Making the most of the Digital Passport

Thank you Vijay. Good afternoon everyone.

As you've heard, my name is Stephen Gee, and I'm from the Australian Passport Office.

Every year, we churn out 2 million fancy little booklets for Australian citizens containing their vital statistics and an unflattering photo.

We issue these booklets as 'ePassports'. We were one of the first countries to do this, and we started way back in 2005.

Despite how much time has elapsed since then, most Australians still have no idea what an ePassport is.

Sure, an ePassport is a fancy little booklet with your vital statistics, an unflattering photo *and* a silicon chip. A silicon chip in a computer or a gadget is something that people understand. But what does a chip in a *booklet* do?

The answer is, as we've heard over the past few days, is that it does some pretty useful things. But it can also do some things that are really quite exciting – things we haven't we yet talked about at this conference.

In the Australian Passport Office, we've realised this for some time.

Other parts of our government, and partners in industry, are now also starting to grasp that the packets of information stored on humble passport chips are an identity verification tool so powerful they could change, for the better, some of the basic ways in which international travel works.

To capture the essence of this idea, we've started calling it the 'Digital Passport'.

It's a simple concept.

There are three components. The first two will be familiar to you. The third might not.

The first component is what a passport chip does.

A passport chip stores information in an easy-to-read format.

At a minimum, that information is

- the data from the passport's machine readable zone (MRZ) and
- a copy of the facial image, in jpeg format.

To see this data, all you have to do is place a booklet on an electronic reader. Readers are commercially available and not expensive.

There are even – and this is important – mobile phone apps that can read information in passport chips.

The second component of the Digital Passport is that we *write* this information using advanced encryption technology that allows any reader to be sure that:

- the information was written by us
- the information hasn't been altered.

The information and its encryption are wrapped up together in what is known as the Logical Data Structure, the LDS.

And the thing is this. There's a sense in which the LDS is your *real* passport. It's the LDS – and *not* the data page in the booklet – that our immigration colleagues authenticate when you cross the border into or out of Australia.

It's the same in many other countries.

Because of its encryption, the LDS is a uniquely secure form of digital identity.

In fact, it's much more secure than anything else in the booklet.

Data pages come with dazzling security features – special inks, intaglio printing, holograms, optical variable features and so on. They're difficult to defeat. But people can try to alter data pages, and although it's difficult and expensive, it can be done in ways that are hard to detect, and people do get away with it.

But if someone changes just a single bit of data on an LDS, even if it's just one pixel in that unflattering photo, a reader can electronically tell that tampering has occurred.

And if someone tried to forge an entirely new LDS, electronic authentication would show instantly that the data hadn't been written by a passport authority.

The third component of the Digital Passport, and the key to what makes the concept so special, is *portability*.

We store the LDS on the chip as a single file with the passport number as the filename.

It's very small – only about 50kb.

And because it's a digital file, it can be transmitted electronically, *separate from the booklet,* without losing any of its security features.

Which means it's possible for people to send and submit their passports digitally, as well as in physical form.

At the moment, people take photocopies or scans of the data page. But these lack the security features of the LDS, and they can be manipulated.

At the moment, airlines manually swipe MRZs for Advanced Passenger Processing.   But MRZs don't contain the images that immigration authorities need to match a passport to a real live person.

At the moment, people manually enter their name, date of birth, passport number and passport expiry date into visa forms, to which they might staple a photo. Often they get the details wrong. They have fat fingers, or they use a different style for their name, or they get the day and the month around the wrong way. Which means authorities can't be confident that the data in visa systems are an exact match for what's in the passport a traveller will actually present.

The Digital Passport has the potential to solve these problems.

Imagine. A traveller needs a visa. The traveller uses an app on her phone to harvest the LDS in her passport and send it instantly to immigration authorities in the receiving country.

It's as if those authorities were *already holding the person's passport in their hand*.

They electronically generate a visa form for the traveller to complete, in which the passport information is already filled out correctly and verifiably.

No misprints by applicants are possible. And because authorities already have the actual passport photo, there's no need to submit a separate photo to go with the visa form, or for the visa authority to follow up to make sure that photo is of good quality.

When the traveller lands, immigration authorities have already matched her LDS to an Advanced Passenger Information record and know when to expect her.

She doesn't have to show her passport at the border, because as she proceeds through automatic immigration gates, facial recognition technology matches her to the passport the authorities already hold in secure digital form.

Airports and airlines could profit from the same technology.

They could harvest an LDS at the time of booking, or at online or physical check-in, replacing the MRZ swipe.

An image of the traveller could be taken and matched electronically with the image in the passport, generating a token.

Facial recognition technology could then securely open the traveller's way through bag drop, security and boarding, with no need for the traveller to keep showing his passport at each new stage.

There would be no need for boarding passes – and no more problems from boarding pass swaps, because you can't swap something you don't have.

Immigration authorities are conducting Digital Passport trials at airports in Australia. We at the Australian Passport Office are assisting.

Australian airports are also conducting trials.

Some airports are already thinking about how they incorporate the Digital Passport into the design of new terminals, through which passengers will flow differently to how they do now.

There are other trials elsewhere in the world. The one with the funkiest name is the famous Aruba Happy Flow.

But this is not about using cool technology just for the sake of being hip.

There are three quite concrete considerations:

- the potential for *cost savings* from automated border clearance
- the increased *security* that comes from processing travellers by means of a consistent algorithm that doesn't get tired or distracted
- the *commercial benefits* that airports can reap from heightened traveller satisfaction.

The Digital Passport also offers benefits for the wider economy. It opens the way for more secure online identity verification for citizens' dealings with government, with business and with each other.

Part of the beauty of the Digital Passport is that the infrastructure already exists.

There are more than 700 million ePassports in circulation.

As we heard yesterday, the LDS on 98 per cent of them has been configured in a way that means they can be verified against the standard in ICAO Doc 9303.

And the ICAO public key directory supports the system that makes authentication possible.

The challenge now is that there are no standards for how the Digital Passport is *used*.

Different vendors offer different solutions to different airports.

Border authorities in different countries may end up using the Digital Passport with systems that can't speak to each other.

That may, or may not, matter very much. But there could be issues and misunderstandings.

The Digital Passport works most securely if photos are of biometric standard. That's why they have to be unflattering.

Authorities might simply try to attach passport images to other information, thinking they would be achieving the same thing as using the LDS.

Designers of systems for using the Digital Passport might not realise the importance of programming in a few extra fractions of a second to *authenticate* LDS data.

And travellers might think the Digital Passport replaces the booklet and start leaving theirs at home. Which would be a bad idea. People will still need to carry the little booklets around for a long time yet. They just won't have to keep pulling them out and showing them so often.

This will be better for them, and for everyone.

The potential fiscal, security and commercial benefits of the Digital Passport are big.

It's taken 12 years, but the technology that's been sitting in the world's travel documents since 2005 is finally being understood. The test now will be to make the most of it.

____

ICAO Traveller Identification Programme Regional Seminar
Hong Kong
12 July 2017

Stephen Gee
Assistant Secretary, Passport Policy and Integrity Branch
Department of Foreign Affairs and Trade
Barton ACT 0221
Australia
Tel: +61 2 6261 3075
E-mail: stephen.gee@dfat.gov.au

Check against delivery