Document Security Alliance
Discussion Paper Summary

Regarding the Real ID Act, Secure ID Documents, and Related Security Processes

The Document Security Alliance (DSA) approach for implementing the Real ID Act supports a set of security principles that the Alliance developed in 2004 to provide critical guidance to state and federal issuers of identification documents as they work to improve the security of IDs to help protect citizens from the threat of identify theft, criminal or terrorist acts, and enhance homeland security. These principles identify and recommend improvements to elements of the ID enrollment and issuing processes, the credential itself, and subsequent authentication of IDs as they are used. They are based on five key elements of a **secure ID system infrastructure**:

1. **Data Capture.** Obtain the applicant's photograph, demographic information, supporting "breeder "documents (e.g., birth certificates, Social Security cards), a digital signature, and, if necessary, appropriate biometrics (e.g., facial image).

2. **Identification Verification.** Authenticate an applicant's credentials and the breeder documents they present, as well as compare select information against the issuing authority's databases or other records (e.g., Social Security Administration data).

3. **Secure ID Production.** Utilize secure workflow processes and authentication technologies to maintain the integrity of the document issuance process. It is necessary to have a robust chain of custody within the production environment, whether with central or over-the-counter document issuance.

4. **Secure ID Credentials.** Incorporate an ID card architecture that includes both difficult-to-counterfeit card materials with sophisticated laminating and finishing processes, as well as a number of overt and covert security features.

5. **Authenticating IDs.** Verify – without infringing on an individual's personal privacy – the authenticity of a proffered government-issued photo ID, no matter where it was issued, at various points of inspection or transaction – public or private sector (e.g., law enforcement, DMVs, banks or retail).

Document Purpose

The objective of the DSA paper is to provide the Department of Homeland Security (DHS) and government ID issuers with the recommendations of the Document Security Alliance regarding the writing of the regulations associated with the Real ID Act. These

regulations will have a significant impact on our society from a business practice point of view as well as affecting the daily lives of our citizens. The DSA suggests taking a practical and holistic approach considering that legacy systems (procedures and practices), interoperability, social, financial, and political barriers must be kept in mind. DSA understands that significant improvements must be made in terms of technology, machine-readability, visual security options, ongoing training and ultimately, genesis (breeder) documents. DSA feels strongly that whenever possible the benefits associated with deeply embedded existing systems and infrastructures be incorporated into any redesign. In this way minimum security system requirements can be met that will set the foundation for future Best Practice improvements. And, this will help meet the requirements in the time frame set forth in the Act, allowing DHS to develop acceptable standards.

Worldwide Security Trends

Tools are available today that put counterfeiting ability in the hands of those that previously did not have appropriate graphics or printing skills, making law enforcement's efforts to stop this crime much more difficult. The continuing sophistication of desk top color printers, color laser copiers, high resolution color scanners, imaging and editing software, digital cameras and the internet have made document counterfeiting, alteration, and photo substitution able to be performed by the general public.

To ensure the ability to discern authentic documents the use of machine-readable technologies are increasingly necessary. The DSA recommends the use of at least a minimum number of security features – two overt, two covert, one forensic and one common identifier. These features should be layered and linked on the cards. Linking ties one part of the document to another (typically by machine-readable technology) to authenticate and secure the card itself. Layering security features means the ID document does not become authentic until all of the components are included at the point of issuance. More and varied security features makes counterfeiting and alteration more difficult by raising the cost and number of technologies that must be defeated by a criminal to produce a fraudulent card.

Present Day Driver License/Identification Issuance

Standards and rules for card production should be applicable to all three existing production/distribution methods for issuing driver licenses and identification cards; over-the-counter, central, and hybrid issuance systems.

The DSA recommends *the current functional uses of the DL/ID documents must continue to be accommodated.* These are: evidence of the privilege to drive, identification of the bearer, age verification, address/residence verification, and automated administrative processing.

Verification Considerations

DSA supports the electronic verification of source document information as required by the Real ID Act. However, many of the automated systems necessary to accomplish this objective are not yet developed or available for all elements of information on a timely basis. Currently, a system exists for verification of the social security account

number through the SSOLV (Social Security On-Line Verification) system and alien status through the SAVE (Systematic Alien Verification of Entitlements) program. Having the availability of a robust verification system for birth certificates through the EVVE (Electronic Verification of Vital Events) still seems to be several years away. The same holds true for the verification of passport information with the Department of State, and military documents with the Department of Defense. In some other cases, there are source documents that may never be able to be verified with the originator of the document (e.g., verification of foreign passports will require connectivity to the foreign government that issued the document).

