

# **SMART CARD USAGE**

*in*

## ***Motor Vehicle Administration***



**AMERICAN ASSOCIATION  
OF MOTOR VEHICLE  
ADMINISTRATORS**

## EXECUTIVE SUMMARY

This document is a product of the American Association of Motor Vehicle Administrators (AAMVA) Smart Card Working Group's fact findings, lessons learned, and exploration of industry usage. The Working Group has sought to explore possible uses of smart cards for Departments of Motor Vehicles (DMV's) applications.

The purpose of this document is to assist jurisdictions in their efforts to explore Smart Card technology and to apply this knowledge base as a tool in making decisions for existing and future applications.

This product has been reviewed by the Smart Card Working group and approved by the Motor Vehicle Information Systems (MVIS) Committee.

The information presented in this document includes:

- How jurisdictions can use the technology
- The required hardware, software and communications infrastructure
- Advantages/disadvantages of the technology
- How industry can assist with the implementation of the technology
- Types of standards required
- Implementation costs to the jurisdictions
- How and by whom the technology will be used
- Guiding principles for the use of the technology

Smart Card technology offers many potential enhancements to card technology and may be of significant benefit to all card issuing organizations in the future. However, the Working Group identified no strong business case for the use of smart cards in either driver licensing or vehicle registration applications at this time. Any jurisdiction considering the use of smart card technology should first complete a thorough investigation of the cost to implement (these costs include the card itself and the infrastructure required to use it throughout the jurisdiction). It should also consider the availability of standards, educating the users, the legal issues associated with the use of the technology, and any private public partnerships under consideration. Most importantly, a jurisdiction should consider/examine/et cetera the willingness of the public to embrace and use the technology.

## TABLE OF CONTENTS

Executive Summary .....	ii
1. Mission Statement.....	1
2. Purpose .....	1
3. Background .....	1
4. Objectives .....	1
5. Conclusions and Recommendations .....	2
6. Smart Card Principles.....	2
7. Description of Smart Card Technology.....	3
8. Smart Card in Commercial Vehicle Operations .....	5
8.1. Smart Driver's License.....	5
8.2. Smart Vehicle Card (SVC).....	5
8.3. Smart Card Electronic Toll Collection (ETC).....	5
9. Standards for Smart Card Technology .....	6
9.1. Driver's License Standard Working Group Composition .....	6
9.2. Project Activity by Time Line.....	8
9.3. Development of a Standard API (Application Programming Interface).....	8
10. AAMVA Best Practices for Magnetic Stripe and Bar Codes .....	8
11. IAB Smart Card White Paper .....	11
General .....	14
Overview of Smart Card Technology.....	14

<b>Application and Migration .....</b>	<b>15</b>
<b>Practical Applications .....</b>	<b>15</b>
<i>Electronic License Renewal.....</i>	<i>15</i>
<i>Electronic Vehicle Registration.....</i>	<i>16</i>
<i>Use of Smart Card Chip by Multiple Agencies.....</i>	<i>16</i>
<b>Contact Cards (Chip on the surface of the card).....</b>	<b>16</b>
<b>Card Type - ISO Compliance.....</b>	<b>16</b>
<i>Physical Characteristics.....</i>	<i>16</i>
<i>Electrical Characteristics.....</i>	<i>16</i>
<b>Physical Card Features .....</b>	<b>17</b>
<b>Electronic Features .....</b>	<b>17</b>
<b>Contactless Cards (Chip or Thin Film beneath the surface of the card) .....</b>	<b>18</b>
<i>Radio Frequency (RF) Technology.....</i>	<i>18</i>
<b>Card Operating Systems.....</b>	<b>18</b>
<i>Answer to Reset.....</i>	<i>19</i>
<i>Memory/File Management .....</i>	<i>19</i>
<i>Memory Protection (Card Security).....</i>	<i>20</i>
<i>Passwords and Password Management.....</i>	<i>20</i>
<i>Electronic Purse.....</i>	<i>21</i>
<i>Cryptography.....</i>	<i>21</i>
<i>Multi-Functional Data Carrier.....</i>	<i>22</i>
<b>Card Personalization/Initialization .....</b>	<b>22</b>
<b>Committee Conclusions .....</b>	<b>23</b>
<b>Appendix A - Glossary of Acronyms.....</b>	<b>24</b>
<b>12. Smart Card Legal Issues: A Preliminary Review (Draft) .....</b>	<b>25</b>
<b>13. Smart Card Customer Service Issues: A Preliminary Review (Draft) .....</b>	<b>28</b>
<b>14. Smart Card Model Legislation .....</b>	<b>34</b>
<b>15. Smart Card Survey .....</b>	<b>36</b>
<b>16. Smart Card Survey Results.....</b>	<b>43</b>

**17. Current Applicable Uses and Experiences of Others..... 55**

**17.1. United States..... 55**

**Indiana..... 55**

**New Jersey ..... 55**

**Ohio..... 55**

**Utah..... 56**

**17.2. Overseas..... 56**

**Malaysia..... 56**

**18. Smart Card Working Group Members..... 57**

**19. Further Information**

**Appendix A..... 61**

## **1. MISSION STATEMENT**

The mission of the American Association of Motor Vehicle Administrators (AAMVA) Smart Card Working Group is to assist jurisdictions in their exploration of Smart Card technology and to apply this knowledge base in making decisions about existing and future applications.

## **2. PURPOSE**

The purpose of this document is to assist jurisdictions in their efforts to explore Smart Card technology and to apply this knowledge base as a tool in making decisions for existing and future applications. This document is a product of the Working Group's fact findings, lessons learned, and exploration of industry usage. The final product, once reviewed and approved by the Smart Card Working group, will be reported to the Motor Vehicle Information Systems (MVIS) Committee for further consideration.

## **3. BACKGROUND**

The driver license has become a de facto identification card. In addition to its original purpose, the driver license is used or is envisioned for use in motor voter, social services, gun-control, "dead-beat parents", cashing checks, social control/social service and other applications.

In its research role, the MVIS committee should play an integral role in exploring current and emerging technologies in order to advise AAMVA of possible uses of smart cards. Motor Vehicle Administrations (MVA's) may well be the supplier of smart cards for non-DMV agencies, such as social services, social administration and health care services.

## **4. OBJECTIVES**

The objective of the AAMVA Smart Card Working Group is to investigate smart card technologies and identify potential applications for motor vehicle operations. This working group will be responsible for establishing communications with other Smart Card organizations and foster the development of technical standards when appropriate.

It is envisioned that the MVIS Smart Card Working Group would deliver a document outlining the potential usage of smart cards. Additionally, the viability of a pilot project would be undertaken if deemed appropriate by the AAMVA Board.

To accomplish these objectives the working group focused on the following:

- How jurisdictions can use the technology
- The required hardware, software and communications infrastructure
- Advantages/disadvantages of the technology
- How industry can assist with the implementation of the technology
- Types of standards required
- Implementation costs to the jurisdictions
- How and by whom the technology will be used
- Guiding principles for the use of the technology

## **5. CONCLUSIONS AND RECOMMENDATIONS**

Smart Card technology offers many potential enhancements to card technology and may be of significant benefit to all card issuing organizations in the future. However, the Working Group identified no strong business case for the use of smart cards in either driver licensing or vehicle registration applications at this time. Any jurisdiction considering the use of smart card technology should first complete a thorough investigation of the cost to implement (these costs include the card itself and the infrastructure required to use it throughout the jurisdiction). It should also consider the availability of standards, educating the users, the legal issues associated with the use of the technology, and any private public partnerships under consideration. Most importantly, a jurisdiction should consider/examine/et cetera the willingness of the public to embrace and use the technology.

## **6. SMART CARD PRINCIPLES**

- The data stored electronically on a smart card must be secure, yet accessible, by commercially available equipment that can be competitively procured.
- Due to the initial investment, participation in any smart card venture should be voluntary. The costs attributed to the smart card should be fairly distributed.
- Smart card applications should be simple and easy to use yet possess safeguards to discourage fraud.
- Secure information so individuals have secure access yet provide firewalls to prevent unauthorized usage.
- Information on the smart card must be maintainable and updatable (on non-static applications).
- Jurisdictional smart card applications outside of the driver/vehicle domain should consider using the driver's license card because of its widespread acceptance as an identification document.
- The addition of smart card technology shall not inhibit the core functionality of the driver/vehicle document.

- Smart card technology must be implemented according to established standards to ensure seamless use of the card throughout all AAMVA jurisdictions.
- Smart card technology in motor vehicle documents must provide interoperability, to the greatest extent possible, with smart card technology in other public and private sector applications.
- Smart card standards should provide flexibility for reasonable options.
- Driver/vehicle documents utilizing smart card technology should support existing technologies, such as magnetic strip and bar code, to ensure compatibility for all card users that invested in those technologies.

## 7. DESCRIPTION OF SMART CARD TECHNOLOGY

A Smart Card (or “chip card”) is a plastic card with a microprocessor, capable of calculations, embedded within it. An integrated circuit (IC) is used as the chip type. The Smart Card retains information in electronic form and is capable of controlling access to and allowing modification of that information. The integrated circuit within the Smart Card holds information in such a way that it can be easily, accurately and securely accessed by authorized persons or agencies through the use of a “reader” or data processing equipment.

Smart Cards are divided into two different types: a memory card and a microcomputer integrated circuit. The memory card simply stores information or values. A good example of this is a phone card or toll card. The “microcomputer” (which is a true Smart Card) allows several different types of access, discussed in the proceeding paragraph. This chip contains a Central Processing Unit (CPU) capable of storing and securing information and making decisions based on the user’s specific application. Essentially, a memory card only “memorizes” information, a microcomputer card can contain random-access memory, read-only memory and nonvolatile memory.

