STANDING COMMITTEE ON CITIZENSHIP AND IMMIGRATION

COMITÉ PERMANENT DE LA CITOYENNETÉ ET DE L'IMMIGRATION

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
OTTAWA, CANADA
K1A 0A6

CONFIRMATION OF APPEARANCE **CONFIRMATION DE COMPARUTION**

BY FACSIMILE

PAR TÉLÉCOPIEUR

TO / À : **Ian Williams**

Tel. (416) 702-3015
Fax (416) 352-5741
E-mail: ianw@idsysgroup.com

FROM / DE:
William J. Farrell, Clerk/Greffier
Room/Pièce 672, 180 rue Wellington St.
House of Commons/Chambre des communes
Ottawa, CANADA K1A 0A6
Tel.: (613) 995-4026
Fax / Télécopieur: (613) 943-0307
E-MAIL / COURRIEL : cimm@parl.gc.ca

TOPIC / SUJET :
National Identity Card / Carte d'identité nationale

Date of Appearance / Date de comparution:	**Thursday, October 30, 2003**
Time / Heure :	**3:30 p.m. – 5:30 p.m.**
Location / Endroit :	***Parliament Hill***
Room / Pièce :	***308 – West Block***

Appearance Before the Standing Committee

Citizenship and Immigration

National Identity Card

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
OTTAWA, CANADA
K1A 0A6

Thursday October 30th, 2003

Parliament Hill,
Ottawa, Ontario
Canada

Ian S. Williams
Principal
Identity Systems Group
ianw@idsysgroup.com

www.idsysgroup.com

Introduction

Mr. Chair, and members of the standing committee, good afternoon, my name is Ian Williams. I am the founder and principal consultant for the firm Identity Systems Group. Thank you for inviting me to present to you regarding the discussion of a National Identity Card, biometrics and other issues surrounding these topics.

Firstly, I applaud the CIC and in particular the Standing Committee for recognizing the importance of constructive democratic dialogue. The process you are undertaking is one of the recommended measures to ensure that any identification system designed for large-scale public use meets it's objectives, whilst addressing the concerns of those that may be opposed. It is often during this process that a government will realize that their intended plan does not meet its original primary objectives.

Background & experience

Knowing that many groups have presented to you, both for and against either a National ID Card or biometric technology, let me first give you an indication of my background on these matters. Identity Systems Group is a Canadian firm that provides guidance to governments regarding the applicability of advanced identification techniques including biometrics, document security and the policies created to enhance enrolment and improve the identification process. ISG was formed out of necessity at the urgency of two government agencies, one Canadian the other American, who could not source "independent" expertise, knowledgeable in all aspects of the identification process, that offered objective opinions on the establishment of government ID initiatives.

Prior to founding ISG, I spent ten years as the Technical Director of Government Programs at the world's largest provider of card based identity solutions, and led the development of biometric enhancement to their document based identification initiatives. I have provided technical, policy and other guidance on over thirty major government ID programmes including National Identity Cards, Passport and Driver Licence programs.

My involvement in the addition of biometric technology to the identification process began well before September 11th, as the evolution of the identification industry warranted better methods of verification and non-repudiation. In 1992 the firm I was employed by developed the process of integrating a photo to a plastic card and subsequently we have seen a mass acceptance of this technology worldwide including Canada. In 1994, I began the task of investigating the potential of biometric technology to further improve the identification process, a task that I continue today.

Many of the programmes I have worked on utilize biometric technology in attempts to improve the identification process. In regard to specific Canadian experience, I have spent considerable time in the last ten years focused on improving the identification process surrounding the issuance of provincial driver licences and identification documents (DLID). I have been employed for the systems currently in place in British Columbia, Newfoundland, Alberta, Saskatchewan and have provided assistance on the systems deployed in Quebec, Ontario and currently into the design of a new system for Manitoba.

