dlid.org

ID World Int'l Congress 2005

North American Government ID

DL/ID to undergo REAL changes

Ian Williams
Principal
Identity Systems Group Inc.

On May 11, 2005, President Bush signed into law the "REAL ID Act of 2005," which was attached to the "Emergency Supplemental Appropriation for Defense, the Global War on Terror, and Tsunami Relief, 2005" (H.R. 1268, P.L. 109-13). Title II of REAL ID—"Improved Security for Driver's License' and Personal Identification Cards"—repeals the provisions of a December 2004 law that established a cooperative state-federal process to create federal standards for driver's licenses and instead directly imposes prescriptive federal driver's license standards.

Some highlights of the law:

Minimum Standards for Federal Use
§202(a)
§205(b)

A federal agency may not accept a driver's license or personal identification card (DL/ID) after May 11, 2008, unless the state has been certified by the U.S. Department of Homeland Security (DHS) in consultation with the U.S. Department of Transportation (DOT) to meet the requirements of the law

Security and Fraud Prevention Standards
§202(d)(7), (8) and (9)

A state shall ensure the physical security of locations where DL/IDs are produced and the security of document materials and papers from which DL/IDs are produced

A state shall subject all persons authorized to manufacture or produce DL/IDs to appropriate security clearance requirements

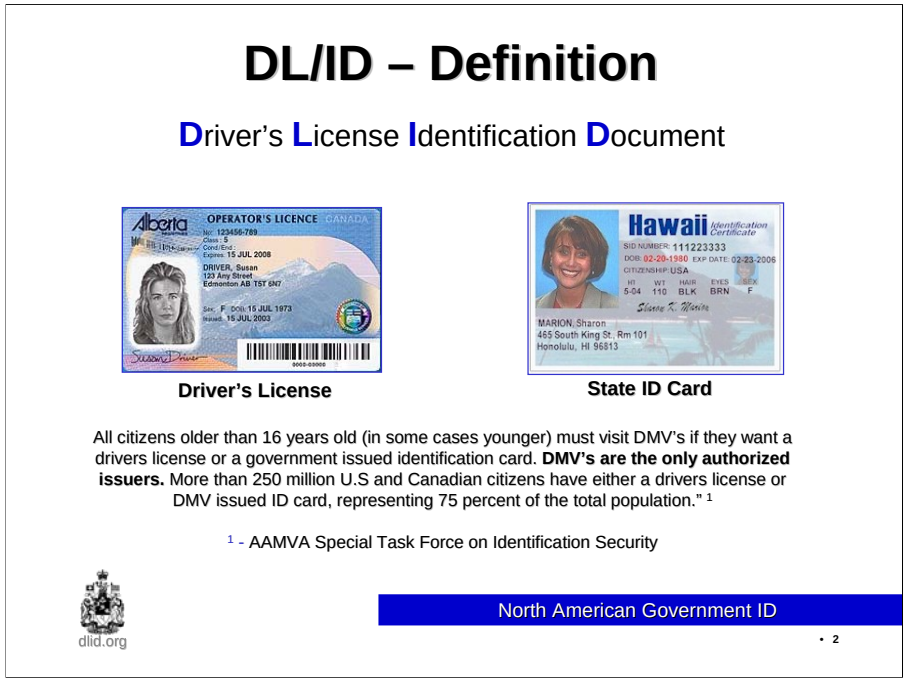
A state shall establish fraudulent document recognition training programs for appropriate employees engaged in the issuance of DL/ID

Non-Conforming DL/IDs
§202(d)(11)

In any case in which a state issues a DL/ID that does not satisfy the federal requirements, a state shall ensure that that the DL/ID: (A) clearly states on its face that it may not be accepted for federal identification or any other official purpose, and (B) uses a unique design or color indicator to alert federal agencies or other law enforcement personnel that it may not be accepted for any such purpose

Verification of Documents

Before issuing a DL/ID, the state shall verify, with the issuing agency, the issuance, validity and completeness of each document to be presented



DL/ID - Definition

DLID – is an acronym for DRIVER LICENSE IDENTIFICATION DOCUMENT and actually means two documents. The common driver license DL is the first, but many folk outside the US and Canada are not aware that states issue the general identification card (ID) most North Americans use as their preferred form of government issued ID.

"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 250 million U.S and Canadian citizens have either a drivers license or DMV issued ID card, representing 75 percent of the total population."[1]

The ID card is issued by the same agency issuing the driver license and is available to residents of a jurisdiction that require government issued photo ID and may not be eligible for a driver license document. These ID cards are normally equivalent in security features to the driver license and utilize similar enrolment and verification procedures in the overall identification process.

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

DL/ID Documents – Why are driver licenses so important?

Deservedly or not, the driver license 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 license does not prove nationality, it is still the most common photo ID document presented when requested for "Government Photo ID" and in most cases used as a scoring document in the validation process for measuring eligibility to higher types of national identification documents, including the passport.

Biometrics and the new Chiptogram OVD should fix everything- Right?