Additionally, source verification is only one part of a complete verification process. It allows checking if information provided on a document is correct and matches and may provide current status information. It does not, however, directly indicate if the document is genuine, nor does it tie the document directly to the bearer. Other forms of verification must also be used to perform these functions. DSA believes that by addressing all three forms of verification (legitimate document issuance, document authenticity, rightful holder), and requiring a solution in all cases, a more robust and secure issuing system will be realized.

There are different ways of authenticating and validating documents. A comprehensive and continuous training program is recommended to empower verification staff to recognize different types of identification documents. Using automated equipment and machine-readable technologies can greatly help verify if the document is genuine and has not been altered. Equipment to provide automated examination of the security features of common breeder documents is currently available. Reading the information contained on the machine-readable technologies allows comparison to other machine-readable and visual demographic data and features on the card. Also, adding the use of PINs, biometric identifiers, or digital images can help tie the person to the document.

DSA strongly recommends an upgrade in the requirements for production and security features/machine-readable technologies on all breeder documents in addition to the DL/IDs such as birth certificates, social security cards, and other documents commonly used in identification proofing for issuing DL/IDs. DSA also recommends the incorporation of new technologies to enable cross-jurisdictional point-of-inspection machine-readable ID (i.e., bar codes, digital watermarks, optical media). In implementing capabilities for cross database applicant verification, care must be taken to protect citizen privacy by not creating centralized data bases or national ID systems. Appropriate laws such as the SAFE ID (Secure Authentication Features and Enhanced Identification Defense) Act of 2003 will provide law enforcement with tools to combat ID counterfeiting.

In addition to document verification, DSA supports the requirements of source document capture, retention, and storage. Images should be captured in a digital format to improve and expedite the electronic exchange of these images within and between authorized entities for verification and investigative purposes. DSA encourages DHS to set a minimum standard (minimum resolution) for the quality of these images.

Machine-readable Technology

The Real ID Act requires jurisdictions to provide a common machine-readable technology on compliant DL/ID cards. In the real world of experience, depending solely upon a visual inspection of a document is not sufficient. DSA endorses a layered and linked security approach whereby the machine-readable data and security features are integrated with the visual data and document features to complement one another and provide a holistic approach. In order for DL/ID card systems to work both intra- and inter-jurisdictionally, one common machine-readable technology must be selected for interoperability. This is important in any environment where the reviewing party or agency is different from the issuer.

DSA recommends that the two dimensional bar code known as *PDF 417* be used as the common MRT for DL/ID documents. It is already in use by most motor vehicle agencies, is very low cost to apply, and is being used to facilitate other automated administrative activities such as law enforcement production of traffic citations and accident reporting systems. This is not meant to limit other machine-readable technologies from being placed on the DL/ID card. It is to standardize by selecting one that all cards will contain allowing universal interoperability. Other features and machine-readable technologies that serve to link data elements on the card together and secure the PDF 417 are highly desirable for card verification (genuineness) and bearer authentication.

Durability

There is a direct relationship between document security and card durability performance. Card deterioration causes authentication difficulty to determine card validity. Today, most North American DL/ID documents require a five-year card life (rarely an eight-year life) under normal use for full performance. The use of security over-laminates and highly durable coatings is recommended by DSA. At a minimum, the use performance criteria in the AAMVA International Specification - DL/ID Card Design is suggested. It should be noted that the ANSI NCITS 322 Accelerated Life Test Procedures mentioned in this specification (and others) do not claim to measure or project useful life of any tested document in terms anticipated years of performance. Actual years of ID card performance presently can only be achieved through experience. Because these tests are most helpful in creating a base performance model, however, DSA recommends their continued use.

Card based substrates should include durable materials. These materials are not limited to, but can include, composite card materials, such as a combination of PVC, polyester, polycarbonate, polyolefin (Teslin) or any other materials that can meet the performance criteria for long-term performance *and be compatible with typical printer personalization equipment presently being used in secure ID document issuance systems.*

Based on the experience of industry experts, DSA recommends a *five-year maximum card life DL/ID* with appropriately layered security features and at least a 1 mil security over-laminate to meet the requirements of the Real ID Act. The longer the number of years a card is in circulation, the more vulnerable it becomes to counterfeiting and alteration because the criminal's technology and familiarity with the older card's technology catches up to the security features. In order to keep ahead of potential

misuse and fraud, the card must be periodically changed and upgraded to more current and different security features that have not been compromised.