Current Status

I submit that my experience is directly relevant to your issues. As Minister Coderre pointed out during his opening remarks at the recent Biometric Forum, the driver licence is not just a certificate measuring

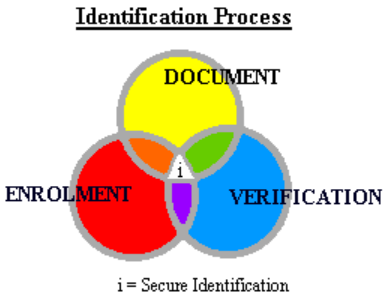
eligibility to operate a motor vehicle. Deservedly or not, the driver licence has become the defacto identification document, both in the US and Canada for many identification purposes including cashing cheques and boarding domestic aircraft. Understanding that a driver licence does not prove nationality, it is still however the most common photo ID document presented and used in the validation process for measuring eligibility to higher types of national identification documents, including the passport. It would likely become a contributing support (breeder) document for any National Identity Card.

As a result of September 11th, the ID business has seen a flurry of activity. However, all this activity has not been beneficial to the identification industry. Without fully understanding the primary benefit of biometrics as a tool to assist the identification process, many government entities both in Canada, the US and abroad, felt immediate need to implement "better" identification systems. As a result, hurried government projects and pilot systems have been implemented without following due diligence procedures, mandatory for the success of any public sector identification application. I will suggest that the primary issue surrounding identification and the most important aspect, that being "enrolment" cannot be addressed solely by technology such as biometrics. Compounding this belief have been vendor exaggerations of accuracy and applicability. Government bodies looking for the "magic" technology solution that will solve all ID issues have been quickly disappointed. Many of these government funded biometric programs and pilots have come under significant media scrutiny. Doomed to fail from the start, the news reports of failures has caused the biometric industry some concern. Identification industry experts may argue that the negative reports have unfortunately set back the natural acceptance and respect that biometric technology was earning as a tool in assisting the ID process.

The Identification Process

I have mentioned the "identification process" a few times; let me explain exactly what I mean by this. Identification is not a technology. It is a multi-layered approach to either validating a claim or proving a denial. The Identification Process in document based systems such as Passport or Driver Licencing can be broken down into three aspects:

Enrolment - Document - Verification



Each of these three aspects carry significant issues that impede their ability to assist the other two. The best identification systems balance all three aspects without placing undue emphasis on any individual component. I will attempt to explain all three aspects and how they are co-dependent upon each other. However bear in mind that the most difficult aspect and the one that must be the focus of any sound identification system is the Enrolment portion.

Within each of the three aspects there are many other issues affecting the overall integrity of the identification process:

Enrolment
- Validation (Proof of claimed Identity)
- Breeder documentation
- Duplication
- Assumed Identity (impostor)
- Secure access
- Privacy
- Reciprocity
- Data security

Document
- Issuance method
- Auditing
- Counterfeiting
- Modifeiting
- Genuifeiting
- Reciprocity
- Materials controls
- Data security & integrity

Verification
- Trust
- Non-repudiation
- Infrastructure
- Privacy
- Data integrity
- Data Security

Document – Second Aspect of the ID Process

Let's start with the middle piece – the document. The purpose of an identity document is to provide a portable, presentable proof of one's identity claim. Possession of which, relies upon the due diligence of the issuing authority, normally a government entity.

The document is typically secured by various means including holograms, laser engraving, machine-readable data and so forth. Similar to currency, these government issued identity documents use methods or technologies that would be difficult or expensive to acquire or duplicate thereby resisting "Counterfeiting". Since there is general agreement in the identification business that there will never be a tamper-proof document, often the documents are designed to resist "Modifeiting", such that tampering to them should be readily evident, thus negating it's acceptance as suitable proof of a claim. Lastly, IT security measures combined with controlled auditing and accountability of the consumable components of the document, and security clearance of individuals handling or accessing these supplies is designed to provide a resistance to "Genuifeiting", which can occur when an unauthorized production of a government document occurs using misappropriated genuine government supplies.

