanting to issue e-Passports.

Major components of a passport issuance system

A passport system or any secure identification document issuance system contains the following key functional components:

- enrolment or data entry system
- entitlement or adjudication system
- printers and print management
- database
- server infrastructure

Enrolment or data entry system

An enrolment or data entry system can take many forms. It could be as simple as a data entry clerk or passport officer greeting a passport applicant and then manually typing their personal details into a data entry screen. Facial images could be live captured or scanned from a photo, and then checked for acceptable quality. Documentary evidence of identity, such as an expired passport, a birth certificate or proof of naturalisation, is examined and sometimes scanned for retention. Many countries require an interview for first-time applicants, suggesting additional data input screens are required to capture responses to questions. Increasingly, some or all of the passport application processes can be completed online. This is especially true for renewals of recently expired or about-to-expire passports.

Entitlement or adjudication system

This describes a decision support system where various databases might be examined for impediments to issuing a passport (for example, is the applicant involved in a court case?) or for identity confirmation (for example, does the applicant information match the civil registry?). The adjudicator may also review the applicant's passport history (for example, are there multiple lost passports?) before taking a decision to issue. Many of these steps are automated, however it

Shelley Bryen *has been the Marketing Director at WorldReach Software in Ottawa, Canada since 2009. Having worked in the technology industry for more than 20 years, Shelley has broad experience in marketing communications, strategic alliances, product management, marketing research and strategic marketing in embedded technology, consular systems and travel documents.*

Steven Grant, *P.Eng. is the Business Development Director at WorldReach Software where he is responsible for global sales of consular management software and passport and visa issuance systems. He has more than 15 years of experience in travel documents, biometrics and border security, and is a member of the ICAO TRIP Implementation and Capacity Building Working Group.*

biometrics 2016

18–20 October 2016 | London, UK

REGISTER BY 15 JULY TO SAVE ON DELEGATE RATES

Building trust in biometrics

DELEGATE AND VISITOR REGISTRATION NOW OPEN

3-day Conference

More than 60 expert speakers will include:

- **Gillian Tully**, *UK Forensic Science Regulator*
- **Richard Vorder Bruegge**, *Federal Bureau of Investigation*
- **Linda Champion**, *International Operations, Australian Federal Police*
- **Krum Garkov**, *Executive Director, eu-LISA*
- **David Ferbrache**, *Technical Director of Cybersecurity, KPMG*
- **Pam Dixon**, *Executive Director, World Privacy Forum*

Plus representatives from:

- CIFAS
- Dutch Ministry of the Interior & Kingdom Relations
- Grupo Santander
- Interpol
- Mastercard
- National Institute of Standards and Technology
- United Nations Development Programme
- US Department of Homeland Security
- International research and innovation centres






Identity management, trust, privacy and data protection

Secure transactions and consumer biometrics

Biometrics and forensics

Border management and law enforcement

Liveness detection and vulnerability assessments

Research and innovation

FREE EXHIBITION – 19–20 OCTOBER 2016 – FREE VISITOR REGISTRATION NOW OPEN

Organised by: ELSEVIER

In partnership with: Biometrics Institute

#biometrics2016

www.biometricsandidentity.com

"Professionally very relevant and topical; really good speakers who know their subject"