Physical Security

DSA presents a set of recommended physical security standards and procedures for DHS to consider for the manufacture, resale, shipping, handling, storage, inventory control, and issuance of components and finished products used for identification documents. Some of the DSA specific security recommendations for facilities, manufacturing, and storage include:

Buildings: should include alarm systems, motion sensors, electronic access controls to production areas (where security products are handled), monitoring and recording by closed circuit television cameras.

Security Materials: should be stored under secure conditions at all times, strict access control to materials areas, surveillance of areas, logs kept of every entry, record movement of materials, and periodic audits. Issuance stations should be under video surveillance, locked areas for after hour's storage, accurate inventory counts, and disposal of security waste materials by shredder or disintegrator.

Personnel: thorough background checks including criminal history, credit, driver license checks, interviews with former employers, and drug screening.

Visitor Control: pre-approval before entering secure areas and escorts at all times.

Secure Shipping Procedures: apply above security rules to materials shippers and handlers.

Training

Robust verification systems will continue to rely on humans. Even with automated technologies there will still be humans making the final determinations, reading the output of the validation and authentication equipment, and conducting exceptions processing. The DSA recommends the AAMVA Fraudulent Document Recognition Training Program and the DHS Fraudulent Document Lab Program as the basis for training the front and second line document reviewers and supervisors.

Any approved training program should contain a module that educates inspectors and review staff on the tools that deal with the familiarity and use of machine-readable technologies (logical) and security features (physical) on these documents.

Any training program should contain a continuing education or refresher training component. DSA recommends that DHS certify training programs for state's use that fulfill the requirements envisioned to deter fraud through document recognition.

ID Security Device Appendix

DSA presents a security device index (as an Appendix) to be used as a tool to aid in the security design of ID documents to cover the common threat areas to document integrity found in North America: counterfeit/simulation, alteration, photo/signature substitution and cannibalization of card components.

Document Security Alliance

REAL ID Security Recommendations

April, 2006

DSA

DOCUMENT SECURITY ALLIANCE

DSA Overview

DSA

- DSA was created as a public/private partnership to provide a forum for government agencies, private industry and academia to work with one another to focus on how to best respond to the production and distribution of counterfeit documents.
- Includes more than 70 companies and 20 government agencies who are working to continually improve security documents and security related procedures.
  - Participants include a broad representation from the credentialing industry including system integrators, card manufacturers, secure printing companies, printer manufacturers; security feature producers, encryption organizations, smart card and biometric providers, as well as security industry associations.
- Draws upon the knowledge and detailed technical disciplines of its members.
- DSA committees provide recommendations on processes, methods, techniques and technologies that can be used to improve document security.

The Need for Secure Documents

DSA

"...a driver license is the most commonly used form of identification in America...[used] to board airplanes, to buy weapons, to enter secure government facilities, to open bank accounts, to cash checks and to cross international borders. ***A driver license carries a presumption of authenticity, it establishes legitimacy.***" (emphasis added)

Rep. Christopher Cox (R-CA) – Chairman House Select Committee on Homeland Security – during testimony on October 1, 2003

"...investigations clearly show that ***border inspectors, motor vehicle departments, and firearm dealers need to have the means to verify identity and determine whether the out of state driver license presented to them are authentic.***" (emphasis added)

Robert Cramer, Managing Director, GAO Office of Special Investigations, in Testimony to the Senate Committee on Finance – September 9, 2003

Government & Association Members

DSA

- U.S. Secret Service
  - Forensic Services Division
  - Information Resource Management
  - Dignitary Protective Division
- U.S. Department of Homeland Security
  - Immigration & Customs Enforcement
- U.S. Government Printing Office
  - Security and Intelligent Documents
- Social Security Administration – Office of Investigations
- American Association of Motor Vehicle Administrators
- New York State DMV
- Food and Drug Administration – Office of Criminal Investigations
- General Services Administration (GSA) – Office of Govtwide Policy
- U.S. Department of Defense
- U.S. DOT – Maritime Administration
- National Academy of Sciences
- Federal Bureau of Investigation
- U.S. Bureau of Engraving and Printing
- U.S. Postal Inspection Service
- U.S. Treasury IG for Tax Administration
- Royal Canadian Mounted Police Forensic Lab. Services

Types of "Secure" Documents

DSA

-
  - Driver Licenses
  - Passports
  - Federal Government Credentials
-
  - Treasury and Commercial Checks
  - Postage Stamps
  - Credit Cards

