

IDENTITY MANAGEMENT - CHALLENGES AND OPPORTUNITIES FOR COOPERATION

KEY NOTE ADDRESS

I would like to welcome you to this workshop to look at the challenges and opportunities in our region for cooperation in dealing with the issue of identity management.

This workshop is part of the Bali Ad Hoc Experts Group II process, which authorises us to take practical steps to implement the recommendations of the Bali Ministerial Conference. These recommendations include that countries should work towards arrangements to share information and intelligence. The recommendations also include that countries should consider ways to cooperate on border management and visa systems management.

The aim of this workshop is to provide an opportunity for you to make contact with your regional counterparts in immigration, border control and national identity agencies and to exchange information about dealing with identity management.

The workshop will, I hope, be a first step in exploring opportunities for cooperation - where you can exchange information about how you identify who is entering, remaining and departing your country - how regional cooperation might be initiated, maintained and improved - and how international standards might impact on these processes.

What I hope we will achieve is the exploration of opportunities for regional and international cooperation in dealing with identity management as well as the potential for cooperative approaches to capacity building.

You represent a diverse range of countries and agencies and I am sure you have a diverse range of opinions about this subject. I look forward to your sharing your opinions and your experiences with your colleagues in this workshop.

Identity management is an important challenge for all our governments - for our immigration agencies, our law enforcement and intelligence agencies, our social welfare agencies, our judicial processes. Effective identity management means we have to deal effectively with the crime of identity fraud.

What do we mean by identity fraud? In essence, it is the use of a false identity for an unlawful, purpose. Identity fraud could be the complete theft of another person's identity or the invention of an identity or the use of fraudulent identification documents or information to alter some parts of the person's own identity - they might be using their own name but have fabricated some parts of their history or citizenship or personal details. The crime of identity fraud is committed by a range of people - from the members of organised crime syndicates to individual opportunists - for a range of reasons.

One of the most obvious reasons that a person commits identity fraud is to obtain benefits - often financial - to which they are not entitled - such as making social welfare claims, misusing credit cards, evading tax, defrauding the bank and falsely receiving mail (such as cheques).

However, identity fraud is also a central part of many crimes that are committed across national borders - generally by organised crime groups - such as drug and people trafficking, gun running, people smuggling, money laundering and terrorism - either to fund the crimes or to commit the crimes.

As such, there is a definite link between identity fraud and our immigration and border control processes. Perpetrators will take advantage of ineffective immigration and border control systems, especially if these are combined with ineffective or non-existent identification systems, to disguise who they are, when and how they entered the country, where they live, where they have been and why they are here.

In the immigration and border control context, individuals and organised crime groups commit the crime of identity fraud for many different reasons. What they choose to do will depend on their reasons for needing that false identity, for example -

- they might steal a passport - or they might obtain a passport by providing false information about themselves or bribing the issuing authority - or they might alter an existing passport or they might completely forge a passport. Their aim is to take on a new or significantly altered identity in order to get past a country's border systems or to apply for an entry visa which they know they wouldn't get if they used their real identity;
- for the same reasons, they might steal and alter a passport that contains a genuine visa - or they might obtain a visa by providing false information - or they might take a visa from one passport put it into another one - or they might completely forge a visa;
- they might destroy all their identity documents - often at the border - so that it is difficult or impossible for officials to know who the person actually is - often in order to claim protection or asylum;
- they might include in their passport, visa or identity documents a false family member - perhaps for criminal purposes related to prostitution or paedophilia;
- they might enter the country illegally and then take on another identity - by stealing someone else's documents or obtaining fraudulent identity documents - often to get access to goods and services they are not entitled to or to escape the notice of the authorities - perhaps in order to participate in terrorist or other criminal activities.

There are many ways of entering a country illegally - swapping boarding passes before getting on an aeroplane, obtaining multiple sets of identity documents in different names - possibly using the names of deceased people.

The amount of identity fraud that is really occurring is difficult to quantify as we only know about the fraud that has been detected. It is certain, however, that identity fraud is a great cost for our governments and our communities - hundreds of millions of dollars would probably be a conservative figure, billions of dollars may be more likely for many countries.

It is also certain that identity fraud is becoming easier and cheaper for the criminals and harder for us to detect - with globalisation, rapid electronic information flows, technological improvements to computers, printers and photocopiers, increased use of the Internet enabling transactions to happen at a distance - and the inevitable move away from face-to-face interactions.

