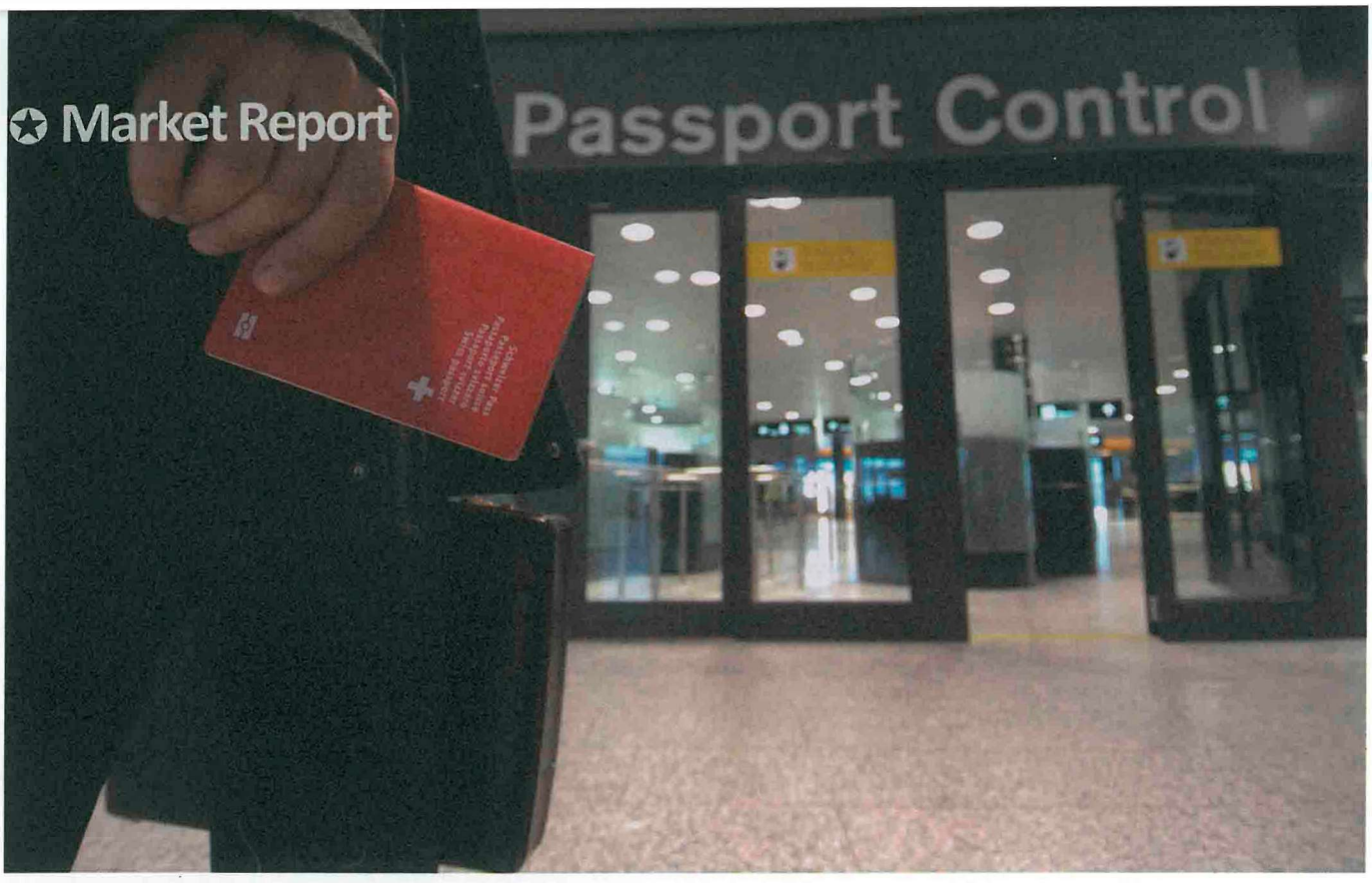
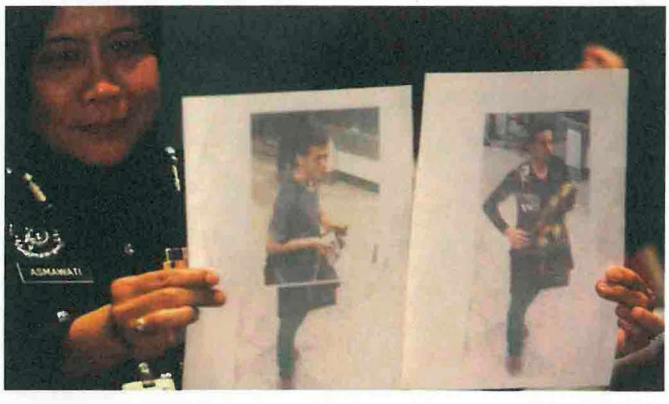