As a result of September 11th, the ID business, including the DL/ID market has seen a flurry of activity. On occasion we have witnessed the vendor community promoting biometrics as the saviour to all ID Program issues. Some government entities both in Canada, the US and abroad, immediately sought to "upgrade" their ID systems without fully understanding the limitations and benefits of technologies such as biometrics. Others governments looked to implement a much newer "safer" identity document with all the latest security gadgets. Ignored were the development of cumbersome required supporting polices, procedures, cross jurisdictional regulations, human training and an otherwise balanced approach to enrolment integrity, document security and subsequent verification.

Unfortunately there is no "magic" solution. Biometrics can assist certain aspects of an identity program but with many limitations. If I'm first in the new enrolment database, even if I am using your identity, it's too bad – for you. An expensive licence or passport document chock full of OVD's, watermarks, chips etc is really no good if it's given to the wrong person in the first place.

I will suggest that the primary issue surrounding improving identification and the most important aspect of any government identity program, be it driver licencing or passport, is of "enrolment" and cannot be addressed solely by technology such as biometrics or security features on documents. 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.

DL/ID Threats – How Easy is it Really?

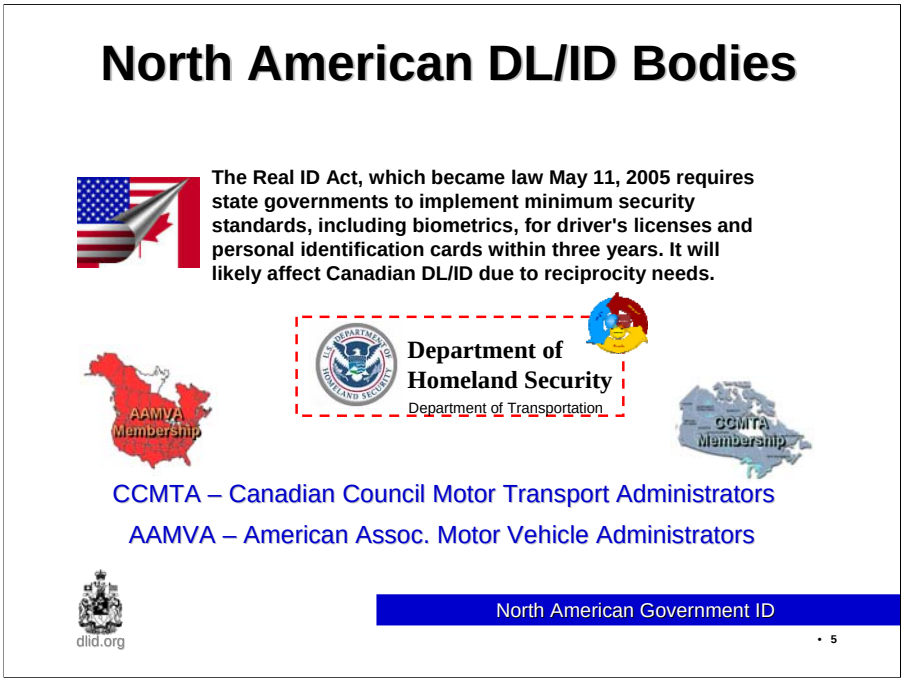
Compounding the issues in DL/ID security we are all aware that there are websites available that “claim” will make you a fake ID. The number of sites has dwindled down in the past few years due to the improved laws in the US regarding mail and internet fraud. Hence most of the sites offering these "novelty cards" are now located in Canada or the UK where the US Postal Service have no jurisdiction (or moreso the ambition to pursue mail fraud in a foreign country). The novelty cards are a minor threat to other basic issues of “Who are You?”

However a bigger threat to Government identity programs are the books and other information available that tells you how to go about creating the breeder documents and other supporting collateral to obtain a GENUINE DL/ID or passport under a bogus identity. Why spend a lot of money on a fake when you can spend less making or obtaining paper breeder documents and get the government to give you the real ID. No pun intended.

If told you how to go about getting a baptismal certificate or a copy of a birth certificate that was not recorded as deceased am I breaking the law. If I pointed out loopholes in a citizenship card program that has misplaced the photo of thousands of the original cardholder and informed you how to go about requiring a replacement using a registered identity that could not be disputed, am I breaking the law or exercising my right to free speech. Organized crime elements know how to exploit these government identity systems and using the concept of breeder document progression, it’s not long before you are facilitating passport, immigration and other frauds of a serious national concern.

Worse still, terrorists & serious criminals who do not shop at Fake-ID-Cards.com have access to financing. These entities may buy the equipment and means by which to produce real looking cards, spending hundreds of thousands of dollars on lithographic and security printing equipment. Remember the Mossad running around the world incognito with Canadian Passports a couple of years back? Lucky for us they were the good guys. No document cannot be compromised given sufficient resources.

The Real ID challenge - Governments must implement ID Programs & documents that not only prevent college kids from changing the birthday to purchase alcohol, but also resist compromise and corruption from organized criminal elements, or possibly foreign government that have resources to funding purchases, but also exercise extortion, human bribery and intimidation tactics to achieve their means.