When we find out about identity fraud, we spend money trying to deal with the problem - investigating and prosecuting people, deporting people (if we can find them). But by then it is often too late to repair the impact of identity fraud on our economies or on our national security. Frequently, the economic costs have to be written off as the money or the goods or the services the person or criminal group has taken will never be recovered. And if the terrorist action has already occurred then our national security and safety have suffered a severe blow.

As well as these direct and obvious costs, the indirect costs of identity fraud have a significant impact on our communities - including on our ability to make improvements to the lives of our people. For example, plans to provide services to communities - such as water supplies or the vaccination of children - depend on our having reliable information about the size and composition of community groups. Reliable information about births, deaths, marriages, name changes and nationalities is essential for the cost-effective provision of social and community services.

And there is, of course, the personal impact on those innocent people whose identities have been stolen. They may have to try to establish their innocence or rebuild their reputations or their credit histories. Or they may have to deal with the trauma of being interrogated about a family member who is alleged to have committed crimes but in reality has died, maybe in infancy.

Of this we can be certain - our citizens suffer the consequences of identity fraud - financially, socially and psychologically.

The financial, social and national security consequences of identity fraud mean that doing nothing is not a practical option. As I mentioned before, perpetrators of identity fraud will take advantage of ineffective or non-existent identification systems and processes to hide who they are, where they have been and why they are here. They will threaten our capacity to protect our borders and our citizens.

The Ministers attending the Second Regional Ministerial Conference in Bali (in April last year) recognised that border security was a key component of national and global security. They noted that transnational criminals ruthlessly exploited border security and management systems - particularly of those countries that were in the process of developing national, regional and global capacities to combat these crimes - and that illegal migration threatened the capacity of States to protect their borders and their citizens and to manage the entry of people through the borders.

Identity fraud is also very high on the agenda of a lot of other countries - and countries that are slow to address the problem may run the risk of having other countries' solutions imposed upon them or of having other countries making it difficult to cross their borders.

Of course we cannot eliminate identity fraud completely - but we can improve our identification processes and our cooperation to make it more difficult for the criminal, the terrorist and the opportunist to commit identity fraud in the first place.

Preventing identity fraud, or deterring opportunities for identity fraud, requires a financial commitment but will result in cost savings in the long term - because it is usually much more expensive in financial and social terms to find (if we can), arrest and prosecute the perpetrators and to try to repair the damage they have done.

In looking at how we can reduce opportunities for identity fraud to occur, we would generally think first about the documents that we use as proof of identity documents. These are usually referred to as **'token-based' solutions'** - where each person has in their possession a document or documents to prove their identity - such as passports, national identity cards, birth, death, marriage certificates, etc. We would first want to ask - are our identity documents up to the proper standard to ensure their security?

And, these days, in considering how to verify or authenticate an identity under the token-based solution, we may also be thinking about incorporating **biometric solutions** - facial recognition, finger or hand printing, iris recognition, to name a few.

On the face of it, the advantages to be gained from incorporating biometric information into our documents are significant. Biometric information can be used to ensure that a person is not issued with multiple identity documents in different identities - and that an identity document is being used by the right person - and for checking an identity against a database of biometric images.

The supporters of biometric solutions will say that we need them because our existing means of identification are not effective enough - documents can be stolen or sold or, with the wide availability of inexpensive computer packages, can be altered or fabricated with relative ease. And they are right. The value of biometrics - especially the use of multiple biometrics - to our proof of identity systems is very significant, not only for these reasons but also because this is the direction in which much of the rest of the world is moving.

However, those who are against biometric solutions also have valid reasons for concern. The cost of installation is high and, in many cases, the effectiveness and accuracy of the biometric solution may be rather less than 100%.

They may argue that biometric technologies have yet to be tested on any sizeable or diverse population group.

If they are talking about identity cards, for instance, they may ask how secure were the documents that were relied upon to issue the biometric identity card - such as a birth certificate.

And there is still the 'human factor' to be taken into account - as well as developing documents with biometric data, we need also to train our officials to understand the database matching processes.

Then there are concerns about privacy - what other purposes the data might be used for. Who will get to see it? Is there potential for other agencies to use the biometric data to find out other information about people? Information that the person did not realise would be collected when they gave their biometric identifier.

All these are issues that we need to be aware of and to address in considering whether a biometric solution is appropriate at this stage in the development of our proof of identity processes.

We can conclude, I think, that a biometric solution is not, by itself, a complete solution to the proof of identity process - if we use them we cannot be complacent that we have the problem of identity fraud solved.

