

# **PRESENTATION TO AAMVA BOARD**

**January 3, 2002**

**Prepared By:**

**AssureTec Systems, Inc.**

**In Cooperation With:**

**UNISYS Corp.**

**&**

**3M Corp.**

## INTRODUCTION

***It is our hope that each member of the AAMVA Board will review this document prior to discussion or public announcement of any action with regard to AAMVA's position on the use of the state DL/identity documents currently issued by its members for a more official role as an nationwide, secure ID.***

***AssureTec Systems, Inc. prepared the following paper in cooperation with Unisys Corporation and 3M Corporation.*** The intent is to provide a document to facilitate open dialogue on the broad pragmatic issues that need to be addressed in order to achieve a solution to meet the many identity verification needs that are vital to protecting a free society while helping to protect the privacy of its citizens and visitors.

The paper describes an approach that facilitates quick improvement in security and avoids the many political, jurisdictional, infrastructure (interoperability), cost, and privacy concerns that represent major hurdles for other approaches. It is focused on the role that AAMVA and its members could play in providing such a solution. There are other elements outside of those described that are needed to provide the maximum impact for a society-wide solution. The same principles described herein can be re-phrased to reflect the necessary steps required for issuing a secure/verifiable passport, visa, or other travel document.

The views and suggestions expressed in the document are not meant to be all-inclusive. Nor are the suggestions necessarily ones that can or need to be adopted exactly as presented. ***Many of these views were expressed conceptually by participants at the November Security Task Force meeting in Cincinnati and at the recent joint security conference held in Washington between invited guests of the AAMVA IAB and the US Secret Service.*** At the Washington meeting there were many ideas presented concerning specific technology for card security, biometric usage, materials control, and interoperability. Several committees have been formed to investigate these ideas in greater depth.

This document was in preparation well before that meeting and a “draft” version was distributed to those who expressed an interest. Though it is marked as “Company Proprietary,” we recognize that many of the components of the overall system described are in the public domain or would have to be moved to the public domain for general acceptance.

**There are many specific details that have been deliberately omitted to avoid the impression of complexity and inflexibility. There needs to be a consensus built that shortens debate and moves us rapidly toward real improvements in security. Many issues that should be addressed to provide the “best” solution need to be put into the context of practicality and prioritized for consideration at the appropriate time.**

Company Proprietary to AssureTec – Patents Pending on some elements discussed.

CONTACT INFORMATION:

AssureTec Systems Inc.  
603-641-8443 x17

Bruce Monk, President  
[Bruce.Monk@assuretec.com](mailto:Bruce.Monk@assuretec.com)

Unisys Corporation  
603-930-3840

David Wells, Account Manager  
[David.Wells@unisys.com](mailto:David.Wells@unisys.com)

3M Security Market Center  
651-737-4454

Steven J. Harrold, Business Director  
[sharrold@mmm.com](mailto:sharrold@mmm.com)

## The DMV as an Identification Document Issuer

### OVERVIEW:

**Background:** Some examples of “primary” identification documents (IDs) include:

- Passport/Border Crosser Card } non-citizens
- VISA } non-citizens
- Alien Resident Card } non-citizens
- Driver license or other state-issued ID Card } citizens/alien-residents

The following suggestions are offered in support of the position that evolution of the current US Driver’s License/State ID system represents the most expedient, cost-effective, and, ultimately, the most secure approach to providing positive identification. The system is designed to protect privacy while becoming an integral element in protecting society from terrorism and the scourges of identity theft and identity fraud.

The positive impact of being able to “...know who you are dealing with..” reflects very broadly across our society. There are security/safety, economic, and social benefits. The opportunities to participate in the design, implementation, installation, support, and operation of the many systems and sub-systems are intuitively very large. Table 1 briefly illustrates some of the areas of opportunity where there is a substantial benefit to individuals, institutions, or society as a whole.