Think of the microprocessor-controlled smart card as the electronic equivalent of a bank’s storage area which contains hundreds of individually-locked safety deposit boxes, and you have some idea of its ability to compartmentalize and safeguard individual fields of data. A chip operating system (COS) limits access to data stored in the microchip. The COS may come with a manufacturer’s secret key which, when combined with the issuer’s secret key, gives the issuer complete control over the main directory, each sub-directory and every field of data. In a fashion similar to modern relational database programs, the issuer would have the power to establish who may read, write, delete or alter each field. With a driver’s license, for example, there might be a “public file” containing standard demographic data, such as name, address, license number, and physical description. The DMV would be able to write and update these fields, but law enforcement and other agencies would only be able to read them. Physicians or paramedics would be able to read, write, and update emergency medical treatment information that could not be accessed by others. A court might record convictions and points assessed against the driver. Law enforcement might have fields reserved for warnings issued to the driver. Though the DMV might be the issuer, it could establish rules concerning these fields that would prevent even the DMV from altering or, in the case of very sensitive information, even reading them, after the DMV initially issues the card. There could also be data fields reserved for cardholders, which

only they could write or update. In summary, smart cards can be made to operate as versatile, well-controlled, interactive data repositories.

The device through which information can be accessed from a Smart Card is commonly referred to as a "reader." However, there are two ways a Smart Card allows access to a reader and that is by what type of card it is: contact or contactless. A contact Smart Card must physically touch the reader as it has a metal contact pad on its surface which must physically touch corresponding contact pads contained in the reader. A contactless Smart Card has no physical contacts, but communicates with a reader by radio frequencies. The range of these contactless cards is one millimeter to several meters depending on its design. The power of these contactless cards can either come from a frequency generated by the reader (passive) or from a battery contained within it (active).

There are several ways Smart Card technology may be beneficial. The first potential benefit is convenience. The Smart Card has the capability to hold the information contained in practically all cards we use today, such as a drivers license, credit card, phone card, toll card, hunting license, calling card, travelers checks, birth certificate record, social security card, etc. Having all of this information stored in one place may be much more convenient for the consumer as well as the information-issuing agency. Security can be one of the Smart Card's greatest benefits. Unlike a magnetic stripe, information stored on a Smart Card can be stored and encrypted in several ways. The Smart Card can have its own built-in security system or key, such as PIN numbers that match the access code, biometric identifiers and digitized signatures. Since the microchip on a Smart Card is embedded in the card, tampering with the card without destroying it is nearly impossible. Many Smart Card applications also eliminate the need to manually enter an access code that could be viewed and misused by an unauthorized person. Privacy of the cardholder is also a benefit. The cardholder has control of who can access the information. For example, a Smart Card could be encrypted by a second key which is known only by a physician or other persons or agencies who need access. So, the first level of security gives the cardholder control over access of the data and the second level of security would allow access to only those persons or agencies authorized to access the information.

Reduction of costs is yet another important potential benefit of Smart Card technology. Though manufacturing costs of these cards can range from \$2 to \$8 (depending on quantity manufactured and type of card), Smart Cards are flexible enough to handle a variety of things. No longer would each jurisdiction agency or vendor need to manufacture and maintain its own card - all cards could be combined into one, thus ending in a partnership and shared costs. In addition, the ability to manage and control expenditures more effectively, fraud reduction, and the elimination of the need to complete redundant, time-consuming forms could contribute to savings.

Telecommunication costs may also be diminished because Smart Cards do not need to use on-line connections to approve and make transactions.

Although Europe has proven to be a leader in the area of Smart Card technology applications, it is anticipated that Smart Card technology applications in North America may grow quickly. This is largely due to a number of recent issues that have encouraged activity. First, the rapid increase in card-related fraud over the past few years has created the need for a high level of security that

Smart Cards can provide. Smart Card technology has also matured significantly and its costs have decreased to the extent that the technology creates savings in well-managed application areas.

The capabilities of Smart Card technology are numerous and its uses can be far-reaching. Several jurisdiction's motor vehicle/licensing agencies are already seriously considering the benefits of this technology. The benefits of this includes not only the obvious security enhancement, but partnerships with other jurisdiction's agencies and programs. The ability to update information contained in the Smart Card's chip and to employ other technologies only adds to its value. However, at this time only one jurisdiction has committed to implementation of a Smart Card that will include Motor Vehicle applications. Most jurisdictions believe there needs to be significantly more investigation and validation of suggested benefits and savings of a Smart Card and what it can bring to the North American Motor Vehicle Application.

## **8. SMART CARDS IN COMMERCIAL VEHICLE OPERATIONS**

On December 1, 1996, The Federal Highway Administration (FHWA) issued a report titled "Smart Cards in Commercial Vehicle Operations." This report was meant to specifically address how smartcards could be applied to commercial operations, but the FHWA discovered that this was not a practical approach and broadened its scope to address both commercial and non-commercial operations. Below are three uses of the smartcard that were determined in this report to be feasible:

### **8.1. Smart Driver's License**

This license would look like an existing drivers license except that it would include a chip capable of digitizing, storing and securing license information in an electronic form. This license would link the cardholder to the card with a biometric identifier, reduce and prevent fraud by carrying the information printed on the card in a secure microchip, make issuing and renewing licenses a much faster process by reusing the card, and allow for electronic certification of automated transactions.

### **8.2. Smart Vehicle Card (SVC)**

The SVC would be able to carry federal, jurisdiction, and local credentials required to operate a truck or bus as well as carry maintenance and fuel usage records. The SVC would facilitate the automation of applications and renewals of commercial vehicle credentials, allow electronic credentials (vehicle-specific and driver-specific) to be sent to roadside inspectors, and assist carriers in the processing of vehicle information.

### **8.3. Smart Card Electronic Toll Collection (ETC)**

The Smart Card ETC would be a smart card with an electronic purse which would allow the cardholder to transfer money to the toll agency, either through a stop-and-pay system

or through a transponder without having to stop. This would eliminate cash toll collection and lower operating costs.

## **9. STANDARDS FOR SMART CARD TECHNOLOGY**

AAMVA and AAMVANet are currently involved in an effort via the American National Standard Institute<sup>1</sup> to develop a standard for Driver Licenses/Identification Cards. The main body of the document will contain general standards information which does not relate to any specific technology such as: card size; data standards on human and machine readable information; security; etc. The document will also include a set of annexes for applicable technologies such as Bar Code, Digital Imaging, Integrated Circuit Cards, Magnetic Stripe, and Optical Memory. The standard on the “smart card” technology will be covered by the Integrated Circuit Card annex.

### **9.1. Driver License Standard Working Group Composition**

ANSI's Accredited Standards Committee, National Committee, for Information Technology Standards (NCITS), is a committee dedicated to creating and maintaining standards for identification cards and related devices - B10. A working group has been formed for driver's license/identification cards (DL/ID) - B10.8. The working group is comprised of industry representation (vendors) and jurisdictional representation. B10.8 has three main offices per compliance with ANSI's organizational requirements. They are a Convenor (Chair) - Kevin Keipper, Polaroid; Secretary - Geoff Slagle, AAMVANet; and Project Editor - Philippe Guiot, AAMVANet. The development has involved broad-based project teams including state driver license agencies, government, equipment and software suppliers, card vendors, and consultants.

---

<sup>1</sup> The American National Standards Institute is a nonprofit, privately funded membership organization that coordinates the development of U.S. voluntary national standards

Currently the following organizations have been participants in the working group:

**Industry**

3M  
AMP Pennsylvania  
Axiohm  
Brush Industries  
CFC International  
DataCard Corporation  
Drexler Technologies  
Empire Plastics  
First Data Corporation  
Intelli-Check  
JCP Enterprises, Inc.  
Naujokas & Associates  
Mag-Tek, Inc.  
Motorola  
NBS Imaging Systems, Inc.  
Polaroid Corporation  
Q & A Consulting  
Rodakis & Associates, Inc.  
Russell Technology Associates, Inc.  
Schlumberger  
Statistica, Inc.  
Symbol  
Transilwrap Co., Inc.  
Verifone/HP

**AAMVA/AAMVAnet**

Mike Anderson, Texas (DL&C Chair)  
Rebecca Bickley, Pennsylvania  
Mike Calvin, AAMVA  
Linda Datzman, Indiana  
Terry Dillinger, Iowa  
Cindy Gerber, South Dakota  
Philippe Guiot, AAMVAnet  
Ray Leard, Maryland  
Pete Poleto, New York  
Joe Sanders, New York  
Karen Schwartz, Wisconsin  
Judy Sibert, Texas  
Geoff Slagle, AAMVAnet

## 9.2. Projected Activity by Time Line

Date	Activity
September 97	1 <sup>st</sup> meeting with ANSI B10, focus: creation of working group for DL/ID
November 97	2 <sup>nd</sup> meeting to organize the working group and create action items for next meeting to include a draft
January 98	3 <sup>rd</sup> meeting, 1 <sup>st</sup> official working group - ANSI B10.8 (NCITS designated), milestone reached with distribution of draft
March 98	Due date for annex contributions
April 98	4 <sup>th</sup> meeting, 2 <sup>nd</sup> working group - redistribution of draft with updates
August 98	5 <sup>th</sup> meeting, 3 <sup>rd</sup> working group - ANSI B10.8
November 98	6 <sup>th</sup> meeting, 4 <sup>th</sup> working group - ANSI B10.8
January 99	7 <sup>th</sup> meeting, 5 <sup>th</sup> working group - ANSI B10.8
April 99	8 <sup>th</sup> meeting, 6 <sup>th</sup> working group - ANSI B10.8
August 99	9 <sup>th</sup> meeting, 7 <sup>th</sup> working group - ANSI B10.8

## 9.3. Development of a Standard API (Application Programming Interface)

The development of a standard API has been discussed in various conference calls with the Smart Card Working Group and several members have expressed their desire to have such a standard developed. The current effort with B10.8 does not include the development of a standard API in its scope, however, it is possible following the publication of the ANSI DL/ID Standard, to develop additional documents called Implementation Guides which will focus on implementation specifications specific to the application of the DL/ID.

These Guides would define the methods to use the cards and the specifications of the various devices needed to implement Driver License's systems. The description would be based on the ANSI standards currently being developed by B10.8 and on other available standards and specifications commonly accepted in the marketplace. The description would define the operational characteristics required of the devices in the card that would be used and define the functions of the processing systems that use such devices. These guides could include an API specification of each device and processing system.