North American DL/ID Governing Bodies

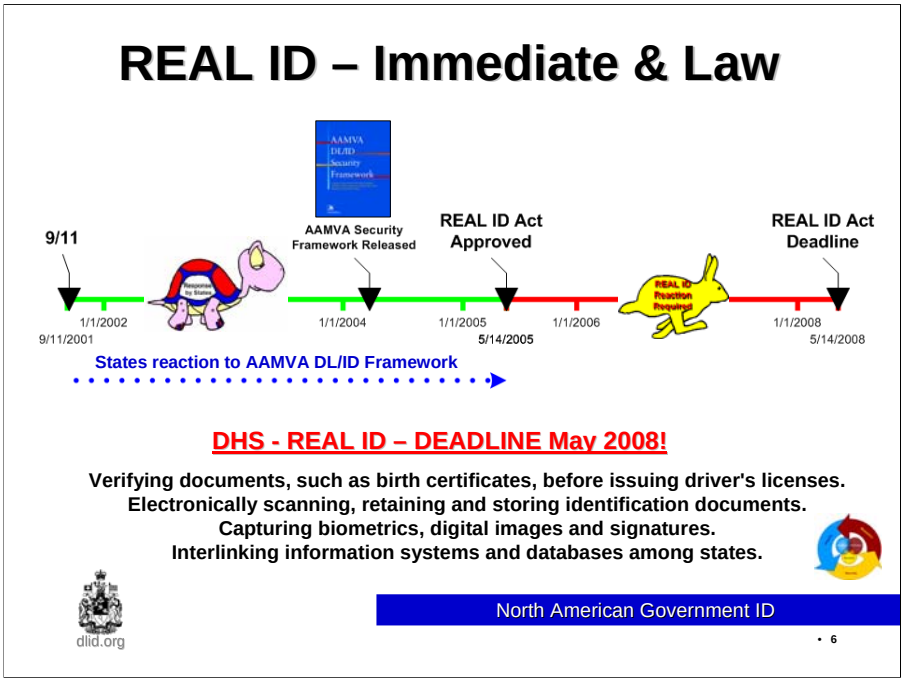
Until DHS/DOT added DL/ID to the REAL ID Act, matters concerning DL/ID security were almost exclusively an AAMVA and CCMTA mandate. In response to 9/11, the American Association of Motor Vehicle Administrators (AAMVA) started addressing the challenge of providing US residents with a uniform driver license to serve their domestic interests. Progress has been made by AAMVA although difficult to implement, since they have no method to enforce their "recommendations" onto the state agencies that issue DL/ID cards. The culmination of the AAMVA DL/ID Security Framework in 2004 was the result of much hard work. The adoption of AAMVA recommendations by state DMV's however has not been forthcoming. There has also been allegations within the community of vendor influencing standards and some of the requirements surrounding specific security requirements are conflicted, with vendor interests often prevailing.

However, many of the recommendations set forth by AAMVA are credible and DL/ID security was moving along, although some industry observers might say at a snail's pace. Many jurisdictions adopted AAMVA recommendations and went about improving their DL/ID programs. Unfortunately many jurisdictions did nothing, or even worse, procured new systems no better than the ones being replaced. Most often a lack of funding is cited for any lack of improvement.

What was required was a Federal mandate supported by legislation – This is where DHS stepped in with certain aspects of the REAL ID Act which addressed areas of driver license security & issuance control. Although the REAL ID Act is severely lacking in detail surrounding the intricacies of DL/ID program management and the reality of architecting a complex infrastructure using cross validation, it does make clear the penalties for not conforming. Denial of Federal privileges associated with the current DL/ID's. That means that the hundreds of millions of people who board an aircraft with a DL/ID card will not have this privilege unless their state government addresses the requirements of REAL ID. This is the enforcement that was required.

Entry into Federal buildings and other matters controlled by the federal government requiring ID will also become difficult for holders of non-compliant DL/ID cards.

States that will not or have not complied by the deadline will need to indicate this on the DL/ID card itself stating that the card may not be used for federal purposes. DL/ID cards have never before distinguished citizen privileges unassociated with driving and this may be too bold a requirement too soon, causing a significant anti REAL-ID backlash from any constituents of non-conforming states.



REAL ID – Immediate & Law

Where the states response to efforts by AAMVA may have been considered slow and somewhat diluted, there should be no doubt that REAL ID is fast and effective. Perhaps a little too fast? Without handing down specific details of the Identification Process required (all requirements of a secure DL/ID Program) DHS leave themselves open to scrutiny that they are not providing sufficient details & information for states to comply. Exacting details of the many number of sub topics in the Identification Process need to be defined by DHS, along with the Policy & Procedure Guidelines or regulations that states will require to implement REAL ID.