<b>Table 1: Opportunities</b>	
<b>Market</b>	<b>Application</b>
<b>Transportation</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for:                             <ul style="list-style-type: none"> <li>○ all public transportation access</li> <li>○ car/truck/plane rental or leasing</li> <li>○ operator licensing                                     <ul style="list-style-type: none"> <li>▪ automobile, motorcycle, commercial, train ...</li> <li>▪ plane</li> <li>▪ marine/vessel</li> <li>▪ hazardous material</li> </ul> </li> </ul> </li> </ul>
<b>Financial</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for:                             <ul style="list-style-type: none"> <li>○ check cashing</li> <li>○ high-value credit purchases</li> <li>○ bearer bond transfers</li> <li>○ securities exchange</li> <li>○ funds transfers</li> <li>○ leasing</li> </ul> </li> </ul>
<b>Controlled Substances</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for purchase of:                             <ul style="list-style-type: none"> <li>○ firearms</li> <li>○ purchase of explosives</li> <li>○ controlled drugs</li> <li>○ hazardous materials</li> </ul> </li> </ul>

**Table 1: Opportunities (continued)**

Market	Application
<b>Age Restricted Access</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for access to:                             <ul style="list-style-type: none"> <li>○ alcohol and tobacco</li> <li>○ lottery tickets</li> <li>○ adult entertainment</li> </ul> </li> </ul>
<b>Public Safety</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for                             <ul style="list-style-type: none"> <li>○ employment of:                                     <ul style="list-style-type: none"> <li>▪ federal/state/local police officers</li> <li>▪ prison guards</li> <li>▪ judiciary</li> </ul> </li> <li>○ suspects/detainees</li> <li>○ witnesses</li> </ul> </li> </ul>
<b>Public Trust</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for employment of:                             <ul style="list-style-type: none"> <li>○ daycare workers</li> <li>○ nursing home/healthcare workers</li> <li>○ bus drivers</li> <li>○ youth coaches</li> <li>○ scout masters</li> <li>○ teachers</li> </ul> </li> </ul>
<b>Public Services</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for potential fraud in distribution of benefits for:                             <ul style="list-style-type: none"> <li>○ welfare</li> <li>○ social security</li> <li>○ Medicaid/Medicare</li> <li>○ unemployment</li> </ul> </li> </ul>
<b>Property Transfer</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background checking for potential fraud in sale of:                             <ul style="list-style-type: none"> <li>○ real estate</li> <li>○ art</li> <li>○ antiques</li> <li>○ collectables</li> </ul> </li> </ul>
<b>Professional Licensing</b>	<ul style="list-style-type: none"> <li>- real-time background checking for falsification of records or qualifications for:                             <ul style="list-style-type: none"> <li>○ doctors and nurses</li> <li>○ lawyers</li> <li>○ plumbers, electricians, ...</li> <li>○ architects</li> <li>○ beauticians</li> </ul> </li> </ul>

<b>Table 1: Opportunities (continued)</b>	
<b>Market</b>	<b>Application</b>
<b>Border Management</b>	<ul style="list-style-type: none"> <li>- effective security, real-time background verification or status of:                             <ul style="list-style-type: none"> <li>○ previous entry violations</li> <li>○ proper documentation</li> <li>○ proposed itinerary</li> <li>○ “wants” or “warrants”</li> </ul> </li> </ul>
<b>Taxation</b>	<ul style="list-style-type: none"> <li>- potential fraud, such as:                             <ul style="list-style-type: none"> <li>○ tax evasion</li> <li>○ tax avoidance through multiple identities</li> <li>○ failure to report</li> </ul> </li> </ul>
<b>Corporate Security</b>	<ul style="list-style-type: none"> <li>- real-time background screening for:                             <ul style="list-style-type: none"> <li>○ vendor access</li> <li>○ hiring</li> <li>○ temporary facility access</li> <li>○ rental agreements</li> </ul> </li> </ul>
<b>Insurance</b>	<ul style="list-style-type: none"> <li>- real-time risk assessment (exposure) for:                             <ul style="list-style-type: none"> <li>○ personal liability insurance</li> <li>○ malpractice insurance</li> <li>○ financial liability insurance</li> </ul> </li> </ul>

**System Overview:** The generalized process is the same for all “Issuance Authorities.” A fundamental assumption is that an applicant explicitly grants permission to crosscheck the information they provide when seeking to be issued an ID and, similarly, when they use the ID to carryout a transaction (i.e. at the “point of use”) they grant permission to validate it using all information contained thereon/in.

In order to ensure the ID created is issued to someone entitled to the direct and indirect privileges it conveys, there must be a high confidence that:

- 1.) The applicant is who they say they are
- 2.) They meet established qualification and/or testing criteria
- 3.) There are no constraints/concerns that disqualify the applicant from being granted the privilege

Once these criteria have been met an ID can be created. However, in order to ensure that the ID truly represents that the privileges granted are due the bearer of the document, it must be able to convey to the examiner at the point of use:

- 1.) Proof that it was issued by the appropriate authority
- 2.) Confidence that it has not been altered
- 3.) Evidence that it belongs to the bearer
- 4.) Assurance that it has not expired, been suspended, or been revoked.