## 10. AAMVA Best Practices for Magnetic Stripe and Bar Codes

In recent years, many AAMVA Jurisdictions have been converting to technology-based DL/ID (driver's license/identification) cards. "Technology-based" refers to the concept that the information contained on the drivers license document is machine-readable. Two machine-readable formats are magnetic stripe and bar code. The MVIS Standing Committee and other

standing committees recognized in 1991 the need to standardize the use of these technologies, to gain the greatest utility for use of the data.

At the 1991 MVIS Workshop, it was agreed that a working group would be established with the task of developing a standard and a format for the use of magnetic stripe technology. The working group consisted of jurisdictional representatives from each of the AAMVA regions in addition to several participants from the IAB (Industry Advisory Board). The working group established a standard published in September 1992.

The working group's goal was to require an AAMVA compliant DL/ID to be readable by the standard credit card readers omnipresent in North America, as well as to establish a common medium that would support both state and local law enforcement. There is a growing need for driver identification information to assist law enforcement in processing traffic citations and other NCIC 2000 compliant reports in a more efficient manner through the use of technology. This will reduce the amount of time offices spend on preparation of reports and allow enforcement to perform their primary job, which is to serve and protect the citizens of their jurisdiction(s). It was then determined that the magnetic stripe with ISO Track #2 encoding (per the current AAMVA Best Practice) would provide one method of technology that would satisfy the driver identification requirement.

Magnetic stripe has a typical data capacity of about 200 bytes. Its primary purpose is for identification, and is normally self-contained with respect to required data to be usable off-line. The best example is the credit card. When read by a cashier, it yields the person's name, account number, expiration date, validity codes, etc., i.e. all the information required to complete the transaction without access to any computer data base. In short, with a magnetic stripe the desired information is stored on the card.

Many DMV program areas are looking at bar codes as potential tools to gain productivity, increase accuracy, and reduce operating costs. Strong interest exists in the registration, titling, and drivers' licensing areas. Bar codes are likely to play a role in redesigned or new systems to deal with the Clean Air Act as well. Bar codes are having a positive role in many areas of motor vehicle and related businesses. A number of standing committees have included the consideration of bar codes in action plans developed as part of their Master Planning processes, which aligns them with AAMVA's strategic direction.

The information systems support arena has recognized the potential for productive use of bar coding technology. In particular, a strong interest developed to maximize the potential to the entire AAMVA community by the development of community-wide guidelines or standards to foster inter-jurisdictional use of bar codes.

The Vehicle Registration and Titling committee (formerly RTVDM), with the assistance of MVIS had started to create a vehicle template which identified all related fields utilized by the jurisdictions. In 1992, the MVIS standing committee formed a Working Group to investigate the systematic use of bar codes in the DMV community. The Working Group included representatives from other standing committees and industry. A preliminary report was developed by the Working Group and presented at the MVIS workshop in the spring of 1993. Subsequent

communication to all Chief Administrators, Standing Committee Chairs, and each jurisdiction's MVIS contact person, included a copy of the preliminary report and a request to review and comment on its content. An entry in the AAMVA Electronic Forum on the AAMVAnet Bulletin Board was created and continues to be used to exchange comments and keep the community informed.

Responses to the request for comments stressed the need for guidelines to address both linear and Hi-Density (two dimensional) bar codes and a desire to have a set of guidelines before the community as soon as possible.

A number of jurisdictions suggested that a staged report would be appropriate, since there was a desire on their part to conform with the community's overall direction as well as a need on their part for a near term solution to intra-jurisdictional issues. Therefore, the Working Group acknowledged that its recommendations did not address all aspects of this issue. Additional recommendations relating to such issues as data structure and encryption will be forthcoming.

At the 1993 MVIS workshop, it was decided that the recommendations to the AAMVA Community should be in the form of a "BEST PRACTICES" report which would be presented to all AAMVA Jurisdictions for both magnetic stripe and bar code technology. Such an approach is characteristic of the process followed by many recommendations which described the process by which the best practices report and any subsequent modifications would be balloted. The policy recommendation was approved by all four (4) regions at their respective meetings and approved at the International Business meeting in August, 1993.

As of this writing - the April 1996 versions of both the Best Practices for Magnetic Stripe and Bar Codes are the most current used. The Best Practice for Magnetic Stripe will completely migrate to the ANSI B10.8 Driver's License/Identification Card Standard (*Please see the "Standards for Smart Card Technology" section of this document*). AAMVA will continue its maintenance of the Best Practice for Bar Codes.

## **11. IAB SMART CARD WHITE PAPER**

# **IAB SMART CARD WHITE PAPER**

**Version 1.1**

This Document was created  
In Conjunction with the  
AAMVA Smart Card Working Group

By the  
IAB Smart Card Committee  
**Monday, August 17, 1998**

## TECHNICAL EDITORS

### Polaroid Corporation - IAB Members

Dino Redmond  
Phone 219-484-8611  
Fax 219-482-2428  
E-Mail [dinor@nbstech.com](mailto:dinor@nbstech.com)

Vic Andelin  
Phone 219-484-8611  
Fax 219-482-2428  
E-Mail [vica@nbstech.com](mailto:vica@nbstech.com)

## CONTRIBUTORS

### 3GI

Steve Zullo  
Phone 703-922-3448  
Fax 703-922-4603  
E-Mail [szullo@3gi.com](mailto:szullo@3gi.com)

### AAMVA Smart Card Working Group

Terry Dillinger - Chairman  
Phone 515-237-3153  
Fax 515-237-3071  
E-Mail [ussia8g8@ibmmail.com](mailto:ussia8g8@ibmmail.com)

## 1. GENERAL

Jurisdiction-issued smart card Driver Licenses could hold Driver information including Driver Data, Drivers Image and Signature and/or Biometrics Identification. Other government agencies are already issuing smart cards in pilot and system wide programs for EBT, immigration, military ID, electronic certification, agency ID's, and medical program eligibility.

## 2. OVERVIEW OF SMART CARD TECHNOLOGY

Smart cards are credit card-sized plastic cards with an imbedded microprocessor chip. Smart cards contain built-in logic capability and currently hold typically 2K to 8K of memory. Right now, smart cards are being used both commercially and by some governments worldwide for a wide range of applications.

Smart cards enable functionality, are standardized, and are cost effective. Examples of smart card functionality include:

- **Portability:** Smart cards are portable data carriers.
- **Multiple Applications:** Smart cards are capable of providing multiple functions. For example, a single smart card can possibly meet multiple needs of an individual by serving as a bankcard, health card, travel card, and identification card.
- **Storage Capacity:** Commercially available smart cards can store typically 2K to 8K of data in comparison to Magnetic Stripes (204 bytes) and 2D Bar Codes (1K).
- **Durability:** This is a critical issue to be looked at since most smart card programs are for shorter periods than the typical 5 to 7 year life expected of a Driver License. Smart cards in real life do not go through the typical wear and tear that a Driver License or ID card does on a daily basis and the tests are less stringent than those for a typical 2-3 year life credit card. Also, a high risk factor would be failed durability and the high replacement cost for the smart card. Another area of concern would be that no empirical study on Driver Licenses has been done and there are a number of unknowns and risks.
- **Security:** Because smart cards contain resident processing capability, they are able to maintain highly secure encryption-based security features which make unauthorized electronic and physical access nearly impossible.
- **Universality and Interoperability:** Smart cards can enable communication between disparate databases that are not connected on-line. Smart cards can serve as a bridge to integrate systems by transferring data from one data repository to another. Most smart card information is compatible with ASCII text applications, and ISO has developed some initial smart card standards.

### 3. APPLICATION AND MIGRATION

Once a Jurisdiction has fully converted its drivers license database, this database can in the future serve as the foundation for the issuance of *smart cards* (cards containing an electronic chip) or *hybrid cards* (cards combining electronic chip with magnetic stripe and/or Bar Code functionality) to deliver a variety of services.

Potential *smart* or *hybrid* card applications include:

**Identity.** Applications where the verification of a citizen's identity is important.

**Eligibility.** Applications which verify a client's eligibility for participation in a service or program.

**Medical Information.** Applications requiring access to, and/or tracking of, client medical information.

**Attendance.** Applications in which proof of attendance is mandatory for either third-party reimbursement or individual record maintenance.

**License/Credential/Permit.** Applications where presentation of documentation as proof of completion of training and/or fee payment is required.

**Value Transfer.** Applications involving a transfer of monetary value directly from the Jurisdiction to a citizen.

**Verification of Authorized Services.** Applications where a list of authorized medical products or services could be stored on the card so that a medical provider can determine what the covered services are for the recipient under the program.

### 4. PRACTICAL APPLICATIONS

The smart card can provide opportunities for a Jurisdiction to possibly recover the cost of issuing the license while at the same time improving their customer service and the role of the license.

#### 4.1. Electronic License Renewal.

Drivers can return to the licensing agency, complete any tests—driving skills, knowledge, vision—which might be required and update outdated license information.

Unless the Jurisdiction has a compelling reason to change the photo and data on the face of the license, it can record updated driver data in the microchip of the original license.

The Jurisdiction will need to determine what circumstances would compel it to issue a new smart card. A change in license type from, say, a normal license to CDL and Damage to the Card would require a new smart card, whereas a new address or facial changes arising from aging might not.

## **4.2. Electronic Vehicle Registration**

In addition to driver information, the computer chip on the card can also store information for vehicles. Renewal of registration can then be done more easily.

## **4.3. Use of Smart Card Chip by Multiple Agencies**

Jurisdiction-issued driver's licenses are widely accepted as proof of identity for public as well as private purposes. Clerks typically copy data from the license onto a customer's check; some even photocopy the license itself. If instead, Jurisdictions were to license software to private businesses, they could easily copy the customer's address and license number into their systems ( Might be a privacy issue here) when the customer presents a driver's license as proof of identity. Such businesses would not have the software and authorization necessary to write or alter data in the card. The hardware and software to read smart cards is relatively inexpensive and available today, but has not penetrated into the retail community yet. The computers already in use by these businesses could possibly be updated to run the software and also operate an added smart card reader.