Some governments go to great lengths to produce a secure document and spend considerable resources in implementing systems to generate them. Others for a variety of reasons, and perhaps through lack of

funding do not. There are mitigating factors such as materials and volumes that affect the cost of these documents. For example, the amount spent per document by governments in the North American driver licence market varies from $0.60 cents to $10.00 per document. A huge delta exists between the documents considered most secure and those that are secured with minimal features.

Governments need also be aware that the provision of a highly secure document alone does nothing to increase the integrity of the overall identification system. Spending monies on document security without balancing the other two factors of Enrolment & Verification actually decreases program integrity since it falsely elevates the perception that the overall system is secure since the card is held in such high regard. This is a dangerous scenario and one that exists today in Canada with certain government issued ID documents.

Additionally reciprocity agreements often dilute the benefit a jurisdiction applies through an improved document. Within Canada this allows for individuals to exchange a document that may be considered less secure for a newer document that has been afforded a higher degree of trust. Each province maintains it's own reciprocity agreements with foreign nations further complicating the matter.

Verification – Third Aspect of the ID Process

Dealing with the third aspect of the Identification Process, Verification also carries certain issues. The verification aspect is two parts. The first part attempts to verify that the individual presenting a document and claiming an identity is indeed the individual the document was intended for and issued by a bonafide issuing authority. The second part is ensuring that both the document and the verified individual are the same identity that was enrolled and exists in the issuing authority records.

Historically, photos, signatures and text information are typical information that can help verify the document to the individual. The complexity of the document security design often provides the authenticity required ensuring that the document is a bonafide issuance. Placing machine-readable data on cards or documents can assist in providing remote verification but with certain risks. Without securing the data, the data is vulnerable to reproduction or modification. Additionally, without providing a method of direct communication to the enrolment database to further validate a claim (three factor authentication) one can never assume non-repudiation that the entity presented is indeed valid via credentials.
Documents that carry biometric information or digital signatures must be secured from access by non-authorized entities. The Public-Private Key Infrastructure (PKI) is a useful tool in securing biometric or personal information on an ID card or document to ensure that the data contained therein is not susceptible to inappropriate access. The data must be safeguarded against theft as well as duplication. This can also serve to increase the trust in remote validation where an online retrieval to the original enrolment database is not available.

In the verification aspect a primary concern surrounds the "privacy issues" or better termed increased intrusion perception. Many ID applications stumble due to the inability to develop acceptable verification policies that are consistent with either existing laws or the consensus of the general public. Biometrics can be a useful tool in assisting the Verification aspect, however with certain limitations. Processes such as fingerprint comparisons are often seen as intrusive and are rebuffed by the intended user base. ID systems that are developed on compatibility platforms or possibly using existing law enforcement technology are also further scrutinized since their exists the potential to exchange personal or biometric data and for that information to be used for purposes for which it was not provided. Other biometric issues that impede verification include the cooperative or non-cooperative design of the intended comparison. For example, if I were to access my bank account using my fingerprint, most likely I would attempt to place my finger on the scanner in a manner, which would improve the possibility of a match, thus allowing me access. However, if the same system was used to measure my entitlement to social services and I wished to collect

benefits using multiple identities I may choose to place my finger in a manner that would not match, or use other measures to further decrease the ability to match my finger with any previously enrolled template. The same approach applies to other biometric technologies such as facial recognition where disguises can be successfully employed. This form of approach could be termed non-cooperative.

The most successful ID systems are designed such that there is always a user privilege in providing the best possible sample. The cooperative approach will likely handle 99.9% of all users in a public sector ID system that provides a benefit to a match. The system can then focus on the 0.1% that pose the highest threat.

One of the biggest hurdles in the Identification Process is handling verification exceptions. These situations occur when the presenter of a document cannot be validated against either the biometric data within the document or the same data within the enrolment system that is claimed as their identity. In many ID systems, administrators have failed to develop consistent enrolment & verification policies that can handle conflict resolutions, presented when an individual is denied a privilege that they insist is rightfully their entitlement. Often glitches, technical difficulties or inaccuracies in the system can wrongfully deny the legitimacy of a true identity claim. Policies & procedures must be developed prior to deployment and supported by legislation if the system is to be applied consistently across a large populous and geographical area.