Identity Matters:
How Technologies Impact Identity Management in the Decades to Come

In 2014, we saw significant events that might have an impact on identity management in the years to come.

by Ir. Prof. Raymond Wong

On 8 March 2014, the sudden disappearance of the Malaysian flight MH370 attracted so much attention to identity management following the discovery that two passengers boarded the plane by means of fraudulently obtained passports. The incident has once again drawn the attention of the travel industry to the topic of how to accurately identify a person in a trustworthy manner, so as to facilitate welcomed travel (e.g. visitors) while maintaining a high standard of security amid globalisation and rocket-shooting number of passenger movements.



In the latter part of the year, the popularity of ePayment using biometrics together with mobile devices, like Apple Pay, Alipay, etc. has prompted many industry players to pop the question: are we entering an era of payment revolution just like the introduction of credit card some five decades ago?

Identity concern is never a new subject. However, in no time before are we so keen to ensure the genuineness and trustworthiness of a claimed identity. Security is one of the main driving forces. Technology advancement, rising accuracy of biometric recognition system, popularity of smart phones and mobile devices, etc. also add to the fuel.

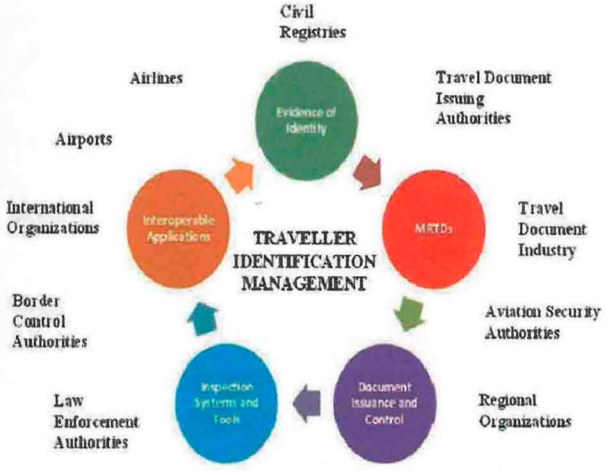
Trustworthy Identity Document for Identification

Hitherto, an identity document is normally required for identification of a person. It serves an important purpose: it tells the personal particulars of the holder, including name, sex, date of birth; a photograph of the holder representing the true likeness of the person so that the identity can be positively and easily confirmed.

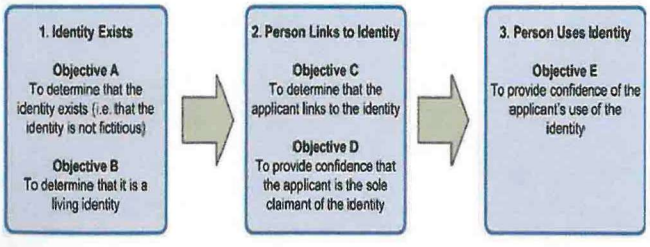
For this purpose, identity documents have to be issued by trustworthy authorities having the legal authority in its own country. To ensure it is recognised as a trustworthy one by the third parties, both macro and micro issues have to be addressed.