# **5. CONTACT CARDS (Chip on the surface of the card)**

## **Card Type - ISO Compliance**

### **5.1. Physical Characteristics**

Various types of smart cards can be distributed throughout the card holder population. The primary restriction for compatibility is all the cards used must conform to ISO standard 7816-1/2/3. The 7816-1 standard defines the dimensions of the card, which is the same as those of a standard credit card. The 7816-2 standard defines the dimensions and locations of the contacts on the card. Though the computer chip is embedded in the card, the contacts used to interface with the chip are located on the card surface.

### **5.2. Electrical Characteristics**

The interface with the chip is partitioned into eight separate contacts. Two of the contacts currently have no function, and are reserved for future use. Of the remaining six, three are used to supply a ground and 5.0 volts of DC electricity to power the smart card chip. Another contact is used as a reset switch for the chip. Virtually all modern computers and smart cards are no exception, and designed to operate at a certain frequency (that is, a "basic" operation is defined to occur so many times per second). The ISO standard for smart cards defines this frequency to be 3.579 MHz, which means that the "state" of the computer can change as quickly as 3,570,000 times per second. This frequency is defined by a timed electrical pulse, which is provided to the card chip by one of the remaining contacts. The final contact is used as a data line, that is, a channel through which data can be stored to or retrieved from the smart card chip. The use of each contact is defined by the 7816-3 standard. More generally, the -3 standard defines the electrical and transmission characteristics of the smart card.

## 6. PHYSICAL CARD FEATURES

The basic criteria for the selection of a smart card are that it must be ISO 7816-1/2/3 compliant, and it must implement the T=0 asynchronous communications protocol as a part of the ISO 7816-3 standard. Though 7816-1 defines the dimensions of the plastic packaging for the smart card chip, it does not place any restrictions on the type of plastic material used for composition of the card. There are several plastics, which are used for smart cards. The most popular plastic is PVC, or polyvinylchloride. PVC is strong, durable, and easy to mold. Another similar type of plastic is called ABS, or acrylonitrile-butadiene styrene. The principle advantage of ABS is it is much easier to recycle than PVC. Unfortunately, standard dye-sublimation printing employed by current card badging stations does not produce a clear image on ABS. ABS is a good choice for smart cards not requiring detailed personalization and that can be printed at the factory. Factory personalization is awkward, at best, especially if a picture of the cardholder is to be printed on the face of the card. For this reason, PVC is recommended at this time. PVC can be recycled also, but since it must be raised to a higher temperature, and it produces more toxic fumes, the cost of recycling is greater. There are some hybrid cards, composed mostly of ABS, but sporting a thin top coating of PVC for clear dye-sublimation printing.

## 7. ELECTRONIC FEATURES

The "smarts" of a smart card reside in the tiny integrated circuit (IC) chip embedded within the plastic of the card beneath the gold-plated contacts generally considered to identify the front of the card. The embedded IC contains a microprocessor as well as an integrated store of persistent memory. Most of the major chip manufacturers currently produce IC's suitable for embedding in smart cards.

The IC embedded in the smart card integrates what is generally considered to be two unique parts of a computer into a single, seamless package. First, there is the microprocessor discussed above. This is regarded as the "brain" of the computer, since it performs all the calculations (along, perhaps, with a coprocessor). Second, there is the memory storage of the card, which "remembers" even when power is not being supplied to the card, that is, the memory is persistent. Memory capacities range anywhere from around 128 bytes up to around 16 kilobytes. Though 2K cards are currently the most popular in circulation, 8K cards are quickly becoming widespread. Very few manufacturers offer anything above 8K, and, though claims have been made of 32K cards, they are as yet unsubstantiated by this study. The lifetime of most smart card memories is rated at a minimum of 10,000 read/write cycles. After this, the persistence of the memory may begin to degrade.

The clock speed defined by ISO 7816-3 of 3.579 MHz is noticeably slower than speeds of common desktop computers (for example, 200 MHz). The reason for this is higher speeds result in greater heat, and the plastics used to package the chips cannot dissipate heat fast enough to permit high clock speeds. A typical maximum clock rate for a smart card IC is 5 MHz, but the slower ISO standard of 3.579 MHz is recommended for compatibility.

Many smart cards currently being produced include two separate ICs, one for standard operations and persistent memory, and another which is dedicated to cryptographic functions. Most cards today have a built-in cryptographic module, which means they can encrypt and decrypt data for various reasons.

## **8. CONTACTLESS CARDS (Chip or Thin Film beneath the surface of the card)**

### **8.1. Radio Frequency (RF) Technology**

According to ISO 7816-3, various contacts are defined to supply power to the smart card IC, and to permit communications of various sorts with it. Another approach for supplying power and providing a communications medium is to use airwaves. This sort of technology is emerging now in a package very similar to that defined by ISO 7816-1/2. The main difference as seen from the outside is that there are no metallic contacts on the surface of the card. Instead, these "contactless" cards employ antennae embedded within the card plastic to support communications with the outside world. In some cases, the antenna is also used to supply power to the embedded IC. In other cases, there is an internal power supply in the form of a tiny, embedded battery. Though this technology offers significant advantages for certain applications, it is just now in the beginning stages of becoming a standard.

## **9. CARD OPERATING SYSTEMS**

The minimum requirements for a smart card are defined by ISO standard 7816-1/2/3. To actually make the card useful, however, some additional capability must be supplied with the card. There is memory, but how does one access it? There are communication lines, but how are they utilized? In the traditional parlance of computer science, this is the job of an operating system (OS).

Modern computers have sophisticated operating systems, which provide a user-friendly interface between man and machine. The essential purpose of an OS, however, is to manage the various resources of the computer. With smart cards, there is no need for a fancy user interface. There are, however, resources to be managed, albeit simple in contrast with typical desktop PC's. The two main resources are the memory and the communications (or input/output) channel. To help manage these and other resources, various smart card manufacturers each offer a different operating system.

Typically, operating systems are highly tailored for efficiency and maximum utilization of the capabilities of a specific microprocessor. Thus, there are few standards for smart card operating systems (COS's), and almost every card has it's own flavor. This notwithstanding, there are several features which are common to many cards.

### **9.1. Answer to Reset**

According to the ISO standard, all smart cards must be designed to perform a standard initialization sequence known as the answer to reset (ATR). When power is provided to the smart card, the operating system automatically executes. As part of the OS boot sequence, an ATR message is sent to the host system providing power. This message is sent across the data line and, in accordance with the ISO standard, is formatted in a certain way, sent using a standard communications protocol, and transmitted at the standard rate of 9600 baud. The ATR message serves to identify the type of the smart card (manufacturer and size) to the host system. It also encodes other information about the processing and communications capabilities of the card. Based on this information, the host and the card can negotiate a different protocol and speed for subsequent communications. Some cards can jump as high as 115,000 baud after the ATR sequence, but most cards still operate at the default 9600-baud.

**9.2. Memory/File Management.** To begin, all card operating systems provide some form of memory management, that is, some way to organize the "real estate" of memory on the card. The elementary OS commands for performing memory management permit memory to be organized similarly to the way the file system of traditional operating systems permit secondary storage to be organized.

**9.3. Memory Protection (Card Security)** One of the greatest advantages offered by smart card technology, secured access, is provided to portable data. The primary facility for securing the privacy of data stored in the smart card memory is the password system included as an extension of memory management. There is generally a way to specify up to a certain small number of "passwords" (for example, eight passwords are typical). Each password is composed of a certain small string of bytes (for example, 8 bytes, where each byte can be one of 256 different values). When a file or directory is created one or more passwords can be associated with an operation to be performed on that file or directory. For example, a file can be protected from writing by associating password number 3 with the write operation on that specific file. The basic operations are change for directories; read, write and update for files; and create and destroy for both. Not all COS's permit all operations to be protected by passwords, but several variations are generally supported.

**9.4. Passwords and Password Management** When a smart card comes from the factory, it is initialized with a mask. In addition, there is generally a master or issuer's password, which is already set in the password area. This password is required to reset the contents of the card and to perform administrative operations such as setting the other passwords and establishing a directory structure with protected files. Most of the other passwords are called application passwords because each one can be used to secure a separate application. There is another password with special uses called the PIN, or personal identification number. Most systems permit the PIN as well as another password to be associated with various operations. Thus, permission to perform selected operations on various parts of memory can be limited to persons knowing the card's PIN which, presumably, should only be known by the rightful card owner.

Once a card has been formatted, a typical use of the card might look something like this:

1. The card is powered up.
2. The card responds to the host with an answer to reset message.
3. The host and the card negotiate a protocol to use for subsequent communications.  
(API)
4. The directory containing the relevant file is selected (change directory command).
5. A read password is presented to the operating system.
6. The command is issued to read the record of the file containing the desired data.
7. The card is powered down.

This is only an example, making many assumptions that need not hold in an actual system, but it does provide an example of what a typical sequence looks like for a simple read value operation.

## 9.5. Electronic Purse

In addition to the standard commands for memory and password management, many COS's now support specialized commands, particularly for electronic purse and cryptographic functions. Though the standard "file system" of the card can be used to implement this functionality, it is much safer to have the operating system perform these operations transparently in special files for the purse. In other words, the COS automatically handles many of the details generally associated with financial-type transactions. The basic operations are debiting and crediting a stored cash value. If, for some reason, the operation cannot be completed (say power is cut to the card) the COS guarantees to maintain the integrity of the card contents. For example, a credit or debit operation may automatically be "rolled back" unless it is finished completely. Thus, with special purse support, credit and debit are offered not only as operations, but also as "atomic" operations. That is, they cannot be decomposed any further or halfway completed; they are either performed 100% or not performed at all. Besides automatic roll backs, other advantages of special purse support include user-induced rollbacks and automatic transaction logs.