Previous delegate

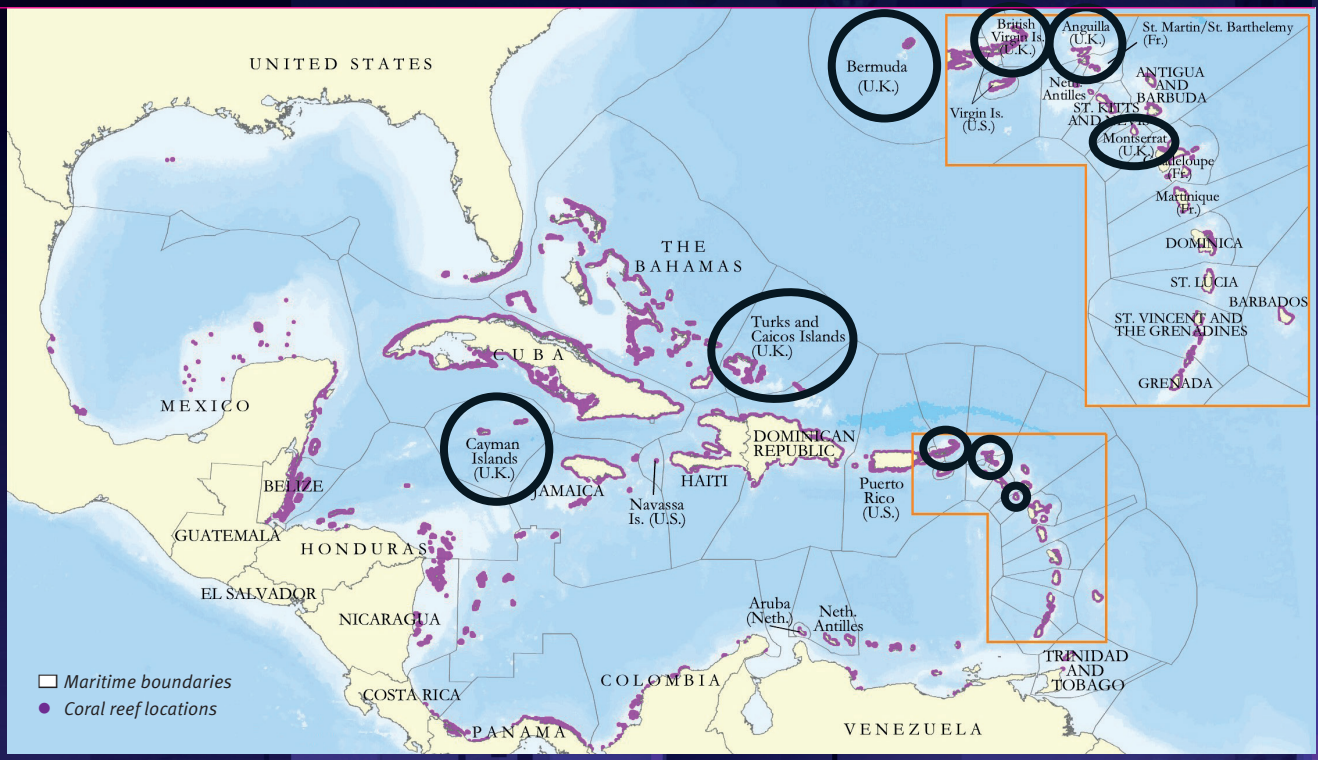

Figure 1:
The six British Overseas Territories.[2]

is quite common that a person is making the final decision to issue a passport.

Printers and print management
The personalisation and quality control of passports requires specialised equipment which is carefully selected for compatibility with the passport booklet. Depending on geography and passport issuance volumes, the print solution may be centralised in one location, or distributed. Many countries issue full validity and/or emergency passports from consulates and embassies.

Database
This corporate repository retains details of all passport applications (issued, refused, expired, cancelled, lost, stolen, etc.). It also contains the administrative details of the operation of the passport issuance system.

Server infrastructure
The various servers and networking equipment will need to be sized appropriately for the organisation and in accordance with any business continuity guidelines of the government. This may entail separate application and database servers, spare equipment, and a data management plan with off-site backup for redundancy.

Optional system components
There are also two optional system components for a secure identification document issuance system:

- biometrics subsystem
- document signing system

Biometrics subsystem
As a fraud prevention tool, many governments have incorporated one-to-many facial and/or fingerprint matching systems into the passport issuance workflow. By applying deduplication techniques, it is possible to determine if any person has applied for or attempted to obtain more than one passport using different identities. For passport renewals, the technology can be used to determine if the applicant is in fact the same person to whom the previous passport was issued.