Current DSA Initiatives and Focus

DSA

The **DSA** is working with specific federal agencies and groups, such as Department of Homeland Security, Health and Human Services and the Social Security Administration on recommendations for:

- Security for FIPS – 201 compliant credentials
- Minimum security for US Birth Certificates.
- Security of Social Security Cards
- Security of Driver Licenses and other State issued IDs

Some Document Security Challenges

DSA

- Advances in imaging/printing technologies which have made it easier for criminals and terrorists to counterfeit identity documents
- Ease of obtaining fraudulent IDs or other breeder documents in the US
- Security holes in the issuance process for government issued ID's that make it possible to fraudulently acquire genuine IDs
- Variety of ID formats and counterfeiting technology has made visual ID authentication insufficient
- Lack of method for machine readable cross jurisdictional authentication of IDs or access to other information regarding an ID holder
- Widespread use of fraudulent IDs to perpetrate criminal or terrorist acts and gain access to:
  - Transportation systems and secure government or private sector facilities
  - Restricted goods (such as firearms or alcohol for minors)
  - Bank accounts or credit
  - Cross borders and gain entrance to, and remain in, the US

Elements of a Secure ID System

DSA

- – Obtain the applicant's photograph, demographic information, supporting documents (such as breeder documents), a digital version of his/her signature, and, if necessary, appropriate biometrics (e.g., facial image or fingerprint).
- – Authenticate an applicant's credentials and the breeder documents they present, as well as comparing select information against the issuing authority's databases or other records (e.g., Social Security Administration data).
- – Utilize processes and technologies that enable secure ID issuance.
- – Incorporate a layered durable card architecture that includes both difficult-to-counterfeit card materials with sophisticated laminating and finishing processes, as well as a number of overt, covert and forensic security features.
- – Verify – without infringing on an individual's personal privacy – the authenticity of a proffered government-issued photo ID, no matter where it was issued, at all various points of inspection or transaction – public or private sector (e.g., law enforcement, transportation, DMVs, banks or retail).

DSA DL/ID Recommendations

DSA

- Ensure the current functional uses of DL/ID documents continue to be accommodated, including:
  - Evidence of privilege to drive, identification of bearer, age verification, address/residence verification and automated administrative processing
- Ensure all "Elements of a Secure ID System" are addressed including Data Capture, Verification, Secure Production, Secure Credential and Authentication
- Upgrading security requirements and authentication capabilities for "breeder" documents (birth certificates, social security cards, etc.) used in issuing IDs
- Electronic scanning and archiving for document capture, retention and storage

DSA DL/ID Recommendations

DSA

- 2D Barcodes (PDF-417) as the standard overt machine-readable technology for carrying data
- Incorporation of new technologies to enable cross-jurisdictional point of inspection human and machine-readable ID authentication (such as barcodes, digital watermarks and optical media)
- Support for current major issuing methods (Over-the-Counter, Central, Hybrid) with security process improvements that enable verification processes and provide better control over materials and security features
  - Including establishing Physical security of materials and facilities
- Implement document durability and performance standards including use of composite cards, PVC and polyester, polycarbonate, Teslin or other card materials that can meet the performance requirements and that are compatible with current typical personalization equipment presently being used in secure ID issuance systems

DSA DL/ID Recommendations

DSA

- Implement capabilities for electronic cross database applicant verification with systems such as SSOLV, SAVE and eventually EVVE, Dept of State and Dept of Defense databases as appropriate (*not* centralized databases or National IDs systems)
- Establishing Security Conscious ID Validity Periods of five years to ensure accurate records and enable security feature renewal/upgrade
- Training on fraudulent documents and human-verifiable and machine-readable features of credentials
- Providing appropriate resources to state DMVs and other government issuing authorities to upgrade issuance processes and incorporate new security features

States Already Taking Action

DSA

Most states taking active steps to upgrade security

45 States already using 2D Barcodes

As depicted in the map, over 85% of states now use Social Security Number Verification System

Source: AAMVA

Summary

DSA

- DSA is a forum of government agencies, private industry and academia dedicated to improving security documents and related security procedures and is focused on how to best respond to the production and distribution of counterfeit documents.
- DSA is identifying new trends in counterfeiting and identifying approaches, through technology, processes or best practices, to improve document security
- DSA has combined the expertise of its members to provide security recommendations for Driver Licenses and IDs associated with the REAL ID Act to DHS and government ID issuers
- DSA will act as a resource for government agencies, policy makers and private industry to improve ID security.
- Visit for more information.