## 9.6. Cryptography

Another class of special commands provided by most smart cards today is that associated with cryptography. With a built-in cryptomodule, most smart cards can encrypt and decrypt data. One common use for cryptography on the smart card is to implement another security feature known as secured messaging. Secured messaging utilizes the on-board cryptographic engine of a smart card to allow it to communicate with a host in a way that precludes eavesdropping by a third party. Using secured messaging, data is encrypted, sent to or from the smart card, and decrypted at the other end. Before this happens, though, a secured channel must be set up. The first step is to insure that each party is authorized to trade information. This can be done in several ways. Often the side initiating the procedure will generate a random number and ask the other side to encrypt it. If the returned number can be decrypted to its original value, then there is high confidence the other party has the key and is therefore authorized. Other security features to thwart a would-be eavesdropper can be built into secured messaging, but this is the basic method when transmitting secured data over unsecured communications channels.

The most commonly implemented cryptographic algorithm in smart cards today is DES. Many cards are also starting to support triple-DES. Both of these are considered private or symmetrical systems. In contrast to the private schemes, there are also asymmetric public-private algorithms. RSA, for example, is quickly becoming very popular among smart card cryptomodules. Some cards support both DES and RSA. Unfortunately, neither RSA nor triple-DES is currently approved by NSA and NIST. Thus any cards recommended for use by the federal government will implement a DES cryptomodule.

### **9.7. Multi-Functional Data Carrier**

Between memory (file) management, password management, purse functions, and cryptographic calculations, the main features of smart cards have been outlined. It is worth noting, however, as an emergent property of these features, smart cards are very well suited to be used as Multi-functional data carriers. The relatively large memory capacities they support are, of course, needed to support many different functions or applications at once. Not only is there plenty of room for various applications to store their data, but the mechanism for establishing passwords and associating them with various operations on selected regions of memory provides a way for multiple applications to share the same space, while at the same time, protecting themselves from one another. In cases where the same data should naturally be shared and kept consistent across multiple applications, only a single copy need be kept to eliminate redundancy and the possibility for inconsistency. Smart cards offer relatively large, portable memory stores to which access can be controlled, protecting the data used by various functional domains from each other while permitting sharing of data elements that are naturally shared. For this reason smart cards are uniquely suited as Multi-application data carriers.

## **10. CARD PERSONALIZATION / INTIALIZATION**

The basic IC chip embedded in a smart card contains all the raw power needed to perform a host of computations. Before the smart card can effectively be used, however, it must pass through three basic stages of preparation. The first process, as discussed previously, is initialization of the chip, whereby the OS or mask is burned into the IC as an “extension” of the raw capabilities of the microprocessor/memory combination. The second stage, also discussed previously, is generally referred to as formatting the card, whereby files and access permissions are established. The final stage of preparation is also sometimes referred to as initialization, but more commonly is referred to as personalization.

Personalizing the card entails any preparation for the card, which is unique for the individual cardholder. Formatting can be performed as part of final personalization, or cards are pre-formatted in batch mode to speed up the issuance process. At any rate, once files have been established on the card chip, certain basic data, such as name, social security number, date of birth, etc. are written to the card. Also, there must be some way to permit the cardholder to define his or her PIN. This information may also be stored on the magnetic stripe of the card or printed on a bar code. Other types of printing are also performed such as printing a picture of the cardholder's face on the card, or printing a digitized image of the cardholder's signature.

## 11. COMMITTEE CONCLUSIONS

*While smart cards give the user more options and flexibility than they have had before they are not without their own set of problems and risks such as durability, a solid business case, a robust and all inclusive API and also the problem of a non existent infrastructure in North America.*

*One of the risks is that each manufacturer of chip uses it own proprietary operating system which make an API (Application Programming Interface) mandatory as different chips might be used by different jurisdictions. This could cause major interoperability problems unless an AAMVA API was developed to handle the inherent differences in each manufacturer's chips.*

*Another is that there are durability issues to be worked out, as current Contact smart cards might not last the required 5 to 7 years of life (Minimum) currently mandated by most Jurisdictions.*

*The committee would also recommend a continued study of Smart Cards by the Smart Card Working Group as this technology continues to change rapidly. This is especially true in the Contactless varieties of the cards. It is the committees educated opinion that the answer to most of the durability questions may be addressed and answered by Contactless Cards and the Smart Card community.*

*Also the use of Smart Cards needs to be addressed by the AAMVA community on a solid business case basis that would include multiple agencies within the jurisdictions as well as non government partners to offset the higher cost of using this technology.*

## 12. APPENDIX A - GLOSSARY OF ACRONYMS

ABS	acrylonitrile-butadiene styrene
ACD	Access Control Database
ACT-E	Access Control Terminals
API	Application Program Interface – So that multiple operating systems (Chip Cards) can be used by a single user application
ATM	Automated Teller Machine
CPU	Central Processing Unit
DBA	Data Base Administrator
DBMS	Data Base Management System
DES	Data Encryption Standard
DSS	Digital Signature Standard
EPROM	Electrically Programmable Read Only Memory
IC	Integrated Circuit
NIST	National Institute for Standards Technology
NIST	National Institute of Standards Technology
NSA	National Security Agency
PIN	Personal Identification Number
PPU	Preprocessing Unit
PVC	polyvinylchloride
ROM	Read Only Memory
RTU	Remote Terminal Unit
SAM	Security Access Module
STI	Standard Terminal Interface
TIU	Terminal Interface Units
TTL	Transistor-to-Transistor Logic

## **12. SMART CARD LEGAL ISSUES: A PRELIMINARY REVIEW (Draft)**

# DRAFT

## SMART CARD LEGAL ISSUES A Preliminary Review

### **PRIVACY**

Although the data on the card could arguably be considered to be a “motor vehicle record” and some of the data on the card itself would be “personal information” as those terms are defined by the Driver Privacy Protection Act (PL 103-322; 18 U. S. C Sec. 2721 et seq.), the card, and thus release of the data, would be under the control of the driver, and thus would not implicate the DPPA. Because the card would be held by the driver and not the motor vehicle agency, it would not be considered a public record under the law of most jurisdictions. Thus, a third party would not have the right to demand access to the data on the card from the motor vehicle agency. Therefore, the agency could lawfully encrypt some or all of the data to prevent its being accessed by third parties. Access to the card itself, including any unencrypted data, would be a matter to be negotiated between the driver and the merchant or other person requesting access.

### **OWNERSHIP OF DATA**

It has been suggested that the agency may wish to charge a fee for access to the data. We recommend that this be authorized by statute. See Model Legislation. Even in jurisdictions where agencies may have some kind of inherent authority to do this, such legislation would be useful in clarifying issues such as the penalty for unauthorized access.

### **RELIGIOUS FREEDOM ISSUES**

Some religious groups have serious objections to being required to carry a smart card because they believe it to be the “mark of the beast” described by the Book of Revelation. (Rev. 14: 16, 17) While this remains a political problem, under a recent decision of the United States Supreme Court, City of Boerne, Texas v. Flores, 65 L.W. 4612 (1997), a requirement that drivers possess a smart cards driver license probably would not violate the First Amendment rights of those who have religious scruples against having them. In Flores, the Supreme Court held that:

“The constitution’s Free Exercise Clause does not relieve an individual of the obligation to comply with a valid and neutral law of general application on the ground that the law proscribes (or prescribes) conduct that his religion prescribes (or proscribes).”

Jurisdiction Constitutions and statutes may provide greater protection than the U. S. Constitution as interpreted by the Supreme Court, so the agency’s legal advisor should be consulted prior to implementing a smart card program.

**FEDERAL ODOMETER DISCLOSURE REQUIREMENTS**

Federal law (49 U. S. C. 32705) and administrative rule (49 CFR Part 580) require that motor vehicle titles contain odometer disclosure forms and be set forth by secure printing or other secure process. Issuance of a smart card motor vehicle title would either require an amendment to the Federal law and rules or approval of an alternative disclosure requirement under 49 CFR s.580.11.

**FEDERAL BANKING REGULATIONS**

A preliminary review of Federal banking regulations has unearthed a regulation which may mean that an agency which issues a smart card driver license, which also may be used as a debit card, may be considered a “provider of electronic fund transfer service” (12 CFR s. 205.14). This would require the agency to various notice and reporting requirements, and may make the agency liable to replace at least part of the value stored on the card if it is lost. This issue will be studied further and, if necessary, amendments to Federal regulations and statutes will be recommended.

### **13. SMART CARD CUSTOMER SERVICE ISSUES: A PRELIMINARY REVIEW (Draft)**

# DRAFT

## SMARTCARD CUSTOMER SERVICE ISSUES A Preliminary Review

### CUSTOMER BENEFITS

From the standpoint of the average customer what would make him or her interested in a chip card to carry in their pocket? The customer must perceive that a need they have is fulfilled, that they can do something with the product they couldn't do before, that they can do something in a new and easier or better way, or that the item is so commonplace that it is accepted and used by others, and perhaps themselves, for other things. At this time, the idea of using a chip-based card for single or multiple applications, whether for government or commercial services, would be foreign to most of the citizens in the United States and Canada.

Most people have credit cards that contain magnetic stripes and bar codes which are on many items we see daily, so we are conditioned to using these machine readable devices. The general population is not educated to the potential benefits of a Smart Card, what information it will contain, where and for what purposes it will be used, who will have access to the information contained on it, and what will this thing do to make life better for them.

Some applications that look like they will use Smart Cards in the near future are internet commerce, telephonic communications and E-cash (especially the market for under \$10 purchases). As chip cards become more visible, so will customer acceptance.

### INFRASTRUCTURE

It is said that in the United States and Canada, where the telecommunications infrastructure is already in-place and relatively inexpensive to use, established credit and debit card companies will continue to make the most of existing magnetic stripe technology before moving to chip-based solutions. Although the technology for delivering the services via chip is fairly well-developed, the infrastructure deployment is still in its infancy. Issues that will affect the customers of early roll-out Smart Card applications will include:

- Availability (number) of terminals in which to use their cards
- The type(s) of locations where they will be available (hours of service, accessibility)
- Type(s) of transactions allowed
- Interoperability with other programs:
  - With other government applications
  - Between governments (e.g., will each DMV adopt the same standards)
  - With other private sector applications
  - Technological commonality

## **SECURITY/IDENTIFICATION**

One of the tasks that Smart Cards can perform better than other machine readable documents is authentication, or access to the card's memory information. While PINs (personal identification numbers) are a form of authentication, Smart Cards allow for a variety of techniques which can provide greater security to the data on the card as well as prevent the use by anyone other than the authorized card owner in case of lost or stolen documents. For example, most scenarios portraying the future of Smart Cards will include a biometrics identification technique as part of the card's on-board access system. The power of having such a device on the card, before other data is read, means you don't have to return to the host system to authenticate the user, there is no need to enter a PIN (the biometric fingerprint, hand geometry or voice print identifies the user), the card itself does the direct identification comparison and third party fraud is reduced because only the user is authenticated.