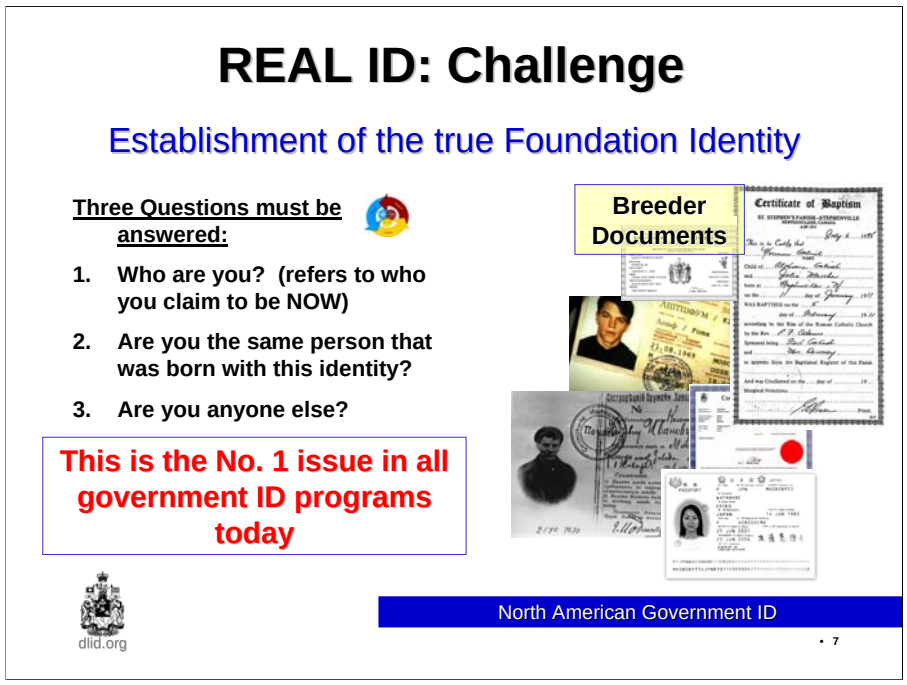
The Identification Process and the many complex articles involved are explained over the next few slides and notes.

The **Identification Process**:

1. Enrollment
2. Document
3. Verification

The Methods of Improvement:

1. Integrity
2. Security
3. Biometrics



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

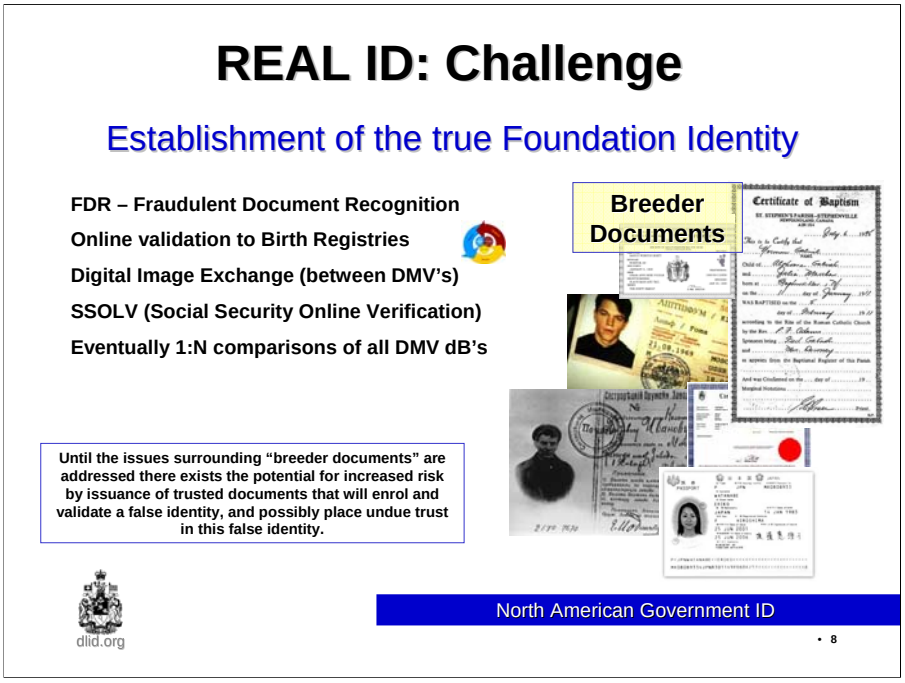
Each of these three aspects carry significant issues that impede their ability to assist the other two. The best identification systems balance all three aspects without placing undue emphasis on any individual component. I will attempt to explain all three aspects and how they are co-dependent upon 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 etc…

Document: Issuance method; Auditing; Counterfeiting; Modifeiting; Genuifeiting; Reciprocity; Materials controls; Data security & integrity etc…

Verification: Trust; Non-repudiation (biometrics); Infrastructure; Privacy; Data integrity; Data Security etc.…



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.

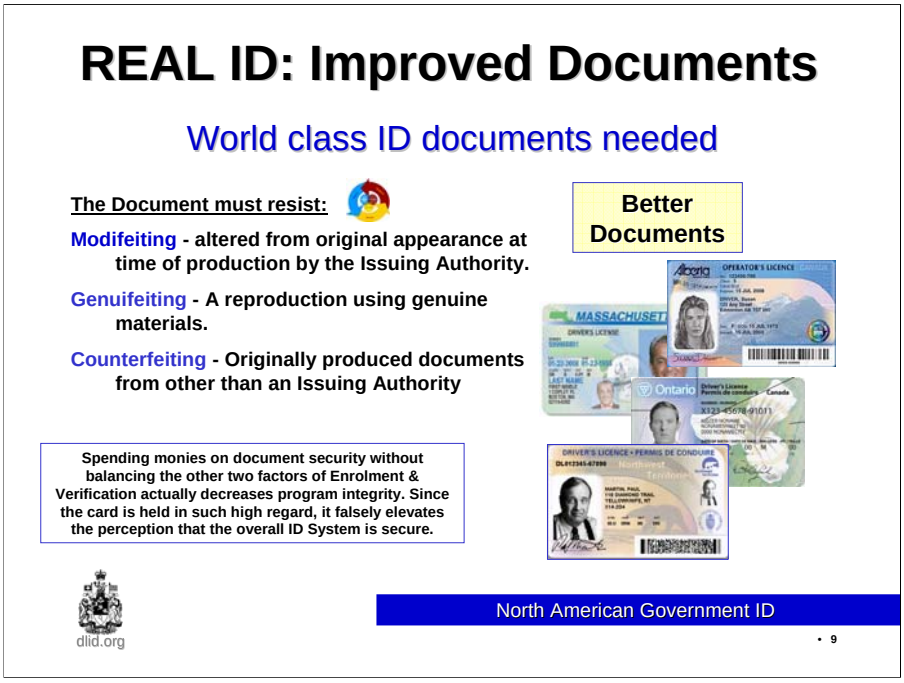
In almost all ID Systems the decision to grant access (enrolment) into the system is based upon the provision of supporting documentation by an individual making a claim and subsequent examination of said documents. Typically these documents are other forms of government issued identification from multiple 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, and validating information given at time of enrolment, is the most serious obstacle in the US, preventing the establishment of any secure DL/ID or national identification system.