Simply creating an ID document does not absolve the issuance authority from its responsibility to help protect those organizations that rely upon the ID from fakes/forges and fraudulent issuance or use. Because these organizations have varying degrees of “value” or “risk” associated with the transaction or privilege being granted each factor will vary in criticality.

In some instances a simple personal check of the physical attributes of the document; photo on the document, indication of bearer’s age and an expiration date are sufficient. However, people have many failings and the security offered by even these simple checks can fall victim to boredom, indifference, bribery, distractions, or intimidation. Features, even very sophisticated ones, which are readily verified by humans under normal lighting variations and working condition, can often be duplicated or simulated with sufficient quality to pass most casual inspections.

Even an authentic document does not convey to the inspector whether or not it has been suspended or revoked and, therefore, might no longer be valid! Hence, comes the need for characteristics that are not readily simulated and very difficult to forge or alter. These characteristics generally require aid to the human senses for manual verification and this means added inspection time and equipment that is simply impractical. Also, there is still the need for real-time status checking on the validity of the document. This level of inspection is most efficiently done if it is automated through use of biometric(s), data, and document characteristics that are machine-readable and verifiable.

The public’s trust given the issuance authority demands evaluation of all available information before granting the privileges conveyed by the ID. This trust implies that the information provided will be protected and used only for the purpose provided. The applicant explicitly believes that the ID when issued will be accepted and function reliably and securely. This requires the issuer’s proactive participation in protection of the integrity of the document, in verification of the link to the bearer, and support for the process necessary to validate its current status.

An approach for the issuance of a driver’s license that meets these criteria can be summarized as follows:

- A) During enrollment, collect sufficient information to guarantee:
  - 1.) The applicant has used this identity for an extended period of time (hopefully since birth!)
  - 2.) That there has been no behavior which would prevent issuance of a license
  - 3.) That the applicant is qualified and physically capable
  - 4.) That the information (biometrics and data) is sufficient to positively link the applicant to this transaction.
- B) Create a DL, which facilitates human verification and data extraction, as well as, machine verification and data extraction. Seal this document and its contents in such a manner as to inextricably link the biometric(s), data, and document characteristics.
- C) Provide a means to support both manual and automated validation of the issuance of said DL and its current validity while protecting the privacy of the information entrusted to them.

## **SUGGESTIONS FOR PRIMARY ID ISSUERS**

### **THE ENROLLMENT PROCESS:**

#### **NEW IDEAS:**

- 1.) Require a secure background check before issuance of the ID.
- 2.) Establish an independent risk indicator for the ID to alert the examiner that there is a risk issue for applicants where there is only limited information or information that is very difficult to verify available; such as for recent arrival, foreign-born applicants.
- 3.) Establish sensible standards for scoring the risk factor (similar to the current point system). Weight independent data sources much higher than derivative ones. Current DL information is a clear example of derivative information!
- 4.) Recommend central issuance as a more secure approach than over-the-counter issuance because it limits access to materials which largely constitute the ID's standalone security
- 5.) Build in a delay to the process sufficient to allow such background checking
- 6.) For each first time application under the new system, automatically collect an application in advance containing information to be used specifically for identity verification through creation of a datametric, such as:
  - A) Personal information (parents names, DOB, place of birth, marital data, citizenship status...)
  - B) Geographic information (current and past residence)
  - C) Employment/public assistance history
  - D) Military Service information
  - E) Academic information
  - F) Financial information
- 7.) Use of an "ID Clearinghouse" (AAMVA service bureau?) to automate data capture and verification against existing commercial and government databases. Apply strict guidelines to minimize retention of personal data and adopt a methodology that supports the verification process without requiring the "owners" of these databases to provide the actual data. Only an indication of the degree to which the data on the application matches is required.
- 8.) Establish "anonymous" datametric database to facilitate screening for potential duplicate identities without using actual personal information.
- 9.) Set mandatory photo capture and size/quality standards
- 10.) Recommend voluntary capture of second biometric (iris scan or fingerprint(s)) for backup duplicate evaluation or ID confirmation for high-risk situations.
- 11.) Restrict period of ID validity to less than 5 years
- 12.) Require replacement of ID whenever a substantial appearance-altering event occurs such as growing a beard/mustache or cosmetic surgery.
- 13.) Require that all subsequent renewals should include biometric verification and an update of the information covering the period of time since the previous application.

