Testimony before the Senate Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia

A Hearing Regarding: A License to Break the Law? Protecting the Integrity of Driver's Licenses

Presented by Richard J. Varn, CIO, State of Iowa, on behalf of the National Association of State Chief Information Officers (NASCIO), the National Governor's Association (NGA), and the Information Technology Department (ITD), State of Iowa

April 16, 2002

Summary

Neither the NGA nor NASCIO have an official position directly on the subject of identity security or enhancing the driver's license and life document systems.

Identity security is a critical component of ensuring accuracy, preventing fraud, and granting privileges and benefits in many programs and processes.

Our identity system is broken and is more likely to actually enable identity theft and fraud rather than prevent it.

Our driver identity systems, cards, and issuance processes are not adequately coordinated to ensure transportation safety or the security of the myriad of their other uses on which we have come to depend.

Our life document systems for recording and providing proof of birth, marriage, name change, and death are inadequate to the task of supporting the issuance of identity and the extension of privileges and benefits. An enhanced life document issuance and verification system is essential to identity security.

Cyber-security, homeland security, secure electronic commerce, compliance with many laws such as HIPAA, and identity security are all related and need coordinated solutions.

Sound security in the creation and authentication of identity needs three parts: something you know, something you have, and something you are. We often rely on only one or two of these to establish identity and extend privileges and benefits. As a result, facts such as social security number, address, birth day, and mother's maiden name, which cannot be adequately protected as secrets, can be used to create identity and extend privileges and benefits fraudulently. It is not these facts or our inability to keep them secret that is the problem: it is that we rely on them alone to establish identity. Moreover, we have grossly inadequate methods of creating and determining the validity of life documents that comprise the "something you have" component. Finally, with the exception of photos, we have not yet embraced a common or coordinated biometric system for presenting "something you are".

The federal systems for legal entry of a person into our country need to mirror and be integrated with enhanced state and local life document and driver's license systems. The federal systems need to document the beginning, duration, course, and end of a legal entrant's "life" in our country regardless of whether they are just visiting or making America their new home. The multiple federal systems need to create a common, electronic, shared equivalent of a birth and death record. That common electronic record can be used by all levels of government in the same fashion as normal birth and death record and would be the referenced document for issuance of forms of identity and the extension privileges and benefits. Such a record for legal entrants could include a common photo, biometric, and the statement and documentation of their life facts such as name, date of birth, and so on. Even if different cards (driver's licenses, visas, etc.) were issued from this document, having the single common record would enhance security, prevent fraud, and increase the interoperability and efficiency of issuance and verification systems.

Addressing the issue of identity security is a process, not just a product. We are at the beginning of that process and it is recommended that mechanisms for ongoing input and consultation are needed on both technical and policy matters.

NASCIO members and the association itself play a critical role in coordination and implementation of federal, state, and local information technology systems and can be an invaluable resource for the federal government if given the opportunity. This is also true of the NGA, American Association of Motor Vehicle Administrators (AAMVA) and the National Association of Public Health Statistics and Information Systems (NAPHSIS) as well, just to name three of the many associations of state officials who stand ready and able to help. Private industry groups, such as the National Retail Federation (NRF), are also very interested in this issue and are playing a role in ensuring that those who must check ID are represented in this discussion.

There are many federal, state, and local projects and programs that overlap, are not coordinated, and have a great potential for duplication, lack of interoperability, and incompatibility. There is a crying need for coordination at each level of government and between levels of government on identity security on technical standards and systems and in policy making. It is not yet clear what the best options or mix or options are for this coordination. Some possible choices include:

- Interstate compacts
- Intergovernmental agreements
- Standards development through recognized standards bodies
- Coordination of information technology system architecture, development, and operation
- Federal funding for enhanced life document systems and driver's license issuing processes, systems, and cards
- Legislative and executive coordination of the funding, development, enhancement, and implementation of identity security programs and systems within and among each level of government
- Establishment of a single point of contact and coordination for various federal initiatives
- Creation of formal or informal federal, state, and local groups to coordinate technical and policy activities and exchange information

The need for coordination, the importance and diversity of interests in identity security, and a spirit of cooperation were in evidence at an Identity Security Forum held in Washington, DC in March of 2002. The forum was co-sponsored by NASCIO, AAMVA, NAPHSIS, and NRF and was attended by representatives of many government entities and private sector interests. A summary of the proceedings is attached under separate cover.