The ability for one to easily obtain supporting collateral such as baptismal or birth certificates, notarized affidavits, college ID. and other official issued documentation is detrimental to all identification systems currently in place in North America. 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 license, 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.



Document – Second Aspect of the ID Process

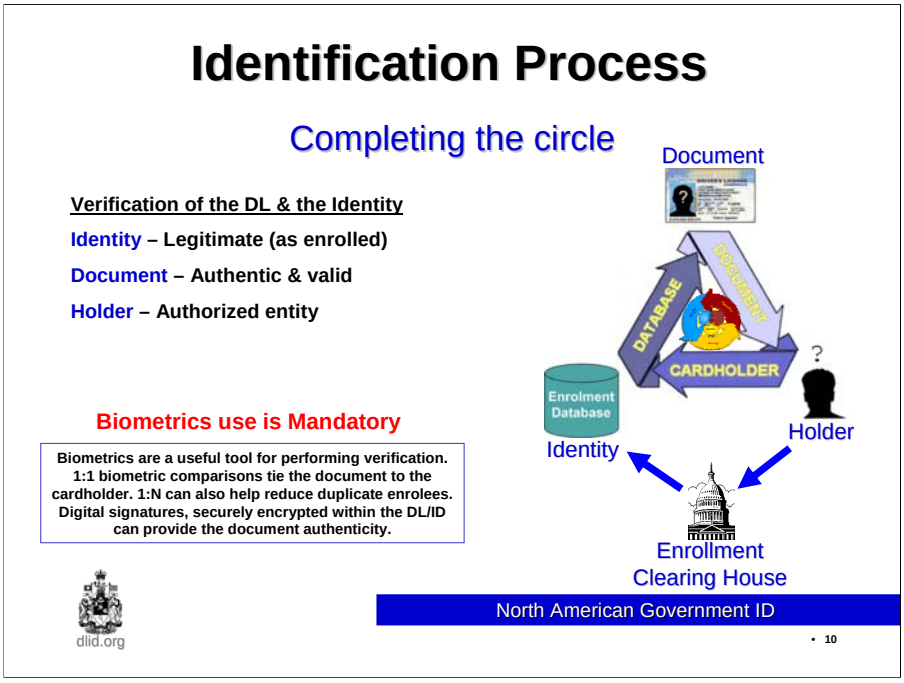
Let's look at the middle piece – the document. The purpose of an identity document is to provide a portable, presentable proof of one's identity claim. Possession of which, relies upon the due diligence of the issuing authority, normally a government entity.

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 license 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 North America this allows for individuals to exchange a DL/ID document that may be considered less secure for a newer document in another state that has been afforded a higher degree of trust. Each state or province maintains it's own reciprocity agreements with foreign nations further complicating the matter.



Verification – Completing the circle - Third Aspect of the ID Process

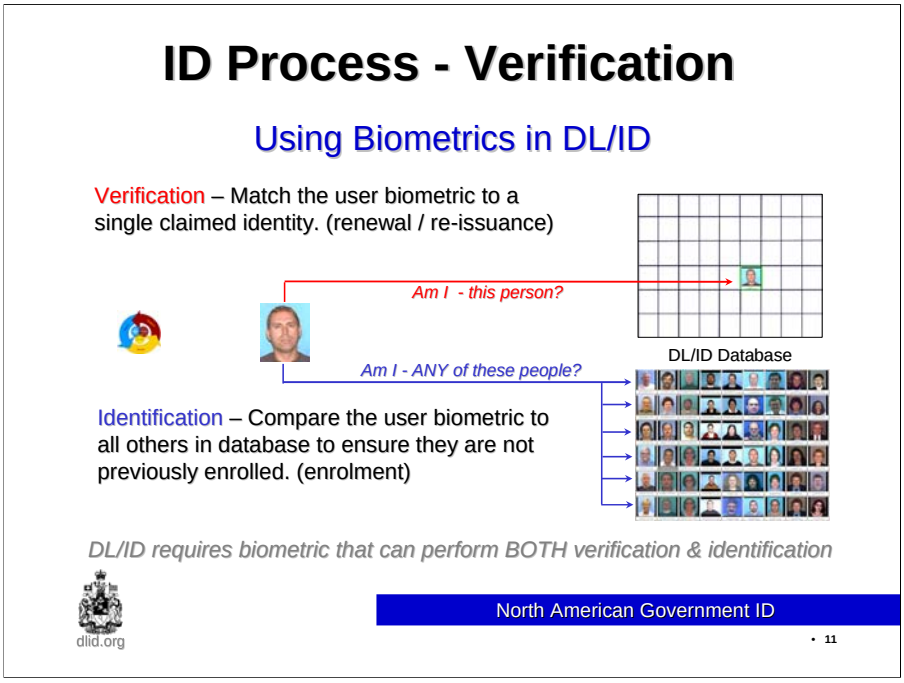
Dealing with the third aspect of the Identification Process, Verification also carries certain issues. The verification aspect is two parts. The first part attempts to verify that the individual presenting a document and claiming an identity is indeed the individual the document was intended for and 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.