The driver license and non-driver cards we issue in motor vehicle agencies are the de facto identification cards used by most of our citizens and accepted by most others (business and government). Providing an on-board level of security would be very valuable to protect against fraud, resist tampering and counterfeiting, and to increase the reliability of (and reliance on) the documents we issue to identify individuals. The cards could be used in financial dealings, air travel ID, immigration, voter registration, secure access to buildings and in combination with other licenses, such as firearms.

This ability to encrypt-decrypt information would allow flexible security levels within the card. Information could be at general levels for most businesses (name, address) while deeper levels could be protected from all but a few users (medical information, social security/social insurance number). The card could operate in isolated environments, making secure ID (knowing that the person using the card is the one authorized to do so) a more widespread and useful tool for both card holders and those they deal with.

## **PUBLIC ACCEPTANCE**

Today, no customers are "beating down the door" to demand Smart Cards to "fix their problems." Quite the contrary, in the one motor vehicle application already announced, the jurisdiction of Utah received a less than enthusiastic reception from segments of their population. Both the extreme right and left argued that personal privacy would be lost, and that religious freedom would be invaded (some calling the chip "the mark of the devil"). There is certainly a lesson to be learned about public relations and customer education in the scenario. Technology is often misunderstood. People fear what they don't understand and are unfamiliar with. In order to overcome the fear of Big Brother or Satan being able to read your life history on a chip or manipulate your life, we need to learn a lesson and actively promote public education to gain understanding and acceptance of how the Smart Card will be used. Some of the issues include:

- Making the public aware of the chip cards in other applications (worldwide)
- Explaining the ease of use

- Explaining what information will be included and how and by whom it could be accessed.
- Training the public in the machine use of the card
- Allaying the fear of privacy concerns (mistrust of government, in particular)
- Explaining the convenience and accuracy of the card, its flexibility and ability to do more with one card
- Explaining the ability to update information on the card without returning to a single source (such as the motor vehicle office)

What we need to remember is that most acceptance will come with familiarity of the product. As more applications become “visible” to the public, some preconceived barriers will be broken down and less public training and education will be necessary. Being the first to introduce something new is more difficult. Since the public will ultimately bear all or part of the cost of any government application, we must also be made to gain not only public, but also political support. It would also be a very helpful step if the customer were to be able to easily read the information on the chip him or herself, check it for correctness and be able to fairly easily correct mistaken information (some sort of ombudsman function). Not knowing what “exactly” is electronically transferred in and out of the chip’s stored memory can be a frightening loss of control to many people.

### **CARD REPLACEMENT**

Customers will “do things” to their cards and a plan must be developed to address the following issues:

- What is the card’s durability? Will it hold up under daily carrying and environmental uses?
- What happens when a card is lost/stolen or a customer needs a duplicate?
  - Who pays for the card replacement?
  - Whose responsibility is it to notify various businesses or government agencies that have information stored on the card?
  - Who “owns” the card?
  - Who “rebuilds” the information, in what time frame, if the customer has been using it in isolated environments?

### **MULTIPLE-USE APPLICATIONS**

Much has been said about the potential advantages of “multiple-use” applications that the memory capacity of a chip card allows the user. But, before we charge off in many directions looking for partners, there are some general issues we must consider, including:

- Compatibility of various users
  - Will the customer perceive any value added if the applications on the card don’t seem to make sense?

- Do we put “anything and everything” on a single card or are there limits to our partnerships or space sharing?
- Who owns the space/data?
  - Who decides what to store and where to store it?
  - How will personal data be entered and formatted on the card?
  - Who decides data field access and how (what security levels are available)?
- Who owns the card?
  - Who pays for it?
  - Who issues the card?
  - Who decides whether a “new partner” will be allowed space?
- Card durability - how often must a card be replaced?
- Rebuilding information
  - Who will collect all of the data that must be replaced if a card is lost/stolen or if a duplicate is needed?
  - Who will pay for the replacement card?
  - Where are the cards “reloaded?”

The reduction in the number of cards a person must carry may be over hyped. As was the case in Utah, some of the public may fear consolidation for reasons of personal freedom or privacy and want individual cards for very specific purposes. One card may not be a desirable product to many consumers.

### **GOVERNMENT MULTIPLE-USE**

There are some specific constraints on government use of data. It is also imagined that there will come a time when several government applications are combined on one card, and perhaps several financial applications on another separate card (although the Utah example would combine both). The following issues are some of the things that must be considered in government combinations:

- Delivery cycles are different (over four to five years for most motor vehicle agencies)
- Different needs of different agencies
- Different customers/clients
- Different infrastructures to build/rebuild
- Availability of resources is cyclical
- Political support necessary
- Turfism on ownership
- Convenience to the public
- Savings in tax dollars by avoiding duplication of systems
- Saves multiple data collection and card issuance (many agencies collect the same information from the customer)
- Centralizes data communications among agencies
- Driver license and non-driver card have become the de facto identification card (motor vehicle agencies have a role, if not the lead, in any multiple government application)

### **EMPLOYEES**

One of the most valuable customer service resources we have is our employees. Each employee must be well versed in the use of any new card system. Some issues are:

- Employee training
- Employee education
- Troubleshooting for customers
- Problem solving for customers

## **14. SMART CARD MODEL LEGISLATION**

**SMART CARD MODEL LEGISLATION**

Section \_\_\_\_\_.-

- (1) The driver license may be made in a smart card format that may contain electronic media, including computer chips and bar coding in order to facilitate the storage and retrieval of information useful to the Department, law enforcement, or the licensee.
- (2) Except for information required by section \_\_\_\_\_ to be shown on the driver license, any information on a smart card used for a driver license under this section shall:
  - (a) be included or deleted only at the option of the licensee;
  - (b) be available for review by the licensee; and
  - (c) be stored and retrieved in a secure manner to allow access only by the department, by law enforcement officers, and by such persons as the department may authorize].
- (3) The department shall ensure that adequate controls are in place for the smart card in order to:
  - (a) minimize errors, security breaches, or other failures in the information, its storage, and its retrieval;
  - (b) provide for timely issuance, cancellation, and replacement of a smart card used for a driver license under this section; and
  - (c) protect the privacy of each licensee.
- (4) The department is authorized to license software to merchants to allow them to retrieve the data on smart card format driver licenses for purposes of identification only. The department may set and collect fees for such software license, [which fees shall be disposed of in the same manner as is provided by law for driver license application fees].
- (5) In accordance with the applicable laws regarding agency procurement and contracting, the department may enter into contracts to provide any or all of the goods and services related to a smart card format driver license under this section.
- (6) A person who stores or retrieves information on a smart card format driver license in violation of this section is guilty of a class \_\_\_\_\_ misdemeanor.
- (7) The department may promulgate administrative rules to implement this section.

## **15. SMART CARD SURVEY**



**To:** Driver License Administrator

**From:** Terry Dillinger, Director,  
Iowa Office of Driver Services  
Chair, AAMVA Smart Card Working group

**Date:** November 18, 1997

**Subject:** Smart Card Usage

Earlier this year, AAMVA formed a cross-program Working group to study Smart Card technology and to determine its viability for use in Motor Vehicle Administration.

A Smart Card is a credit card size card (the size of a driver license) that has a “chip” embedded in the card that contains information on the holder of the card. This technology is similar to the magnetic stripe or 2D bar coding technologies in that it allows for other authorized users of this information to be able to electronically access and read this information. The primary difference between Smart Card technology and the magnetic stripe and 2D bar coding technologies is that the information on a Smart Card chip can be updated by authorized personnel.

Several jurisdictions have initiated studies into the use of Smart Cards for Motor Vehicle Administration purposes only or are looking at the use of Smart Cards combining Motor Vehicle Administration purposes with other jurisdiction-wide identification or service-provision purposes. For example, some jurisdictions are investigating the use of the driver license as the primary jurisdictional identification card as well as the means for electronic benefits transfer for social service programs. These cross-agency initiatives offer many potential opportunities for the realization of economies of scale in terms of cost for providing identification and services. However, on the other hand, these same initiatives offer many challenges as well.

The AAMVA Smart Card Working group is preparing a position paper for review by the AAMVA community on the use of Smart Cards. In order to gather more information from the jurisdictions regarding their potential use of Smart Cards, this Working group has developed the attached short survey.

Please take a few minutes of your time to complete the survey and return it to Sonja Freeman at AAMVAnet. The address and fax number may be found on the attached survey. Thank you in advance for your time in completing and returning this survey by December 5, 1997. Your responses will go a long way in providing direction for the AAMVA Smart Card Working group.

cc: Smart Card Working group Members



**To:** Sonja Freeman  
**Fax:** (703) 522-1553

**Phone:** (703) 908-5842

**From:** \_\_\_\_\_

**Phone:** \_\_\_\_\_

**Jurisdiction:** \_\_\_\_\_

**Please fax back all 5 pages.**

**Thank you in advance for your support in completing and returning this survey. Survey return request date: December 5, 1997.**

\*\*\*\*\*

**AAMVA Smart Card Survey**

**1. Has your jurisdiction considered the use of Smart Cards within the motor vehicle environment?**

If so, in which business areas (circle all that apply)?

Drivers' Licenses

Registrations

Titles

Motor Carrier

Inspections

Enforcement

Other (Please specify) \_\_\_\_\_

Other (Please specify) \_\_\_\_\_

Other (Please specify) \_\_\_\_\_

If not, please proceed to Question 5.