Iowa is working on creating an identity security clearinghouse process to ensure that life documents are not misused, used in illegal duplicate fashion, nor used without the knowledge of the subject of the document. A summary of this project is included with this testimony.

NASCIO, NGA, ITD, and I thank you for the opportunity to provide input on this critical issue.

Identity-Security Clearinghouse

Iowa Information Technology Department

Version 1.0
2/8/2002

http://www.infoweb.state.ia.us/ecomdev/current_projects/identity/index.html

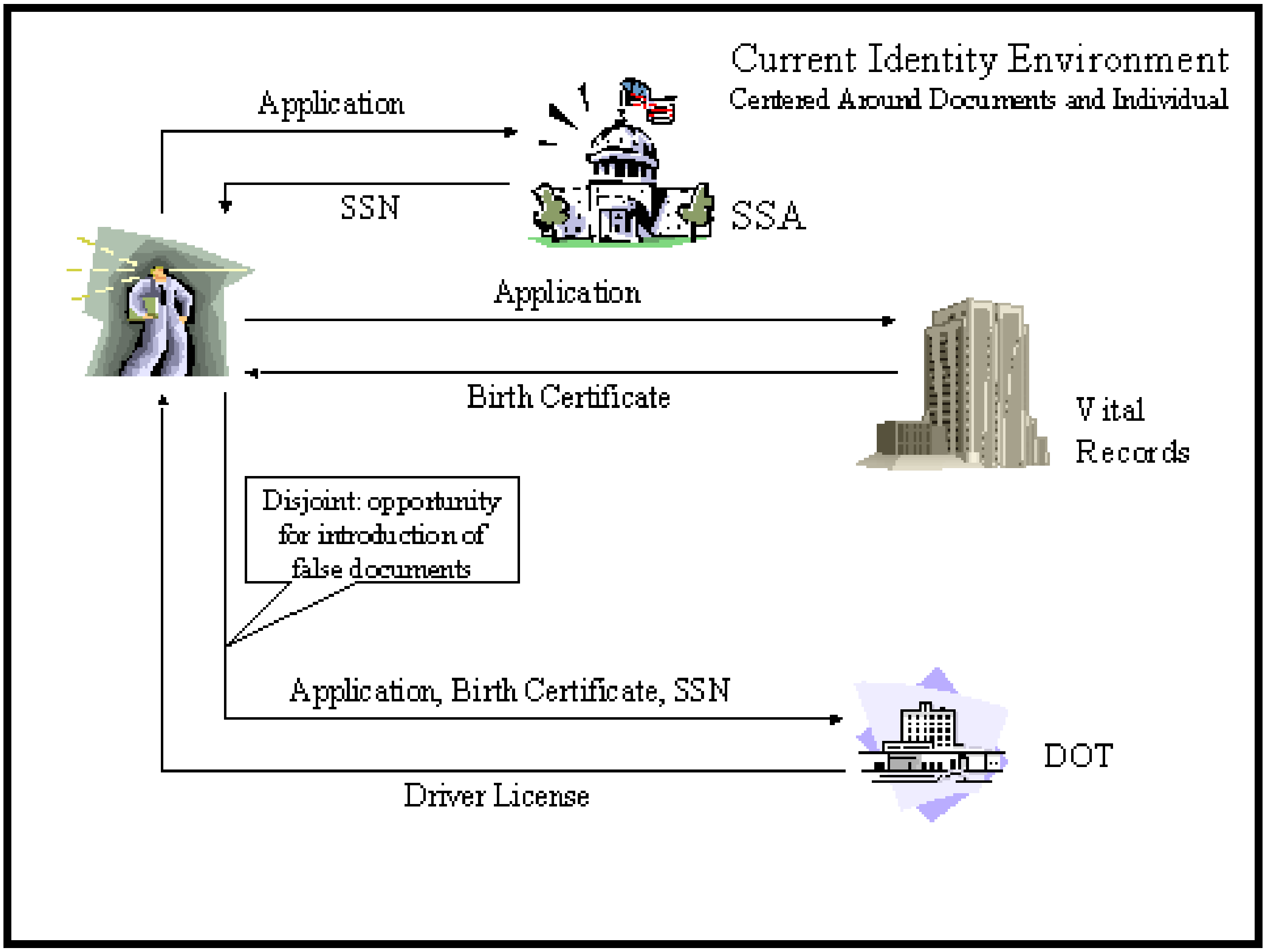
Powered By ITD

Existing Identity Security Environment

There exists today an identity-security infrastructure that relies heavily on identity documents issued by a variety of agencies and organizations. This infrastructure consists of the processes, personnel, and security requirements of each of the issuing entities. The identity documents are then given to the individual as a symbol to other entities that use the document for identification purposes. For example, once you receive your birth certificate, you can receive your Social Security Card, and then in the future present these for a number of other permissions such as your driver’s license or school enrollment.

The system has mostly relied on the integrity of the individual presenting the document as opposed to relying on the issuing entity of the identity indicia. For example, a clerk at a driver license issuing station may recognize a presented birth certificate as having the same size, shape, color, wording and stamp as an Iowa birth certificate but unless that can be verified back to the issuing entity the presented document is nothing more than a piece of paper. Therefore the reliance on the individual leads to a disjointed identity system that can easily be abused or circumvented.

The exhibit below demonstrates this based on a scenario for applying for a driver license. The applicant at birth received both a birth certificate and a social security number on a card. Both of those identity indicia can be used for the issuance of a driver license. Since there is a reliance on the judgment of the agent viewing the documents it is easy to see the point in the process where an individual could obtain false documents and present them for the driver license. If there is no reason for doubt of the documents and the individual, a driver license is issued.


Current Identity Environment
Centered Around Documents and Individual
Application
SSN
SSA
Application
Birth Certificate
Vital Records
Disjoint: opportunity for introduction of false documents
Application, Birth Certificate, SSN
DOT
Driver License