ID Process – Verification – Using Biometrics for DL/ID

The two scenarios above translate into what is commonly termed in the biometric community as either a ONE: MANY or a ONE: ONE comparison. To simplify these further and put it into a driver license perspective, consider the following: Have I been issued a driver license before, perhaps under a different name? The first scenario would then compare my biometric data against all other previously issued records, comprising the ONE: MANY aspect of Identification. The second scenario, being a ONE: ONE, and as an example possibly an airport counter, a comparison to see if I was indeed the person this driver license was issued to, thus entitled to a privilege by Verification.

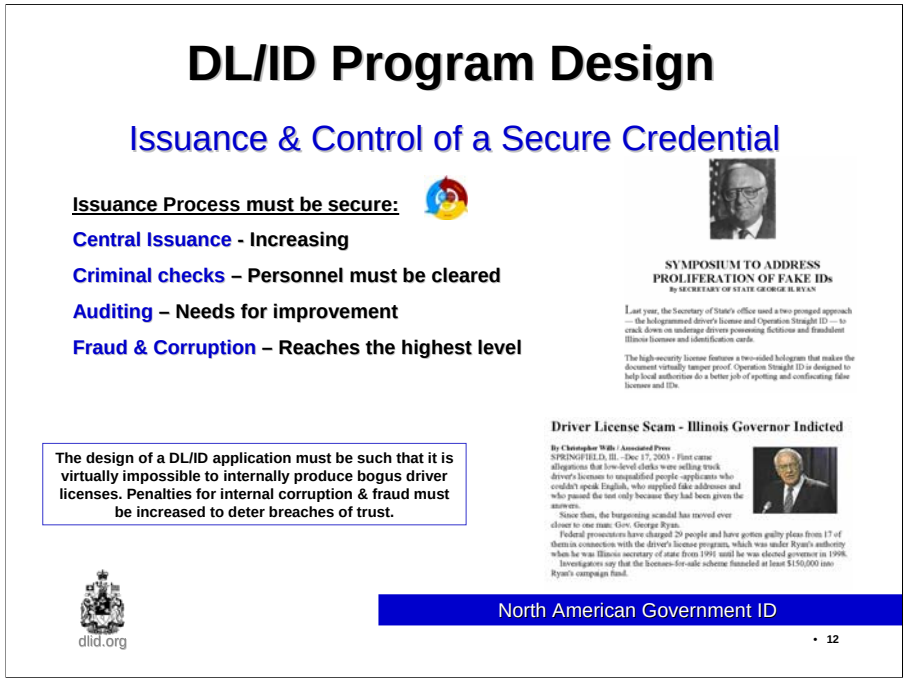
.

The ONE: MANY comparison in a driver license environment would almost certainly have to be performed at an enrolment station since it would require biometric data to be communicated securely to a host that contained biometric data for every constituent of the jurisdiction that had been previously enrolled. Inter-jurisdictional comparisons will require the data be transmitted across state, provincial or national borders for comparison against each jurisdiction's database or else the creation of an (inter) national database of drivers and their biometric data.

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.