Similarly, identification systems have the potential to present a probability that an individual is actually another identity. Again, in this scenario where an individual may have to present further evidence of their true identity to support their denial, possibly through a secondary examination, policies and procedures that are supported by legislation are required to facilitate the resolution measures necessary. The policies and procedures must be uniformly applied across the entire ID System, including any enrolment or verification points.

These issues require extensive deliberations including input from many stakeholder organizations. Support for the policies and procedures must be established during the initial design phase if the ID system is to be successful, including the necessary supportive legislation. Attempts to have legislation adapt to the system through court challenges after deployment have caused the demise of many technically sound ID initiatives.

Enrolment – First Aspect of the ID Process

There is no doubt that deciding whom is eligible for enrolment in any public sector identification system is the biggest challenge faced by program administrators. Unlike corporate or private ID systems that are deemed "closed" since enrolment can be ascertained from employee databases or other fixed eligibility criteria, public sector ID systems must perform the measurement of all eligible enrolment criteria to unknown identities.

The two other identification process aspects of document and verification are rendered useless if the ID system cannot prevent unauthorized entities from gaining entry through wrongful enrolment. Provision of a trusted document, further validated by positive verifications can actually pose a bigger threat when applied to an individual that was not originally entitled to access into the ID system.

In almost all ID Systems the decision to grant access (enrolment) into the system is based upon the provision of supporting documentation by an individual making a claim and subsequent examination of said documents. Typically these documents are other forms of government issued identification from multiple governmental levels and often other countries. These documents are referred to as "breeder documents".

Many ID Systems use a process of scoring breeder documents that determine enrolment eligibility. Commonly, when a certain total score is reached that individual is considered having proved their eligibility to be enrolled. Unfortunately, the vast array of potential "breeder documents" combined with a lack of technology, procedures, fraud training and familiarity with detecting false documents makes it difficult for enrolment operators to make informed decisions regarding eligibility.

The issue of recognising legitimate supporting identification documentation, either from home or abroad, is the most serious obstacle in Canada, preventing the establishment of any secure identification system.

The ability for one to easily obtain supporting collateral such as baptismal or birth certificates landed immigrant papers, health cards etc. and other official government issued documentation is detrimental to all identification systems currently in place in Canada. Compounding this issue is the fact that most of these documents are recognized as supporting documentation for other ID systems considered "higher" such as driver licence, passport and immigration applications.

Until the issues surrounding "breeder documents" are addressed there exists the potential for increased risk by issuance of trusted documents that will enrol and validate a false identity, and possibly place undue trust in this false identity.

A Canadian solution

There is no doubt that the driver licence has evolved as the defacto domestic identification document. Since it is likely that this document will continue to exist it is therefore logical that we address the issues surrounding it. The issues that would negate the effectiveness of a new National Identity Card already exist in the driver licence arena and can be addressed, in a uniform approach by provincial and territorial agencies with decades of ID document issuance experience, if coordinated through a federal mandate.

"All citizens older than 16 years old (in some cases younger) must visit DMV's if they want a drivers license or a government issued identification card. **DMV's are the only authorized issuers.** More than 228 million U.S and Canadian citizens have either a drivers license or DMV issued ID card, representing 75 percent of the total population."[1]

Many provinces currently issue a Provincial Identification Card (PIC). The PIC is issued by the same agency issuing the driver licence and is available to residents of a province that require government issued photo ID and may not be eligible for a driver licence document. These PIC's are normally equivalent in security features to the driver licence and utilize similar enrolment and verification procedures in the overall identification process.