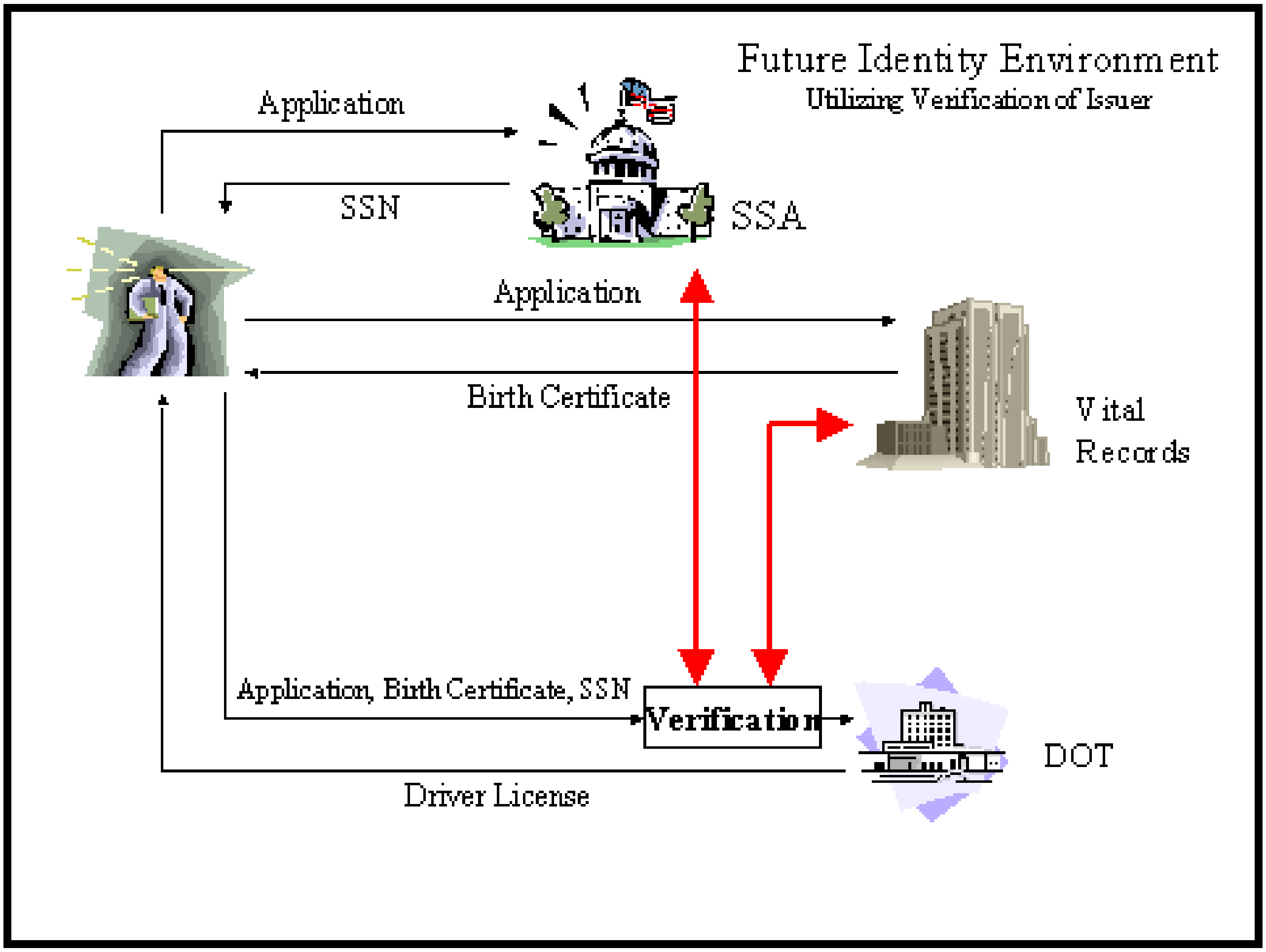
Recent Events

This disjointed process relying on paper and individuals creates a system that is primarily reactive and only reacts when disaster occurs. In other words, if a person can circumvent the identity system and create a false identity it may go unnoticed if the person does not do anything to draw attention to them.

The events of September 11, 2001 have raised quite a number of issues concerning identity theft. The terrorists reportedly used assumed identities to gain access to funds, training and the planes used in the attack. The end result is a sense of urgency surrounding all security issues including the accurate verification of a person's identity.