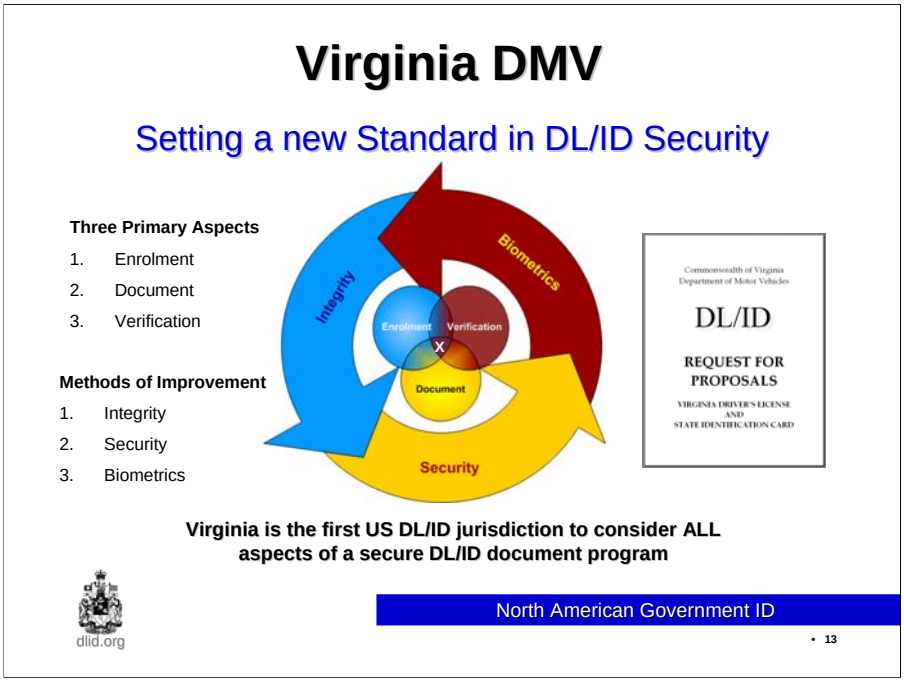


REAL ID – Accountability – Issuance and control of a secure credential

Fraud & corruption in DL/ID programs can reach the highest levels. The example above is Gov George Ryan of Illinois. Ryan while Secretary of State in 1998 made a big deal about improving the security of driver license issuance. Only a few years later in 2002 when as governor he was caught up in a DL/ID scam that claimed he ordered staff to issue alias DL/ID for some high profile friends. Also caught up in the scandal were industry lobbyists that the state attorney's claim influenced the vendor award and took bribes.

DL/ID application programs must be designed that they offer safeguards and audit methods to protect the state government from corruption within. Although a common method of inducing in-house fraud is the lure of lump sums of cash, recent incidents in the US & Canada have occurred where state employees were threatened or blackmailed into committing the crime of issuing non-validated DL/ID.

Security clearance procedures combined with an application design that recognizes false transactions or intercepts pending transactions during the verification process will help preserve the integrity of the DL/ID program by limiting entry and identifying fraudulent activity.



Virginia DMV – Setting new standards in DL/ID Security

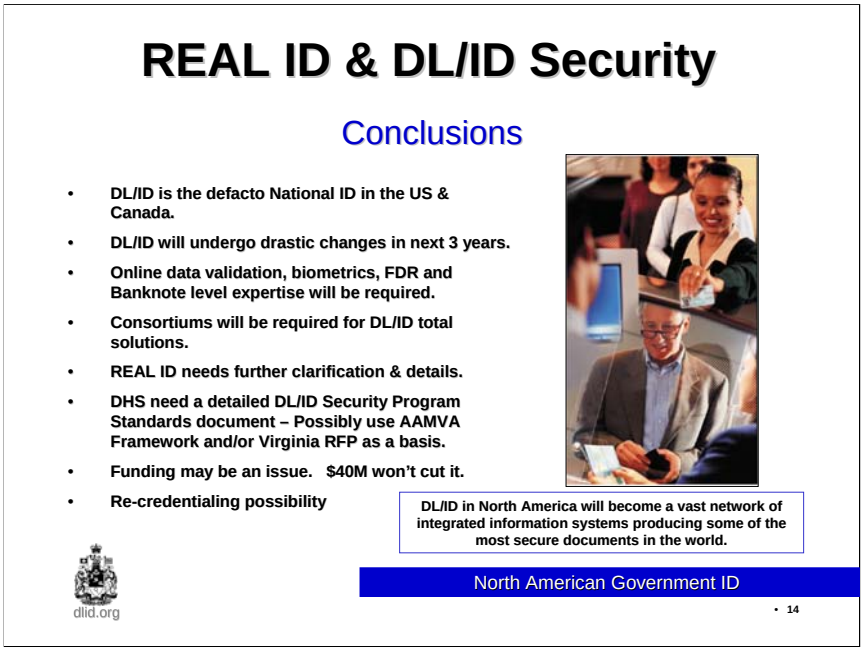
The Virginia DMV released a tender document recently to procure a new secure DL/ID solution. Virginia is taking REAL ID seriously and is the first state in the US to attempt to address all the aspects identified in the earlier slide as part of the Identification Process.

Virginia DMV are moving all DL/ID card production into a single secure facility where folks involved will require federal security clearance and the facility will be continually monitored. Any vendor providing services or supplies will require special security certifications. Recognizing the changing threat toward internal fraud and possible coercion, application design will flag suspicious activity and non-repudiated transactions may be reviewed.

Items such as criminal background checks on every person handling a card component to random audit checks on supplies are requirements. Virginia will also introduce the first DL/ID Card Design Security Program, which is a concept borrowed from the banknote industry where each banknote is continually monitored for security threats and has safeguards in place to pre-empt compromise. Continuing on this new path of DL/ID security, Virginia will add Biometrics and Fraudulent Document Recognition technology to help improve the integrity of the Enrollment database and improve verification.

The requirements included in the new Virginia DL/ID solution may set the standard in the United States for DL/ID. It may also cause a ripple effect throughout other states as no state ever wants to be the lowest on the DL/ID Security totem pole since reciprocity agreements precipitate you effectively become the favorite target for DL/ID fraud from everywhere else.

DHS might want to consider some of the requirements in the new Virginia DL/ID Solution as the basis for building the Program Standards document they need to give states, allowing them to have a roadmap to get from what they have today, to REAL ID compliance in just over 2 years.