The Canadian Council of Motor Transport Administrators (CCMTA) is a non-profit organization comprising representatives of the provincial, territorial and federal governments of Canada, which, through the collective consultative process, makes decisions on administration and operational matters dealing with licensing, identification, registration and control of motor vehicle transportation and highway safety. It also comprises associate members whose expertise and opinions are sought in the development of strategies and programs. These associate members are comprised of representatives from major firms involved in supplying identification technology to governments including the new immigration card and the current Canadian passport. Within the organization there exists standing committees that have been addressing the

[1] AAMVA Special Task Force on Identification Security – December 2001

issues surrounding the driver licence use as an ID document for several years. Recently, they have begun addressing the issues outlined in this document.

In addition, CCMTA is based in Ottawa and its federal government member is Transport Canada. Other federal government departments are associate members of CCMTA and attend CCMTA meetings as the need arises. For example, Foreign Affairs attended a recent meeting when the issue for discussion was foreign driver licence reciprocity. Additionally, foreign reciprocity agreements for Canadian provincial driver licences, although a provincial mandate are generally negotiated and agreed to by each member province or territory through the CCMTA committee process. CCMTA is a suitable vehicle to ensure that reciprocity agreements reached are uniformly implemented and abided to by all provinces.

It is my position that CCMTA is the most suitable entity to coordinate a process of ensuring a practice of Uniform Canadian Identification across Canada. Using the driver licence and provincial ID cards, this would serve the interests of Canadians and address the same issues proposed by a new National Identity Card. The application of Uniform Canadian Identification to the existing infrastructure would not require the formation of a central national database of information on Canadians. There exists a procedure for cross reference checks between all Canadian jurisdictions for driver licensing that could be expanded to include the provision of a Uniform Canadian DLID.

The government members of CCMTA have already begun the process of using biometric technology to improve their Identification Process. This trend in DLID is expected to expand uniformly across Canada. Biometrics can play an assistance role in the ID process, particularly helpful in reducing the problem of multiple enrolment of the same identity. Biometrics also provides a means to improve the verification aspect of the entire process. However, biometric technology cannot address the most important challenges in the ID process surrounding entitlement to enrolment. This hurdle must be overcome by application of consistent eligibility criteria established through a due diligence process of policy and procedural design.

Summary

In the United States there is little discussion of a National Identity Card. In fact the US equivalent of CCMTA, the American Association of Motor Vehicle Administrators (AAMVA) have begun the challenge of providing US residents with a Uniform Driver Licence to serve their domestic interests of a National ID. Supported by the US Federal government, AAMVA have established a Uniform Identification Process that equally addresses the issues of Enrolment-Document-Verification across all states. I invite you to review the progress made by this organization and to consider the applicability of their mandate through CCMTA.

In summary, there is no point in establishing another identification program until the issues that are causing current programs to fail are addressed. Once existing programs such as the driver licence and provincial identification are improved there may be little need for another National Identity Card.

Explanation of Terms used
I have seen prior presentations to you, so I will assume that you are aware of many of the terms used when discussing aspects of any identification process, and the significant differences implied. For the purposes of this discussion I will define the following:

Cooperative (participation) – Applications where enrolees wish to be matched.

Counterfeit – Originally produced documents from other than an Issuing Authority, generated to appear to be similar or identical to the real thing.

Covert usage – Applications where data is obtained without consent.

DL – Driver Licence.

DLID – Driver Licence Identification Document. Includes Provincial Identification cards and often provincially issued Health Cards.

Genuifeit – A reproduction using genuine materials. These are very difficult to detect since they are created from misappropriated genuine supplies. They can either be personalized on the Issuing Authorities own equipment, or on similar equipment obtained by fraudsters.

Identification – Measurement of a single identity against multiple identities

Modifeit – A document, which has been altered from original appearance at time of production by the Issuing Authority. The most common examples of Modifeits are altered DL's. Often a birth date is changed to allow for the purchase or consumption of alcohol or tobacco.

Non-cooperative – Applications where exists a desire to avoid either verification or identification

Overt participation – Applicants are fully aware of their provision of certain personal or biometric data.

Reciprocity – Ability to exchange or obtain government ID documents and enrolment entitlement with minimal validation.

Verification – Measurement of an identity against a single claimed identity