An obvious situation where biometrics alone cannot provide a complete identity solution is at the time of first contact with a person - when we need to decide, for the first time, who that person is.

If we were to use a biometric (and token-based) identifier solution alone at this first contact point, we might simply be providing the person with an opportunity to link a false name, or other false information, to that identifier. We have to find a way to verify a person's identity the first time, before giving them the biometric (or token-based) identity document.

For this situation, we need **knowledge** to help us decide if the person is who they say they are - what information do we have that we can use to cross-check who the person is? For example - do we know their previous addresses, their movements in and out of the country, their identity numbers, their date of birth, date of marriage (perhaps date of death if we have information to that effect) their previous applications for identity or other documents?

In summary, when we are considering effective proof of identity solutions we need to consider a combination of solutions: the token-based solution with or without a biometric solution and the knowledge-based solution.

Before moving on from proof of identity solutions to processes, I would like to touch briefly on another system that is sometimes used - especially by law enforcement agencies and often also at border checkpoints - **profiling**. Profiling, when used appropriately, combines a reason to suspect a particular person with an established profile of people with particular characteristics - that might include country of origin, gender, age. The profile would have been developed by calculating the statistical 'behaviour' of the group under examination.

When used properly, profiling can be a useful tool - but it can be misused. The problems with profiling usually arise when demographic profiling alone is used - and is not combined with a reason to suspect a particular individual.

It might be fairest to conclude that profiling should be seen as a useful 'tool' for further investigation but not as a proof of identity solution in itself.

I have mentioned some issues we need to think about in developing proof of identity solutions. Just as important as the solutions we choose, however, are the processes and procedures that we put in place to back them up.

An identity document is only as good as the procedures used to issue it and the safeguards employed against counterfeiting and theft. We should be asking ourselves:

- how accurate and secure are our records and databases and alert systems?
- how accurate and effective are our checks at the borders - when people are arriving and when they are leaving?
- how effective is our training of the officials who issue documents, and of those who check them to verify an identity - our immigration officials, our border officials, our law enforcement officials?
- do we have in place rigorous document examination techniques? What do we need to do to build these up?

How do we identify and manage risk? For example, what could we do away from the borders, maybe in visa offices, so that officials have more time to focus on problems and to make decisions? Could we get advance information about travellers, maybe by way of an Advance Passenger Information System?

In summary, there is no one solution to dealing with the problem of identity fraud and an effective system of deterrence is likely to require a mix of processes, procedures and solutions to authenticate and verify identities.

As well as the issues I have mentioned already, different geographic and demographic factors mean that different countries have different needs - and even within a country different situations might need different solutions.

Land borders, air borders and sea borders, for example, might each require a different process or a different solution. Certainly, those of us with land borders cannot effectively manage these unless we do it in cooperation with our neighbours.

The numbers of people we have crossing our borders each day will also have an important effect on our identity fraud processes and procedures. We need measures that will improve our proof of identity processes without unduly inconveniencing the genuine people - and if we have very large numbers of people at the border at the one time then we will have problems if we have to keep them all there for long periods of time.

We might need different processes for different groups of people. For example, how do we deal with frequent business travellers - or people who are in transit, en route to a third country? What about the customary movement of indigenous groups - moving from island to island for fishing, for example?

And, as we cannot completely prevent identity fraud, we also have to ensure that our legislation, investigation and law enforcement measures are effective. Is identity fraud recognised as a crime under our current laws? Can we prosecute identity fraudsters? Can we convict them?

There is already a lot of work going on within individual countries and we shall hear about some of these initiatives during this workshop. Brief descriptions of recent national initiatives by some countries in the region are also contained in the background document in your workshop folder.

However, the 'transnational' nature of many identity fraud crimes means that none of us can effectively deal with the problem in isolation.

I spoke before about the need for **knowledge-based solutions** to cross-check an identity when we are trying to find out who a person is for the first time. This is an area where cooperation between countries and regions can play an important role in deterring and combating identity fraud. The sharing of information on lost or stolen passports, for example, or the development of regional alert lists.

Some of you are already involved in bilateral cooperative approaches with your neighbours - for example, Malaysia's and Brunei are trialing the use of their multipurpose identity cards as travel documents between the two countries. Malaysia and Singapore are considering a similar cooperative arrangement.

The Republic of Korea and Japan are trialing a new "E-Check In" system, using iris recognition technology, at Incheon Airport in Seoul.