Future Identity-Security Environment

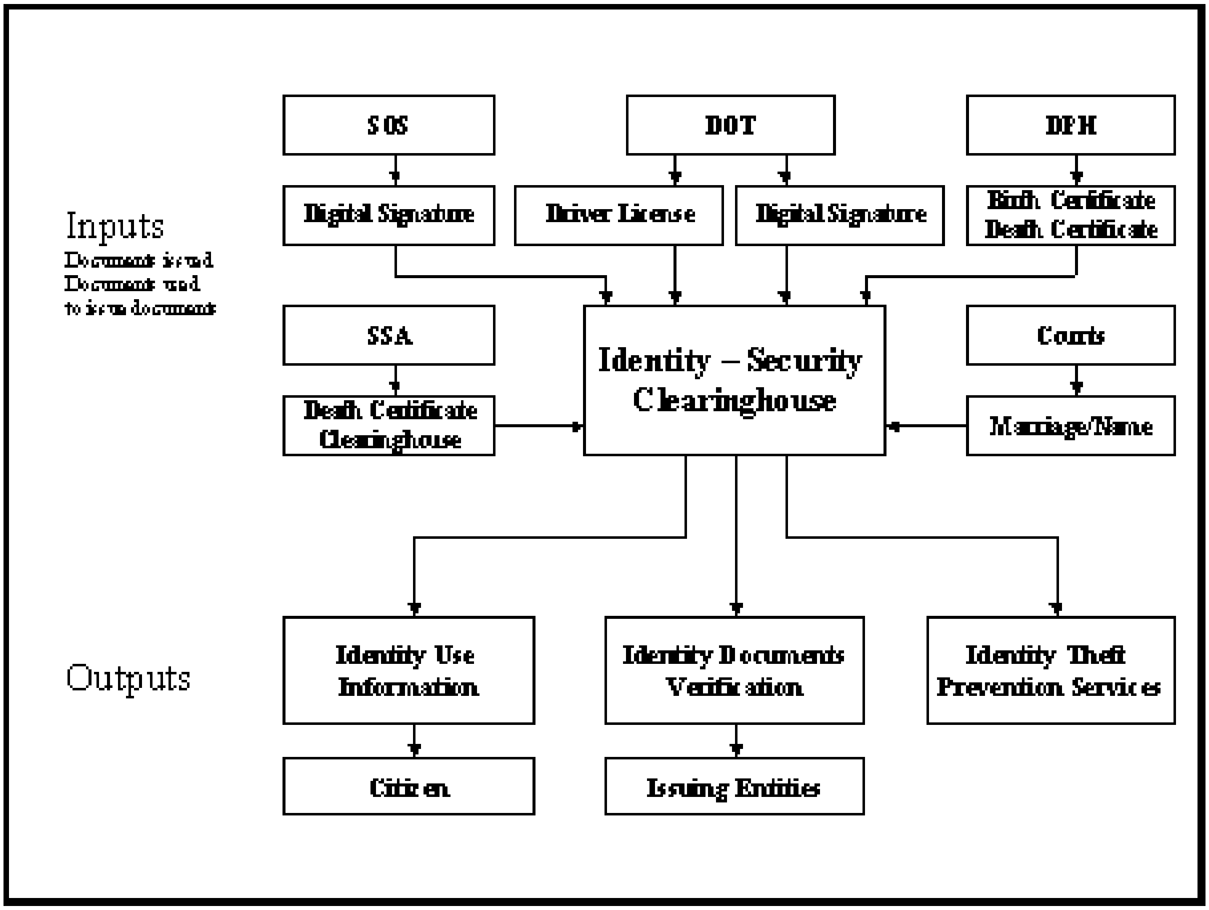
For the identity-security environment to improve, the processes for issuing identity documents need to be linked to provide verification of the documents. The previous illustration could be modified in the driver license scenario to include a layer of verification.


Future Identity Environment
Utilizing Verification of Issuer
Application
SSN
SSA
Application
Birth Certificate
Vital Records
Application, Birth Certificate, SSN
Verification
DOT
Driver License

The above example incorporates the concept of identity verification where the DOT would verify the authenticity of the documents and the identification information on those documents. Verification would eliminate the use of falsified documents, and other problems that can arise when there is a disjointed system of identity. The ITD has been working to consolidate this continuous concept of identity into an Identity-Security Clearinghouse that would perform the verification and minimize the load on the issuing entity.

Identity-Security Clearinghouse Concept

The Identity-Security Clearinghouse will link the documents used to create identity. These documents will include social security cards from the SSA, birth and death records from the DPH, driver's licenses and ID cards from the DOT, court filings such as marriage and name change filings affecting identity, and other identity documents. Identity rules and standards would be developed to ensure proper identity use.



Initial discussions on the Identity-Security Clearinghouse concept have centered on ensuring that only one legitimate birth certificate will be used to issue each social security number and each driver's license/ID. At the point of issuance for a social security number and DOT-issued driver's license/identity card (hereafter called ID), the birth certificate presented as proof of identity could be referenced against a state birth certificate database. If the birth certificate is valid and no other ID's have been issued from it, the birth certificate would be linked to ID's issued from it. The birth certificate record would also be electronically tied to the DOT photo database.