From the macro perspective, it entails a comprehensive life cycle about an identity management mechanism of persons and a comprehensive national register on persons. The following model (Sjef and

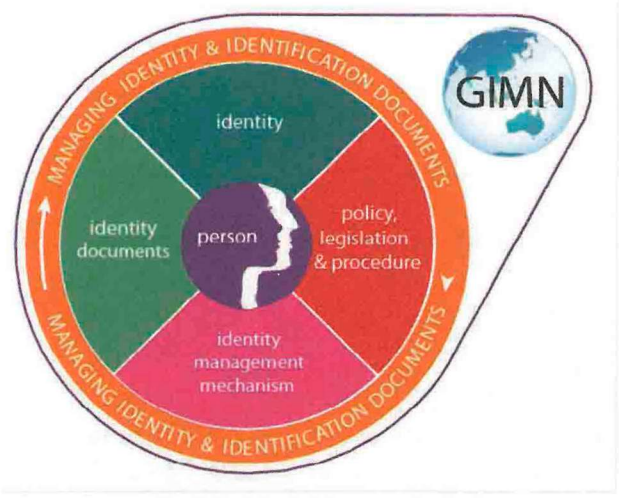
)ICAO TRIP



Components of ICAO TRIP



The links of an identity under ICAO TRIP



GIMN stands for global identity management network

Raymond Model: Keesing Journal of Identity and Document, Annual Report, 2010) illustrates the host of issues to be taken care of.

International Civil Aviation Organisation (ICAO) of the United Nation in early 2014 introduced the Traveller Identification Programme (TRIP) Strategy. The concept, in simple terms, is to ensure the identity of a traveller to be established and linked in all related aspects instead of just looking at the face information of the identity document alone. This echoes the gist of the Sjef and Raymond model.

On the micro side, there must be a fault proof and credible breeder document cum identity document enrolment system: a trustworthy database on registrants without duplications or mistakes, and most important of all, a secure identity document with necessary security features protecting the card from being forged or tampered with, etc..

Identity Document as a Token for Records

The identity document in fact serves as a physical token for the enrolled personal records maintained by designated and competent authorities in the said country. The token tells a story about the holder. A trustworthy one will normally be accepted by the one checking it without resorting to the issuing authorities or worrying about the cogency of the information stored therein, i.e. the story about the holder.

In case there is any doubt on the genuineness and credibility of the document or the identity behind the document (for example, cases of suspected forged document, imposter, etc.), the authorities responsible for the issuance of the document have to be consulted for verification.

Identity document nowadays include identity card, passport, driver licence, etc. These are well accepted token of the holder's identity for identification purpose.

Electronic Identity Documents

With the advent of technology, many identity documents have incorporated an integrated circuit chip or radio-frequency identification (RFID) technologies. These type of electronic documents enable digital storage of personal information, without limiting to traditional personal biographic data like name, sex, date of birth and photograph. Biometrics of the holder like fingerprint, iris information, etc. are also included. The electronic devices also allow advanced digital encryption of personal information, protecting them from being tampering and accessed without unauthorisation. Examples of these identity documents include smart ID cards, electronic ID cards and electronic passports.

Despite the wide application of electronic elements in a traditional physical identity document, the document itself still serves as a token for access to the backend records. In other words, a physical token is still needed for identification purpose.

The Impact of Emerging Technologies

Electronic ID card

With fast developing information and communication technologies (ICT) in recent years, we have seen innovative applications of electronic ID card for value added services (i.e. services other than traditional identification function). Examples of these add-on services include using the card for mobile identification purpose as in the Estonian eID card or using it with banking facilities like the Malaysian Mykad and German eID card. In these cases, a physical card with tailor-designed electronic elements, both hardware and software, is always required for specific applications.

Hong Kong has recently announced that a new generation of smart ID card with latest technologies and capabilities will be introduced in 2018. It will be interesting to see how new and innovative applications will be brought forth by this new electronic ID card.

Electronic passport

Electronic passport has come into play for 10 years. Over a hundred countries have already introduced it, some of which even in its second generation. Industry players estimate that about 75% of passports in circulation in 2016 will be in electronic format.