China and the European Union have also recently been exploring ways to improve cooperation in the fight against illegal immigration by the exchange of knowledge on the recognition of false documents.

Regional associations are also looking at cooperative initiatives. For example, the Asia-Pacific Economic Cooperation has introduced the APEC Business Travel Card Scheme. They are also looking at ways to improve immigration processing and border security - such as Advance Passenger Information Systems, best practice travel document examination and standards for immigration legal infrastructure.

APEC is also looking at the feasibility of a Regional Immigration Alert System to enhance security without noticeably slowing down the movement of travellers.

The Pacific Immigration Directors' Conference addressed the issues of identity fraud, people smuggling, people trafficking and illegal migration at its annual conference in Tonga in September 2003. The PIDC is also fostering the provision of technical assistance in the Pacific region. For example, 15 new Training Instructors have begun work in the region - having attended the Border Control Training Program conducted at the PIDC Forum Secretariat in May 2003.

In their Statement on Counter-Terrorist Action on Border Security in June 2003 the ASEAN Regional Forum members recognised the need for cooperation to strengthen border security and for common global standards for the collection and transmission of Advance Passenger Information.

The Regional Forum members also supported efforts to gain agreement on minimum standards for the issue of travel documents and identity documents and on ways for sharing data for incorporation into regional alert systems.

They supported the work of the International Civil Aviation Authority to develop minimum standards for biometrics in documents and improved procedures for sharing data on lost or stolen passports.

These initiatives all represent opportunities for practical cooperation in dealing with identity fraud. But there are other benefits to be gained from mutual assistance and cooperation. The sharing of experiences for example - so that those of you who are starting to develop solutions and processes can learn from the experience of those who have already developed theirs.

What problems or issues did you face and how did you deal with them? Would you do some things differently if you were starting now - whether in respect of the solutions or systems you chose or the business processes or procedures you put in place?

Did the identity fraudsters find ways to cheat the solutions and procedures? Could the solutions and procedures be readily changed in order to stay ahead of the criminals?

How was training handled? Was it effective? Can that training be shared with other countries?

But we must also think about our national and regional solutions in the broader international context. We must align our systems, processes and standards to the international standards - for economic reasons if nothing else. It would not be practical to develop a system that was not compatible with systems being used by other countries.

ICAO, for example, has recently adopted a global blueprint for integrating biometric information into passports and machine-readable documents - including visas and identity cards. They have decided upon facial recognition - and countries will have the option to include one or two secondary biometrics to supplement this.

In June last year, the International Labour Organisation adopted a global convention to require commercial seafarers to carry new biometric identity cards - fingerprint, face, hand, or iris data. This convention attempts to balance security concerns with the need to move goods expeditiously by sea, while at the same time deterring piracy, fraud and forgery.

The International Organization for Standardization and the International Electrotechnical Commission have established a Joint Technical Committee on Information Technology. This includes a subcommittee for the development of formal international biometric standards.

UNHCR is investigating the use of biometrics in the registration of refugees, with a view to developing a standardised worldwide registration system to help identify refugees in need of resettlement.

Our solutions and processes need to be compatible with and respond appropriately to relevant international standards and developments.

The Ministers attending the Second Regional Ministerial Conference in April last year (that I mentioned earlier) also noted that cooperation between regions was an important and complementary strategy to regional and bilateral cooperation initiatives.

Let me conclude by saying again that the problem of identity fraud is a national, regional and global problem as it becomes increasingly used by opportunists, organised gangs and terrorists to commit their crimes. The cost of identity fraud - to our economies, our national security, our social structures, our reputations and to the wellbeing of our people - is enormous. Doing nothing is not an option but we also cannot effectively deal with the problem in isolation from each other.

In this workshop I hope that we can begin to consider the way forward. We can begin this process by exchanging information on what each of us is doing now - to develop better proof of identity documents, better issuing and verification processes and procedures and to improve how we deal with the perpetrators of identity fraud when we find them. And we can exchange information on what we would like to be doing in the future to improve our documents and our processes.

We can discuss what is possible and what is practicable - for our individual countries and as a region. How can we cooperate to achieve workable and cost-effective outcomes? What networks can we build and what contacts can we make? What can we learn from each other's experiences? What is the potential for cooperation in building capacity?

We will not, in this workshop, resolve the problems facing us in respect of identity fraud. However, I believe that we can take the first steps towards cooperation and assistance within our region and build networks and develop contacts that will keep the discussions going after this workshop finishes.