This has three advantages:

- When an ID is then presented in certain situations calling for strict security, a check could be run against the face database stored by DOT and identity could be established. (i.e. airport counter)
- Only one ID would be issued per birth certificate. This would allow easier identification of individuals attempting to falsify identity if the birth certificate is presented a second time.
- Enhanced procedures will lead to a decline of identity theft and fraud.

For residents outside of the State of Iowa, the birth certificate could initially be scanned at the point of issuance to tie it to the picture ID. (As standards are adopted for vital records databases and such databases are completed, the records would be linked in the same way as in-state records.) The basic information would be captured and indexed to cross reference against future ID issuances from the same birth certificate.

The end result would be a system that incorporates individuals, picture ID, processes, documentation, and identity. The current system does not link these components and makes identity theft too easy. Future stages would include establishing a national clearinghouse for death records that any jurisdiction could reference.

Identity-Security Benefits

The initial benefits of the Identity-Clearinghouse concept directly effect authentication methods within the State of Iowa:

- Enforcement of the 1:1 relationship between identity indicia will increase the reliability and integrity of the identity system.
- Standard methods for verifying identification will decrease the need for entities to develop their own method.
- There is potential for decreasing identity theft and fraud with State programs.

The development of an Identity-Clearinghouse also has benefits for the State of Iowa in improved customer service and enterprise data sharing.

- Digital signature implementation will bring State agencies into a "circle of trust" that will facilitate shared user authentication across multiple agencies facilitating portal growth.
- Identity data standards will allow the State of Iowa to formalize programming standards reducing development time.
- Identity standards will provide a common format for the sharing and security of information between State agencies where such sharing is permitted.
- The Identity-Clearinghouse could serve as a national model and become the one point of coordination for the State of Iowa with a federal national ID effort.

Current Status of the Iowa Project

The following actions have occurred:

- The DOT and DPH are creating a system for verifying Iowa birth certificates
- DOT is participating in AAMVA discussions on identity standards
- DPH has indexed and imaged approximately 11 million birth certificates going back to the 1890's
- ITD has facilitated a conversation between DOT, DPH, DPS, and the Social Security Administration to discuss common needs and identify future direction.

Next Steps in Iowa Project

Actions associated around this implementation of the Identity-Security Clearinghouse:

- Evaluation of documents, standards, and procedures used by issuing authority used by the DOT to confirm and establish identity. (i.e. primary and secondary documents)
- Coordination between DOT and DPH to tie individual birth certificates to an individual driver license.
- Further coordination to tie individual death certificates to the ID revocation process.
- Establishment of a history trailer for ID and related documents such as birth certificates to allow the citizen to track issuances of and requests of their ID.
- Coordination of the ability to access the DOT face database to confirm the photo ID where appropriate and allowed.
- Further development of the driver license to contain and access a unique identifier such as a PKI certificate and other biometric data.
- Consideration of a pilot to allow criminal justice, DPH, and other state agencies real-time access to the Social Security Administration.
- Align the DPH birth certificate database with national standards being developed by the National Vital Records Association and NAPHSIS.
- Instituting a timely electronic filing of death notices to the DPH and SSA
- Establishing a national clearinghouse for death and birth information.

Once these modifications have taken place, the following needs to occur:

- Adoption of identity standards (i.e. policies, procedures, and implementation) for an enterprise to secure its systems.
- Digital signature implementation based on identity standards and with the scope of Iowa Code Chapter 554D.
- Implementation of technology and policies for use of identity at secure facilities (e.g. airports).
- Implementation of Iowa Code 18.138 (Government Services Card) through the improved Iowa Drivers License/PKI systems.
- Explore the possibility of the DOT and Secretary of State becoming the issuer of PKI digital certificates.

Related actions:

- Creation of an Identity Theft Advocate in the Office of the Attorney General. This Office would help victims of identity theft and have the authority to verify their claims and through affidavits and other mechanisms, repair the credit history and reputation of the victim.

For More Information:
http://www.infoweb.state.ia.us/ecomdev/current_projects/identity/index.html