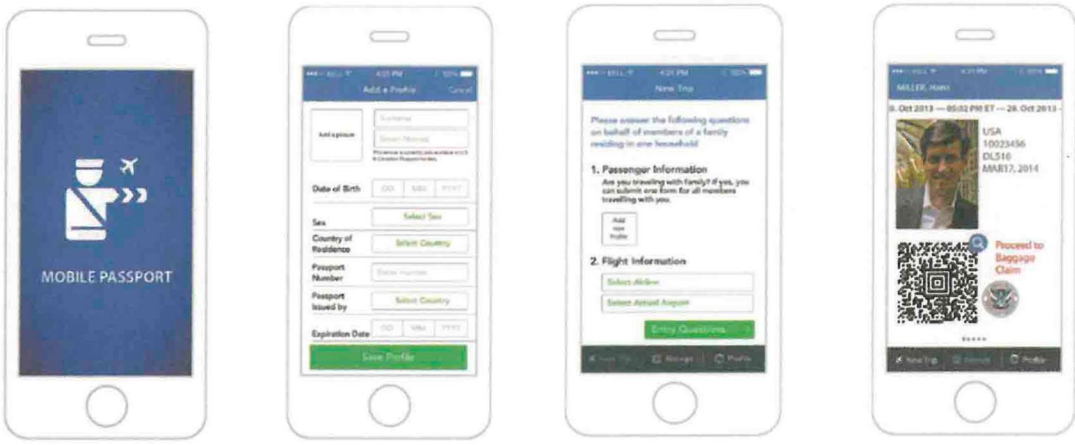
There are rising needs to check personal information (both biographic and biometric) stored in the chip of ePassport by border management agencies, for example, using Automated Border Control Systems for both citizens and visitors holding ePassports to ensure more secure identity verification as well as for facilitation purpose,

Likewise, the ICT system, both hardware and software, deployed at checkpoint counters will become more sophisticated, feeding counter officers with all useful information from various sources, including but not limited to, ICAO Public Key Directory (PKD), the Interpol databases, shared data among countries, big data analysis and so forth. The objective is to empower counter officers with all available information about the identity of the document holder in front of the counter, enabling the former to make an informed and wise decision within seconds whether to allow the entry of the visitor or not.

Combining eID and ePassport into one Single Identity Document

From a user's perspective, one will query why one has to carry a thick passport and not just a simple card for all these purposes. This indeed is a justifiable request. For many years, we are not required to carry a bank book for banking services anymore. With the advent of smart devices, wearable devices together with state-of-the-art ICT systems, there must be a way to turn the thick and paper based passport book into a more innovative token.

The Chinese government has taken a big step forward in this aspect by introducing a new form of Entry / Exit Permit for Chinese nationals travelling to Hong Kong and Macau since May 2014. This document, previously in the format of a passport book, has been redesigned into a smart ID card. It contains all necessary information for identification and travel purposes, including, inter alia,



source: US Customs and Border Protection website

biographic and biometric information of the holder, eVisa information, movement records (five most recent ones) etc. The card has received widespread applause from users and immigration authorities in China, Hong Kong and Macau since its launch. The significant and immediate benefit to the card holders and the authorities is that holders can make use of the card for self-service immigration clearance through the Automated Border Control system in China, Macau and Hong Kong. They do not have to queue up at the conventional immigration counter for examination and stamping. Processing time is significantly shortened.

This is a vivid example demonstrating the direction of identity document transformation in the years to come.

Mobile Technologies and Related Applications

Similarly, the rapid development of smart phone and tablet together with associated apps has also triggered discussions on whether a new era of identification has arrived.