Document signing system
More than half of the ICAO member states are now issuing e-Passports containing an integrated circuit chip. For those countries a Public Key Infrastructure (PKI) with document signing capability is required in order to make full use of the digital security features available with e-Passports.

Overseas Territories issuance system
The new passport issuance system is deployed by WorldReach Software to the British Overseas Territories.[3] It is a hybrid system, which means that it is a combination of different cloud models (for example between public, private and community clouds). This approach was chosen to take advantage of the cost-effectiveness of supporting the common issuance components between all Overseas Territories, while benefiting from the security of a UK-based cloud (delivered by Skyscape Cloud Services, a specialist provider dedicated to the provision of assured cloud

services to the UK public sector). All of the system components described above are included, with the exception of the biometrics subsystem. One unique characteristic of the system is that the passports are personalised – and the chips electronically signed – within the United Kingdom by HMPO on behalf of the six Territories. The issued passports are a variant of the UK passport. They are unique to each Territory.

Printers are nonetheless still needed locally. In the past, none of the Territories needed to issue special emergency passports. If a passport was needed urgently for a medical evacuation flight for example, an ordinary passport was issued quickly, often after hours by on-call staff. With e-Passports being personalised in the UK, this is no longer possible. The new system includes the capability to locally issue 8-page emergency passports on an urgent basis when required.

Cloud-based components

One of the unique characteristics of the system is that the enrolment and entitlement functions are performed locally in each Territory. Subsequently, the e-Passport personalisation and document signing takes place in the UK. Another notable characteristic of this system is that, with the exception of the local printers for emergency passport personalisation, all other major system components are cloud-based: the enrolment or data entry system, the entitlement or adjudication system, the database and the server infrastructure, including backup and redundancy.

Risk mitigation

Understanding that the odds of having no unplanned outages for the system life (whether locally installed or hosted on the cloud) are very low, it is important to have a risk mitigation plan. This system also has a 'standalone' capability to print a passport offline if internet access is down.

Local users in each Territory access the system via secure connections over the public internet. Despite the very long distances involved with an ocean between the client PCs and the servers hosting the system, performance has been excellent. The hosting infrastructure based in the United Kingdom has proven to be very robust with zero unplanned outages since the system went live in May 2015.

Advantages and disadvantages of cloud hosting

According to The Public Cloud for e-Government Report by the International Journal of Distributed Systems and Technologies, one of the main advantages of using cloud-based hosting for e-Government systems is cost-effectiveness.[4] Public agencies do not have to spend their limited budget setting up their own cloud or IT infrastructure. In addition, costs can be saved due to lower maintenance demands such as operating system updates or security patches of the environment. The cloud also offers high availability, high elasticity (or scalability in peak times) and in many cases much more redundancy than most governmental agencies can put into place effectively. This is particularly useful for smaller countries and island territories where a national disaster could affect the whole country.

Disadvantages can sometimes include challenges regarding the compliance with legal regulations, such as data protection constraints. In some regions, such as the EU, a country's legislation can forbid sensitive data storage in countries outside the region. This is something to consider closely when choosing a cloud vendor and the location of the cloud site. Furthermore, governments must contend with having less control of the infrastructure and treatment of data, but this can often be addressed through contracts or agreements. Customisation of cloud services and cloud-based applications can also be an added expense, given that the underlying business concept of the cloud relates to taking advantage of economies of scale of commonly used components supplied to many clients. Many customisations can also lead to some kind of dependency to the cloud service provider in which switching (for example data migration) can be more expensive than staying with the vendor.

Table 1:
Evaluation of public cloud computing in e-government.