REAL ID & DL/ID Security – Conclusions

1. DL/ID is the defacto National ID in the US & Canada.

Although never called a "national id" the DL/ID will serve the nations interests as domestic government ID for many years.

2. DL/ID will undergo drastic changes in next 3 years.

The low end security cards and OTC delivery methods we see today driven by the cheapest-cost-per-card-wins premise, will be replaced by sophisticated centrally issued cards that can compete globally as the most secure documents in the world. If a transition to DHS for DL/ID design occurs then we may actually see support for other machine readable formats such as chips or RFID cards that have never been supported at an AAMVA level.

3. Online data validation, biometrics, FDR and Banknote level expertise will be required.

There will be large demand for online verification methods. IT integrators will see a large opportunity to tie in older legacy systems with new DL/ID IT systems. Biometrics use will increase. The obvious facial recognition use will see serious competition from Iris as the From Patents expiry will provide affordable systems that can prove successful large 1:N results. POS document verification systems such as the Viisage Proof, Assuretec I-dentify, CBN Falcon and Foster & Freeman will enjoy the benefit of the requirement for document verification & FDR at the front line. Finally, the expertise in document security that is possessed by many European & international providers of banknotes, passports etc. will be required as the DL/ID documents themselves undergo a significant shift to tamper proof and multi-level secure credentials.

4. Consortiums will be required for DL/ID total solutions.

The DL/ID systems provided today are typically competed on by less than three companies. Future DL/ID systems (soup to nuts) will require solution sets, resources and skills beyond the means of current players. Where we have one company today, expect to see the formation of consortiums that bring the highest level of competency in their area of expertise to form winning teams that can provide every aspect of the total solution.

5. REAL ID needs further clarification & details.

DHS would benefit from releasing a comprehensive DL/ID Security Program Standards Guide that provided details on the exact needs required to comply with the high level indicated in the REAL ID Act. Everything from personnel clearance requirements to facility security measures should be included. Also included should be a revised DL/ID standard that indicates the exact requirements of cards and the level of adversarial analysis they must withstand. DHS can build upon the prior work of AAMVA and to be fair to states, provide this before they attempt to meet compliance. The document must also contain the necessary exemption rules and procedures and be supported by specific legislation to counter court challenges of a constitutional nature.

6. DHS need a detailed DL/ID Security Program Standards document

– As indicated above, possibly use AAMVA Framework and/or Virginia RFP as a basis.

7. Funding may be an issue.

The $40M currently allocated is simply not enough. It is highly likely that a complete re-credentialing of US citizens will occur. With over 300 million DL/ID documents in the US alone this far exceeds current funding – without doing anything new! The average North American DL/ID costs each state approximately $3 per card just to the card vendor. Without considering the cost of DMV staffing this aspect alone will cost almost a Billion dollars without adding the online transactions and other REAL ID requirements. REAL ID likely needs 2 billion dollars minimally to work across the USA.

Author's comment:

Often in cost per card deployments a primary goal is to reduce the cost of the finished document. This is sometimes achieved at the expense of card security features. This is unfortunate today since a digitized driver license card has become the defacto piece of identification for most people in North America. It is commonly used for boarding an aircraft and a multitude of other applications where photo ID is required. Although sometimes accompanied by other forms of identification, it is the driver license that is used most frequently, and that we rely upon.

The following statement was included in a paper prepared by this author as part of a developing DL/ID standard in 1999, 2 years prior to 9/11:

"We strongly urge all DMV's to fully consider the possible impact and subsequent consequential damage that a poorly designed DL/ID application or easily duplicated or obtained driver license document can cause. Easily duplicated or false DL/ID become targets for organized crime elements within North America and often from abroad, and can effect the stability of banking, economical and even political arenas."

Pre 9/11 DL/ID security was a topic that typically ended up on the bottom of any political agenda. The concern for improving the security & integrity of DL/ID was a backbench item, with little or no support for improvement from our political leaders. Today, we cannot ignore this issue as we now fully understand the consequences. Action groups like the Coalition for a Secure Driver License have formed as concerned citizens lobby for our political leaders to act on DL/ID security matters.

Even today, although fewer, many state jurisdictions are approaching DL/ID with the same lethargy that was so prevalent pre 9/11. The REAL ID Act sections related to DL/ID should be recognized as a positive action from the DHS. The REAL ID requirements can build upon the AAMVA efforts and accelerate the prior work from the DL/ID community which may never have realized full compliance or potential without a necessary Federal mandate.

Regarding adherence to REAL ID, there continues to be friction in regards to sovereignty over DL/ID issuance control. Is it a Federal or State controlled matter? Frankly, if you are a DMV administrator and you don't believe you are in the national ID business, you have your head in the sand. Rather than blindly oppose REAL ID the states should embrace REAL ID and work along with the DHS in developing policies and standards that will truly work. The Feds need the expertise from the DMV's who know this business better than most. Most DMV's have been issuing millions of identity cards over periods spanning 40-50 years.

REAL ID will work in DL/ID, provided that the states and DHS work together, and we all can help make sure it does.

Ian Williams:
ian@dlid.org
Phone: 01-519-942-9408
www.dlid.org