On 11 August 2014, US Customs and Border Protection (CBP) announced the launch of an app which expedites a traveller's entry process into the United States. The app, Mobile Passport Control (MPC), allows eligible travellers to submit their passport information and customs declaration forms via a smart phone or tablet prior to CBP inspection. The process comprises just a few simple steps:

- Download the MPC app from the Apple App Store prior to arriving at the custom
- Create a profile with the passport information of the holder
- Complete the "New Trip" section upon arrival at the United States
- Submit the customs declaration form through the app to receive an electronic receipt which comes with an Encrypted Quick Response code. This receipt will expire four hours after being issued
- Bring the passport and smart phone or tablet with the digital barcode receipt to a CBP officer
- The above flow is illustrated in the diagrams below

This smart phone app does not replace the need for an identity document since inspection of passport by the United States CBP officer at the checkpoint is still required. The app just facilitates or speeds up the border control process. However, it does echo the prediction that mobile apps will sooner or later invoke a revolution or transformation of identity documents.

Other than smart phone, there is also a rising use of wearable technologies and ubiquitous computing for personalised services and person tracking / surveillance in airports. For example, applications of iBeacons have been introduced by airlines (like American Airlines, Japan Airlines, Qantas, etc.) and airports for interacting with and empowering passengers at airports. These applications include way finding, staff tracking etc. It is believed that with increasing popularity of iBeacons, wearable technologies (like smart glasses, smart watches), in-house wi-fi based tracking solutions, etc. will be taking a giant leap towards creating a digitally-enabled and personalised applications for travelling purposes.

With the drive of electronic payment (ePayment) by means of biometrics, like Apple Pay, AliPay, etc. through mobile devices, it is forecast by the financial sectors that we have entered another payment revolution like the introduction of credit cards some fifty years ago.

Japan Airline staff equipped with smart watches enabling the control desk tracking their whereabouts using iBeacons (source: Future Travel Experience)

In China, smart phone apps have been adopted by hundreds of millions of people for a wide range of daily activities including information collection, reservations, shopping (including real estate property), taxi booking, etc. The popularity of using mobile apps to make purchases even drove internet sale in China on 11 November 2014 (Singles Day in China) to a record high of US9.3 billion through Alibaba's Tmall and Taobao.

Smart Devices and Biometrics Replacing Identity documents

There have been propositions by a few service providers in Europe for a 'Person token' or 'Human token' approach in airports whereby identity documents, tickets, boarding passes, etc can be got rid of so as to process passengers quickly and securely. The envisaged process will make use of integrated ICT applications like biometrics, self-service check-in kiosk and luggage drop kiosk, Automated Border Control systems, eBoarding gates, mobile access to services, etc. It puts passengers at the heart of the operation and a shared customer is to be focused on and cared for by all parties at the airport, including airlines, border control officials and other parties involved.

Trial runs of these initiatives are being planned and are regarded as one of the top-on-the-agenda visions for future airports.

Challenges

It is difficult, if not impossible, to predict when and how new electronic and ICT applications will be replacing a physical identity documents (or token) for identification purpose. Technologies are just developed every minute and are transforming, prompting a total rethink of the traditional processes. We have seen many examples in which new technologies are turning impossibilities to 'can dos'.

Instead of trying to predict what technologies will be coming up for identification, it is more important to examine critical issues of the basic functionalities that these new technologies should achieve for the purpose.

Security of personal data

The obvious challenge is security concern. Personal information is very important data concerning privacy, security and facilitation. Any unauthorised or abusive use or tampering of the information shown in the identity document or token by unauthorised party or even by the data subject without proper authority will defeat the whole purpose of identification. The crux of the issue is therefore the 'trustworthiness' of the personal data so displayed by the token, physical or digital, or a combination of both. How secure is the information protected from abuse? How accurate is the information representing the records in the database? These are just some of our concerns.

Storing personal data in a mobile device is never a secure and the best approach. Any security protection, including very secure encryption, is vulnerable to attacks. The best way to protect our personal data is to have it securely stored in a backend system or even in a virtually closed system. The information so stored in the database should not be casually released or in fact not be released at all to any outside party.