2. **Please elaborate on your jurisdiction's plans/considerations for Smart Cards within the motor vehicle environment.**
3. **What benefits does your jurisdiction anticipate as a result of these initiatives?**
4. **What barriers do you anticipate which may hinder the success of your jurisdiction's plans in this area?**
5. **If your jurisdiction has considered and rejected the use of Smart Cards for Motor Vehicle Administration purposes, please explain the reason(s) the use of the Smart Cards was rejected.**
6. **What technologies do you currently employ within your jurisdiction (circle all that apply)?**

*Driver Licenses:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Registrations:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Titles:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Motor Carrier:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Inspections:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Enforcement:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Others (please specify) \_\_\_\_\_*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Others (please specify) \_\_\_\_\_*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Others (please specify) \_\_\_\_\_*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

7. **What technologies do you plan to implement/utilize within the next 5 years?**

*Driver Licenses:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Registrations:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Titles:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Motor Carrier:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Inspections:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Enforcement:*

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Others (please specify)* \_\_\_\_\_

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Others (please specify)* \_\_\_\_\_

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

*Others (please specify)* \_\_\_\_\_

Mag Stripe	1-D BarCode	2-D BarCode	Smart Card	Other
------------	-------------	-------------	------------	-------

- 8. Does your jurisdiction currently have plans to utilize the driver license as the primary identification card through which other jurisdiction services will be accessed?**

Yes

No

If not, please proceed to Question 14

- 9. Please elaborate on the potential uses for the driver license within your jurisdiction.**
- 10. Which jurisdictional agencies are included in your plans for the expanded use of the driver license? Please list contact persons within your agency and those other agencies that are participating in these efforts.**
- 11. What benefits does your jurisdiction anticipate as a result of these initiatives?**

**12. What barriers do you anticipate that may hinder the success of your jurisdiction's plans in this arena?**

**13. Does your jurisdiction have any published studies regarding the plans for these cross-agency initiatives?**

Yes

No

If yes, is your jurisdiction in a position to share those studies with the AAMVA Smart Card Working group?

Yes

No

**14. If your jurisdiction has considered and rejected the use of the driver's license for cross-agency purposes, please note the reason(s) the expanded use of the driver's license was rejected.**

**THANK YOU VERY MUCH FOR YOUR TIME. PLEASE FAX BACK BY  
*DECEMBER 5, 1997.***

## 16. SMART CARD SURVEY RESULTS

### 1. Has your jurisdiction considered the use of Smart Cards within the motor vehicle environment? If so, in which business areas?

35 jurisdictions have responded to this survey.

- 25 said “no”  
(AR, HI, ID, IL, IN, IA, KS, LA, ME, MA, MI, MN, MO, MT, NE, NV, NY, ND, PA, SD, TN, TX, VT, WV, WI, WY).
- 9 said “yes”
  - DE considered for the driver license, enforcement and security.
  - GA has considered for the driver license.
  - NJ has considered for the driver license.
  - NC has considered for the driver license.
  - OH for the DL, registration and motor carrier applications as well as food stamps, WIC (Woman, infant, children payments), ADC (Aid for Dependent Children), payments for those on permanent Workers’ Compensation and Secure system access (biometric id).
  - OR said they have discussed it, but not seriously.
  - SC is having high-level discussions on a universal card for the jurisdiction using a smart card
  - UT has considered this technology for the DL
  - WA is considering this technology for the DL.

### 2. Please elaborate on your jurisdiction’s plans/considerations for Smart Cards within the motor vehicle environment?

- DE Within DE we are considering the use of Smart Card technology for a jurisdiction-wide security access program. We are also exploring the use of Smart Card on the drivers license as a means of additional identification and possible financial payment.
- GA The Smart Card was considered during the preparation of our last RFP. However, it was cost prohibitive at that time.
- IL No plans at this time. We are in the process of converting to a digital driver’s license. Any consideration for a Smart card would be post implementation.
- NJ At present, the digitized photo license will be the platform for an undetermined number of applications. Latest thinking is for a 5-year DL smartcard.

- NC Smart card was considered in 1996 as we looked at digital imaging system. We decided against it for the present time because of (1) possible negative public reaction, (2) difficulties coordinating across jurisdiction agencies and (3) technology concerns.
- OH Smart cards were reviewed for possible motor vehicle applications approximately 18 months ago. An RFP was issued and awarded to an OH company who in turn contracted with Phoenix, Planning and Evaluation, Ltd., a VA company. A study was conducted to determine if there was justification to build a smart card application around the DL/ID card. During the course of the study, all major departments were reviewed to identify potential applications. During the study, the DL/ID application was reviewed as being the nucleus of a jurisdiction-wide smart card. A copy of the Executive Summary of the “Jurisdiction of Ohio Identification/Benefit Card Feasibility Study” that explains the focus and results of the study will be mailed to AAMVAnet.
- SC South Carolina is looking at a universal card for the entire jurisdiction. We will be looking at a “smart card” for our DMV but we are still several years away. Any information you can give me on these topics would be appreciated. We currently only have digitized commercial drivers’ license with a mag stripe. The SC DMV is currently reviewing its entire DMV organization for modernization. At this time, we do not have a feel as to the impact the smart card would have on our new organization. We will definitely look at the smart card, budget permitting.
- UT Last year we proposed legislation providing for the addition of a smart chip to our driver license. The bill passed the House, but was placed on the interim study calendar by the Senate. The issue was not addressed by any interim legislative working group. There are no plans to resurrect it this session, although our Governor is still supportive of the concept and may, at some time in the future, suggest we take another look.
- WA Very preliminary consideration - no plans yet.

**3. What benefits does your jurisdiction anticipate as a result of these initiatives?**

- DE Allow Delaware customers to take advantage of “non-stop shopping.” Payment on DMV processed transactions. Storing of jurisdiction supplied programs, information.
- NJ First benefit is it gets NJ a digitized mandatory photo license. We hope the costs will be supported by the other users of the card.
- NC It was not real clear to us what benefits would have been.
- OH By issuing a Jurisdiction of Ohio DL/ID with a smart card that could be used for multiple applications, the Jurisdiction envisioned a significant savings over the issuing of multiple smart cards. Other advantages would be the public would be required to carry one card even if they qualified or wanted to use multiple other jurisdiction services.
- UT Our concept was to build a public/private partnership in which the vendor would supply an IC type chip in return for 75% of the chip’s space. The Jurisdiction would utilize its 25% of the chip to duplicate the demographic information printed on the front of the card for security purposes. The vendor would have been allowed to sell their space for things like frequent buyer programs, credit and/or debit cards, etc. As the space available on the chip increased with new technology, we anticipated buying space from the vendor for everything from voter registration to hunting and fishing licenses, public assistance programs, etc.

**4. What barriers do you anticipate which may hinder the success of your jurisdiction’s plans in this area?**

- DE Placing all the vital information on one media and having card with value.
- IL N/A - However, we anticipate that cost will be a major issue.
- NJ There are no facilities to read a smart card with a chip.
- OH Barriers identified included: Initial and replacement cost of cards, questions of how and where to replace cards, i.e., if multiple users on a single card, who will maintain the database for replacement cards. Many of the applications reviewed could be done with mag stripe at a considerable lower cost and questions as to how well the smart card would hold up for 4 or 5 years. Perhaps the biggest barrier the study identified was a small overlap between DL/ID holders and those that would qualify for jurisdiction benefits.
- UT See question #5.

**5. If your jurisdiction has considered and rejected the use of Smart Cards for Motor Vehicle Administration Purposes, please explain the reason(s) the use of the Smart Cards was rejected.**

DE Have made no decision at this time.

ID Not seriously considered due to lack of standards, cost, yet to be adopted by private industry, too new.

IL We really have not considered and/or rejected the use of the Smart Card.

IN IN has not specifically looked at smart cards for the near future. We have, on the other hand, looked at having a multi-agency government ID/benefits card. We believe some institutional barriers exist which must be resolved or eliminated before we can successfully combine cards. IN does not see use of a smart card for at least 5-7 years.

IA A need for the smart card has not been identified by any of the users of driver's license data. At this point it appears far more cost effective to use our well developed information infrastructure to query the agency host data bases for dynamic information.

ME <sup>1</sup>The discussions never progressed to a point where the concept was rejected. Rather, the discussion was an acknowledgment that the technology is out there and needs to be considered in the future. <sup>2</sup>Not sufficient benefit for the extra cost

MA Cost prohibitive

MI Unacceptable, as electronically encoded data needs were not sufficient enough to support use of smart cards. Smart card storage capacity was far greater than our need. Privacy issues were also of major concern in MI.

MN Cost prohibitive. Current DL contract does not provide for smart card technology.

- MO The jurisdiction of Missouri is in the midst of conversion from a central drivers license issue environment to a digitized over-the-counter system. Beginning in early 1998, the jurisdiction will begin installation of a new field automation system for titling and registration. Until these projects are completed, it would be counterproductive to consider additional changes.
- MT Not allowed by our law, new technology that should be proven. Past cards with chip in place do not hold up to eight year license cycle.
- NE Not considered.
- NV Uncomfortable with new technology.
- NC See question #2.
- NY Have not considered their use except at the very fundamental discussion level. No plans to design any systems using smart cards, but have not rejected any uses either.
- ND Have not considered them.
- OH Smart cards were considered and rejected for motor vehicle applications at this time because of cost and the applications did not require smart card technology. However, it is agreed that applications in other areas other than motor vehicles will be pursued within Ohio and that the use of the smart card will be reviewed in 2 or 3 years for possible use as a Jurisdiction Identification/Benefit Card that includes the DL/ID.
- OR Not enough interest at this time for such far-reaching technology.
- PA The cost is extremely high - very difficult/expensive to replace cards that are lost.
- SC To maintain the data would require considerable maintenance to issue new smart card.
- TX Initial review was in 1995. Reasons for rejection included cost, public acceptance, overall usage and lack of exposure.