Company Proprietary to AssureTec – Patents Pending on some elements discussed.

- 14.) Build into the process the ability to seamlessly adapt to take advantage of future improvements in the security of breeder documents such as birth certification standardization and linked death certification, etc.
- 15.) Log all steps in the enrollment process including, but not limited to: operator (password), location, station, date/time, edits/changes.
- 16.) Audit the event log from above against the issuance event log generated and generate a reconciliation report that highlights any deviations from “normal” practice.
- 17.) Distribute said report to internal management authorities and an independent audit authority (AAMVA?).

### IMPACT:

- 1) Much shorter implementation time than would be required for the mammoth infrastructure changes necessary to correct many issues with breeder documents.
- 2) Higher degree of security than breeder document approach due to integration of biometric and datametric cross-verification. Note neither birth nor death certificates have a positive biometric link to an individual.
- 3) More efficient (less expensive) and easier to administrate than individual state implementations, especially for smaller jurisdictions
- 4) Consistent standard for enrollment data.
- 5) Assures interoperability amongst jurisdictions.
- 6) Allocates expenses on a “per transaction” basis that assures affordability to smaller jurisdictions.
- 7) Facilitates cross-state identity checking without privacy evasion (anonymous datametric database).
- 8) Alerts the point of use that closer screening of the document bearer might be appropriate.
- 9) Automates alerts for potential fraud by in the front-end enrollment process.

### **ID CREATION:**

### NEW IDEAS:

- 1.) Eliminate all non-essential data on the ID, including SSN, DOB, address, sex, hair, wt. etc. retain only name, DL#, expiration date, transaction code, organ donor status.
- 2.) Do not algorithmically create DL # using DOB or SSN.
- 3.) Establish a random document expiration date in 1 yr period following the “N” year validation period (avoid link to DOB).
- 4.) Use specific card delimiters for < 18, <21, > 70 etc.
- 5.) Add “confidence” identifier based on score achieved where there is no evidence warranting denial of driving privilege, but insufficient information/quality of information for absolute identity verification.
- 6.) Create a machine-readable code (MRC) linking photo, data, a transaction code, biometric(s), and intrinsic card characteristic. Encryption of the MRC can be specified but it is not critical since the intent is for machine readability and verification at the point of use against ID properties and local or central lists of valid IDs.

- 7.) Standardize basic card layout.
- 8.) Use protected write-once, multi-dimensional barcode with symbology size suited to reliable reading to store the MRC. Locate it in a standard place on the card to facilitate low-cost optical readers.
- 9.) Mandate use of overt inks that facilitate machine-readability in the presence of optical protection devices and represent a security feature in themselves. For example inks/dyes with unique IR absorption properties (especially if the distribution can be regulated), i.e. color/clear vs. use of resin/carbon black.
- 10.) Establish rigid guidelines for photo quality and size (at least 1.25"W X 1.5"H).
- 11.) Avoid security features that compromise the ability to view the photo under all lighting conditions.
- 12.) Avoid use of any on-card mass storage mechanism (smart card, large 2-D barcode, etc) containing information that is non-essential to the identification of the bearer and verification of authenticity.
- 13.) Log all steps in the issuance process including, but not limited to: operator (password), location, station, date/time, edits/changes.
- 14.) Log all inventory adjustment events; such as, material received, cards produced, scrap, ...
- 15.) Audit the event log from above against the issuance event log generated and generate a reconciliation report that highlights any deviations from "normal" practice.
- 16.) Distribute said report to internal management authorities and an independent audit authority (AAMVA?).

IMPACT:

- 1) Easier for inspector to validate photo and security features at a glance.
- 2) Easier for inspector to read and compare names.
- 3) Protects privacy by limiting access to information such as DOB, SSN, and address.
- 4) Allows for introduction of low-cost automated authentication devices.
- 5) Facilitates inspector and machine 1:1 facial matching.
- 6) Sets standards for security and facilitates periodic nationwide changes in security characteristics.
- 7) Reduces cost and aids law enforcement by allocating more space to and facilitating automation of the items needed for validation against central records.
- 8) Establishes self-authentication properties/process for the ID that will improve even further as new technology is adopted periodically to link better controlled materials with unique identifiable "documetric" (intrinsic document characteristics) to the datametric and biometric.
- 9) Automates alerts for potential fraud, collusion, or material theft related to the ID creation process.