Human token

The 'person / human token' now being studied is one direction in addressing this challenge. The biometrics of a person, once enrolled by the competent authorities, will be stored in a secure backend system and will be used for accurately verifying a person's identity in an effective way. A traveller's biometric information, including face, fingerprint or iris, or combination of all or any of them, will be useful for identity identification (one-to-many in the whole database) or identity verification (one-to-one after the input of simple unique identifier) with the database maintained by competent authorities, given the state of play of available technologies. Presenting a physical identity document will not be necessary. It is only a matter of investment in technologies for quick, secure and accurate transmission of information among the parties involved. Rather than a technology issue, the feasibility of this 'person or human token' approach is more about management and legal consideration.

About Writer:

Professor Raymond Wong is the Adjunct Professor at the Biometric Research Center for the Hong Kong Polytechnic University. He was former Assistance Director with the Immigration Department of Hong Kong Special Administrative Region (HKSAR) where he served for 35 years. At the HKSAR, Raymond was instrumental in the development and management of information systems helped pave the way for numerous developments within Kong Kong's identity management systems. Since retiring from the government, Raymond has been serving as independent consultant for countries around the world on projects on identity management issues including, biometrics, identification documents, automated border control systems, etc. He also leads research projects on innovative technologies as well as authoring specialist articles and eBooks. He is acknowledged as one of the world class experts in relevant fields.

The beauty of the 'person / human token' is that the personal information is not stored in any media or token. This has alleviated the problem of forgery of the document or token. The person is using just his or her biometrics as a token for identification purpose. Forgery or tampering is very difficult though, if not impossible. With appropriate design, the system does not have to divulge any information to outside parties. All it has to do is to confirm whether the biometrics submitted by the person is in fact referring to the one stored in the database.

Other than for travelling or immigration purposes, the 'person / human token' concept can also be technically applicable for ePayment purpose over the internet in a similar way, provided that there are some forms of secure communication between the registration authorities, financial sector, retailers and consumers. Likewise, this will be more a complex management and legal issue rather than a technical issue.

Risk of fraudulent attempts

The challenge of using 'persons / human token' or a token through smart or mobile device for identification purpose is how to ensure personal information presented is in fact submitted by the data subject (the person in question) at the time of identification. It is necessary to ensure that all data or personal information used for identification purpose is indeed submitted by the data subject himself or herself and not by any other person, or it is not done through using any fraudulent means like wearing masks, wearing neo-real fake finger cover, etc. for the purpose.

Despite counter-measures like Presentation Attack Detection (PAD) devices, the 'persons / human token' approach will predictably be subject to a lot of fraudulent attempts. These include presentation attack, imposters, identity faults at various stages of enrolment, double / multiple identities (depending on the credibility of the trustworthy identity management system), insider frauds (abuses, corruption, carelessness ...), illicit attempts, etc.

In some cases, surveillance system through cameras, CCTVs or human supervision may help. The whole operation shall be a well-designed and integrated system. The challenge is how to integrate various state-of-the-art technologies to make the whole process a proven and fraud-proof system for the purpose, particularly when financial interest is involved. It is interesting to see how technologies development in the years to come solve this problem.

The need for a physical identity document

The 'person / human token' approach will likely be a possibility for replacing a token of identity or identity document for identifying a person within a designated region or a country domestically. The identity verification process can even be sped up if some simple tokens are used (for example, a unique token provided by an app of a smart device which is not for identification purpose but just uniquely pointing to the relevant records in the database for quick one-to-one verification). Likewise, the 'person / human token' approach should be viable in domestic travel or within a particular region like EU where there is no limit of stay for a specified group of persons or standardisation of personal data is not impossible.

This approach will be difficult for universal application given the different operational and security requirements among countries with varying culture, value and standards. Thus, some forms of a trustworthy token for identity, for example, the passport or a passport card, should be still required in future. Of course, with fast emerging technology and possible standardisation by ICAO, any impossibility can become a reality.

No doubt, a physical identity document is always the best way during system failure or outage to ensure business continuity. It is therefore likely that a physical document with state-of-the-art security features and design or a simple token of identity (physically, electronically, or a combination of hardware and software application like mobile app) will be still in place for the next decade for the convenience sake. This will also allow more time for discovery or development of a more innovative and revolutionary approach for the ultimate goal: quick identification of a person in a trustworthy and irrebuttable way. IDM