Advantages	Disadvantages
No infrastructure and set-up costs	Compliance with legal regulations
Low maintenance costs and effort	Less control
High availability	Expensive customised services
High elasticity	Dependency to provider

Availability of secure cloud-based systems

The private sector has been using the cloud for mission-critical systems for some time now. ERP systems for just-in-time supply chain applications, and even HR management systems are commonly found in the cloud. Many of these are not dedicated systems hosted in the cloud, but are multi-tenant true Software-as-a-Service deployments of a common software platform. Looking at the building blocks of an e-Passport issuance system, many of the key modules are already available in the cloud:

Biometrics subsystem

Multiple vendors offer Biometrics-as-a-Service products with enrolment, biometrics image quality control, matching and biometric storage in the cloud. Speed of deployment and lower capital investments make these systems very attractive to potential clients.[5]

Document signing

The PKI system used for the Country Signing Certificate Authority (CSCA) and Document Signer (DS) is a complex subsystem. The availability of a cloud version has been described since 2012 or perhaps even earlier.[6] There are already multiple instances of cloud-based PKI systems being used to sign documents for national governments and international organisations.

ICAO Public Key Directory

The ICAO Public Key Directory is the database maintained by ICAO holding national cryptographic keys related to the authentication of e-Passport information. This data sharing mechanism was established by ICAO to enable participating states to publish their public keys without the need to establish bilateral agreements with all other e-Passport issuers (and receiving states). It resides in the cloud.

Cloud-based passport issuance system for other countries

Passport issuance systems are expensive, and e-Passport systems even more so, particularly for countries issuing low volumes. The alternative to a cloud-based system would have required conventional on-premises hardware installation, with all the support and maintenance that entails. The costs would have been compounded by the need to provide even modest provisions for business continuity, because being unable to issue passports for an extended period of time due to a system failure is not acceptable for a critical government service.

Collectively, the six British Overseas Territories participating in the project issue well under 100,000 passports per year. Many countries and territories which issue fewer than 300,000 passports per year could benefit from a cloud/SaaS-based passport system.

Although ICAO does not require that countries issue e-Passports – it is currently a recommended practice – many countries feel compelled to do so in order to keep up with their neighbours and improve security. Some countries believe their passport will be more respected and more widely accepted if it is an e-Passport, such as for access to visa waiver programmes of other countries. This is perhaps partially true, but there are many factors considered by receiving states when establishing visa policies, the security features and integrity of a country's passport system being only one factor.

At a recent ICAO event, several small developing states pleaded their case for ICAO to leave e-Passports as non-mandatory, due the additional costs and complexities involved which these states are unable to absorb. Perhaps a cloud-based system is an accessible, more cost-effective way for these countries to go about it. This is particularly advantageous when combined with an e-Passport personalisation provider also operating on a fee-for-service model.

Figure 2:
Each passport is unique to each Territory, personalised by HMPO.

References

1 *International Civil Aviation Organization – ICAO (2015). Doc 9303: Machine Readable Travel Documents. Current version: seventh edition.*
2 *World Resources Institute: The Caribbean Region Map. http://www.wri.org/resources/maps/caribbean-region Accessed on 31 March 2016.*
3 *WorldReach Software secures SaaS-based passport-issuance clients. http://www.securitydocumentworld.com/article-details/i/12026/. Accessed on 31 March 2016.*
4 *Zwattendorfer, B. and Tauber, A. (2013). The Public Cloud for E-Government. International Journal of Distributed Systems and Technologies, Vol. 4 (4), pp. 1-14. http://www.irma-international.org/viewtitle/104714. Accessed on 31 March 2016.*
5 *Fujitsu Biometrics-as-a-Service. http://www.fujitsu.com/us/services/application-services/saas/biometrics-as-a-service/index.html. Accessed on 31 March 2016.*
6 *Kumar, V. (2012). E-MRTD PKI Trust: Software-as-a-Service. http://www.icao.int/Meetings/mrtd-symposium-2012/Documents/10_am_Entrust.pdf. Accessed on 31 March 2016.*