## **VALIDATION SUPPORT:**

### NEW IDEAS:

- 1.) Implement jurisdictional “Trust Authorities” that:
  - a. Support manual validation by authorized agents, i.e. through touchtone DL# vs. Transaction code vs. expiration date. Report DL status valid/invalid.
  - b. Support automated validation of data + graphic (photo) for current issue and MRC when implemented.
  - c. Protect data by providing only query matching to authorized users.
  - d. Support 1:1 biometric matching to resolve potential duplicate identities.
- 2.) Integrate links to authorized judicial and law enforcement agencies to “flag” the status of the ID stored by the Trust Authority.
- 3.) Establish a special Trust Authority (ID Clearinghouse) anonymous datametric database (under AAMVA management?) to facilitate detection of duplicate/multiple identities.
- 4.) Log all query transaction codes as keywords in ID holder record to support law enforcement inquiries when authorized.

### IMPACT:

- 1) Assures interoperability amongst jurisdictions and federal agencies.
- 2) Fast and comparatively low-cost to implement.
- 3) Preserves traditional issuance roles.
- 4) Preserves responsibilities of current owners of relevant database information.
- 5) Maintains the “trust” relationships that are in place.
- 6) Opens real-time validation to everyone with “a need to know”, but protects privacy while doing so.
- 7) Self-funding, usage fee charged for non-AAMVA or law enforcement participants
- 8) Validates all current documents and tracks confidence in the security as the ideas above are implemented.
- 9) Simple to administer either directly by the jurisdiction or by a third-party trusted outsourcing vendor.
- 10) Easy to implement because a common template and guidelines would be created for all jurisdictions that would only require minor editing relative to specific IT/network issues.
- 11) Facilitates federal implementation of an anonymous activity database that stores information relative to activity at points of use but contains no personal data. This database would be used to implement neural network searches looking for patterns of travel and other activities independently and in relationship to other patterns. This type of analysis is critical to advanced threat analysis for all kinds of criminal behavior and not just terrorism.

If a potential threat is detected then law enforcement can trace the pattern to the issuer of the ID to further investigate. This type of analysis provides the “ounce of prevention” that can aid interception of the conspiracy to commit a crime and avoid the actual commission of the crime and subsequent need to find and prosecute the criminal, i.e. the “pound of cure.” In the event the crime is not prevented the pre-compilation of such information will greatly improve the tools that law enforcement would have to rapidly locate and apprehend the suspect(s).

## **AAMVA ID CLEARINGHOUSE CONCEPT:**

### **Overview:**

There are several benefits to the Jurisdictions if a third-party (the ID Clearinghouse) provides a standardized infrastructure and methodology to support the driver's license application process. The enrollment system elements that are readily outsourced include:

- 1) Data capture
- 2) Data Validation
- 3) Multiple Identity crosschecking.

It is important to note that the ID Clearinghouse's sole function is to support positive identification of the applicant by verifying the information supplied on their application form. The Clearinghouse would retain no personal data and no biometric information would be passed to it. The individual state Trust Authorities would be responsible for protection of all personal data including biometric information. Any final assessment of possible multiple identities will ultimately be made through communication between Jurisdictions through the Trust Authorities.

This approach adapts to the variations in current processes and procedures used by each Jurisdiction. Therefore, this architecture provides the following benefits:

- 1) The needs of all sizes of DMV can be met cost effectively, because the business model used is primarily "usage" based charge with a fixed monthly support/maintenance payment.
- 2) There would be no need for individual state capital expenditures
- 3) Privacy is protected.
- 4) Datametrics provides a faster and more accurate means for identity screening
- 5) The enrollment security improvements can be realized almost immediately since the data needed for crosschecking is already available in databases.
- 6) There is no need to wait for the birth/death certification process to be upgraded/standardized because that information is only one element in the overall datametric for the individual.
- 7) Existing costs are lowered for the DMV because the Clearinghouse provides elements such as data entry.
- 8) Internal security problems from employee collusion are minimized through integrated auditing by the third-party.
- 9) As the physical security features of the ID are enhanced, the integrity of the data protected will match the improvement in protection!
- 10) On-line validation can immediately provide enhanced security using current data through the Trust Authority and get steadily better as the enrollment process is tightened up.
- 11) There is minimal change required to any existing DMV legacy system.
- 12) Enhanced security can be achieved while issues such as instant vs. central issue, card layout standardization, and what/how biometrics on the card are addressed.