- UT We had strong opposition from two groups - one religion based and another concerned about government intrusion. The first group claimed the chip is referenced in the Book of Revelations and is the "mark of the beast." The second group saw the chip as "big brother's" way of tracking their activities. We heard everything from it would be the way the government would know everything about an individual's finances for tax and other nefarious purposes to the chip could be read from satellites in outer space.
- VT Not considered.
- WV Unable to get other jurisdiction agencies to coordinate services and buy into this concept.
- WI Cost
- WY Cost and equipment

## 6. What technologies do you currently employ within your jurisdiction?

Magnetic stripe on driver license	AR, IA, KS, MN, MT, NY, OH, PA, SC, TX, WI
1-D bar code on driver license	IA, MN, NY, OH, OR, PA, TX
2-D bar code on driver license	DE, GA, IA, NY, ND, OR, PA, WV
1-D bar code for registration	HI, ID, KS, ME, NY, TN (ID for renewal notices)
2-D bar code for registration	DE, NY, PA
1-D bar code for titling	KS, OH
2-D bar code for titling	DE, MO
1-D bar code for motor carrier	ME
2-D bar code for motor carrier	DE, IA
1-D bar code for inspections	NY
2-D bar code for inspections	DE (under development), NY
2-D bar code for enforcement	DE (testing), IA
"Other" technology	NV, PA (NV for all applications and PA for titling)
Smart Card	OH (food stamps)

## 7. What technologies do you plan to implement/utilize within the next 5 years?

Magnetic stripe on driver license	AR, IN, KS, MI, MN, MO, MT, NV, NJ, WY
1-D bar code on driver license	HI, IL, ME*, MI
2-D bar code on driver license	AR, ID, IL, IN, ME*, MA, MN, NV, NJ, NY, ND, OH, SD, TX, UT, WA (WA depending on legislative authority), WY
1-D bar code for registration	HI, KS, ME*, MI, MN
2-D bar code for registration	ID, IA, ME*, MA, MO, NV, NY, OH
1-D bar code for titling	IL, KS, ME*, MI, MN
2-D bar code for titling	ID, ME*, MA, MO, NV, NY, OH, PA
2-D bar code for motor carrier	ID, ME*, NV, NY
2-D bar code for inspection	MA, MO, NY
2-D bar code for enforcement smart card	OH DE, NJ, OH (WIC, ADC, Worker's Compensation and Security area access)

SC is looking at bar coding technology in general, haven't narrowed to specific application yet. WV says any future technology utilization is unknown at this time.

\* ME will be deciding on whether to use a 1-D or 2-D bar code for above applications.

## 8. Does your jurisdiction currently have plans to utilize the driver license as the primary identification card through which other jurisdiction services will be accessed?

- 27 said "no"  
(AR, GA, HI, ID, IL, IA, KS, ME, MA, MI, MN, MO, NE, NY, ND, OH, OR, PA, SC, SD, TX, UT, VT, WA, WV, WI, WY) (Though IA, ME and OH have not ruled it out.)
- 4 said "yes"
  - DE said it was possible - still being discussed
  - IN replied that they have organized a task force of a few key agencies to discuss a multi-use card with a pilot between BMV (Bureau of Motor Vehicles) and FSSA (Family and Social Services Agency) within 3-4 years possibly.
  - MT replied that they do have plans (and elaborate below).

**9. Please elaborate on the potential uses for the driver license within your jurisdiction.**

- DE Please refer to question #3.
- IN See question #8.
- MT Montana Fish, Wildlife and Parks. They are planning to use the driver's license and read the mag stripe for people to obtain hunting and fishing licenses.
- NJ Undetermined at this time
- OH The future use is to someday combine other smart card applications such as food stamps, WIC and other benefit programs to a universal Jurisdiction Identification/Benefit Card which will be the DL/ID card. This may not happen for a few years but the current applications are such that the change could easily be made.

**10. Which jurisdictional agencies are included in your plans for the expanded use of the driver license?**

- DE Department of Transportation, Health and Social Services, Board of Elections
- IN See questions #8 and #9.  
Michelle Moore, Director of MVIS, (317)232-0661
- MT Barney Binkelman, Fish, Wildlife and Parks, P.O. Box 200701, Helena, MT, 59620-0701, (406) 444-4558. Lisa Wanke, MVD, (406) 444-2476
- NJ Treasury, Health, Commerce, Labor, Jurisdiction Police, Insurance
- OH Dept. of Administration Services, Ron Vidmar, (614) 466-8398  
Dept. of Human Services, John Scaggs, (614) 466-2303  
Dept. of Public Safety, Don E. Cort, (614) 752-7692  
Bureau of Workers' Compensation, Dale Hamilton, (614) 466-8051  
Dept. of Health, Dave Albrecht, (614) 752-5186  
Consultant to Identification/Benefit Card, Bill Griffith, (614) 881-5896

**11. What benefits does your jurisdiction anticipate as a result of these initiatives?**

- DE Unable to address at this time, still being discussed.
- IN Task force noted in question #8 above to determine.
- MT First user of the mag stripe on a MT license.
- NV Improved customer service. Improved productivity. Security increased. Cross-utilization by law enforcement.
- NJ We have titled the project "Access New Jersey" and hope to ultimately have this as the primary identifier and authorization for all government services.
- OH By issuing a Jurisdiction of Ohio DL/ID card with a smart card that could be used for multiple applications, the Jurisdiction envisioned a significant savings over that of issuing multiple smart cards. Other advantages would be the public would be required to carry one card even if they qualified or wanted to use other jurisdiction services.

**12. What barriers do you anticipate that may hinder the success of your jurisdiction's plans in this arena?**

- DE Legislation and the ability to store personal information along with the applicant's signature.
- IN See question #14.
- MT None at present time for our department. Fish, Wildlife and Parks must program and equip numerous vendors in jurisdiction who sell hunting and fishing licenses.
- NV Potential for legislative hindrances.
- NJ Technology availability and cost
- OH Barriers identified included: Initial and replacement cost of cards, questions of how and where to replace cards, i.e., if multiple users on a single card, who will maintain the database for replacement cards. Many of the applications reviewed could be done with mag stripe at a considerable lower cost and questions as to how well the smart card would hold up for 4 or 5 years. Perhaps the biggest barrier the study identified was a small overlap between DL/ID holders and those that would qualify for jurisdiction benefits.

**13. Does your jurisdiction have any published studies regarding the plans for these cross-agency initiatives?**

AR no  
DE no  
IN no  
MT no - project not completed  
NV no  
NJ no  
OH yes

**14. If your jurisdiction has considered and rejected the use of the driver's license for cross-agency purposes, please note the reason(s) the expanded use of the driver's license was rejected.**

GA Current format has little unused area within the 2-D bar code.

IL Movement to a digital driver's license would be a prerequisite to any consideration in this area.

IN Institutional barriers exist right now. Who will issue the card? Who is responsible for replacing lost cards? Who owns the data on the card? Implementing gov't multi-services offices rather than individual services offices (one-stop shopping).

IA Lack of a champion. The principal legislative supporter left government and no one else has picked up the cause.

KS Has not been considered.

MA Not enough benefit to be derived.

MI This has been discussed, but interagency coordination is complex considering the diversity of needs; the methods for sharing expenses are unclear.

MN Costs. Future DL contracts may incorporate cross-agency use; however, not in the immediate future.

- MO Other agencies weren't interested.
- MT We have suggested that the drivers license also be used for welfare, but the agency opted to use their own "smart card" since federal funds paid for pilot.
- NE Not considered.
- NY We have considered cross-agency use, but timing and resources have not allowed efforts to move beyond the talking stages thus far. We have shared the use of "Digitized Image Data" (photographs and signatures) for purposes other than DMV use, for example, government employee I.D. cards from data in DMV files.
- ND Have not considered.
- OH We prefer to say the use of a DL/ID smart card for cross-agency use has not been rejected but delayed. The primary reason is that the cost did not justify the use of smart card on a DL/ID at this time because there was too small an overlap between the DL/ID holder and those who would qualify for jurisdiction benefits. However, OH is conducting studies using smart cards for building access, for Workers' Compensation benefits that were permanently awarded and is in the process of implementing Food Stamps using the Smart Card concept. WIC program is planned to migrate to the Food Stamp smart card within two years. Within a few years it may be practical to use a universal smart card as a means of verifying an eligible voter. All these programs are viewed as potential candidates for a Jurisdiction of Ohio multi-application citizens card built around the jurisdiction DL/ID card.
- OR We weren't ready yet to move into this technology.
- PA Very limited interest has been shown in this area at this time.
- SC Primarily the administrative expenses.
- TX Statutory limitations
- VT Not considered.
- WV The Division has looked at demonstration at AAMVA conference, but has never had an in-jurisdiction demonstration.
- WI Cost for integration. System issues and privacy issues.
- WY Will still be looked at as a possibility.

**Contacts completing survey:**

Mike Munns	AR	(501) 682-7060
Major Don Peacock	GA	(404) 624-7896
John Lovstedt	HI	(808) 832-5824
Richard Holloran	ID	(208) 334-8744
Jo Ann Wilson	IL	(217) 785-1441
Linda M. Datzman	IN	(317) 232-0067
Terry Dillinger	IA	(515) 237-3153
<sup>1</sup> Gregory Hanscom	ME	<sup>1</sup> (207) 287-8985
<sup>2</sup> David Schulz		<sup>2</sup> (207) 287-6840
John Houghton	MA	(617) 351-9949
Kim Metzger	MI	(517) 335-7083
Virginia Lockman	MN	(612) 296-3204
Raymond Hune	MO	(573) 751-5398
Darrell Beckstrom	MT	(406) 444-4536
Keith Dey	NE	(402) 471-3906
Dana Mathiesen	NV	(702) 688-2322
Pat Scheffer	NJ	(609) 292-4121
Joe Sanders	NY	(518) 474-2955
Wayne Hurder	NC	(919) 715-2374
Don E. Cort	OH	(614) 752-7692
Sandy Wood	OR	(503) 945-5112
Janet Dolan	PA	(717) 787-7713
A.J. Billings	SC	(803) 896-8009
Vona Lasater	TN	(615) 251-5217
G. Barton Blackstock	UT	(801) 965-4405
Sharon Romeo	VT	(802) 828-2028
Judith Giniger	WA	(360) 902-3850
Karen Schwartz	WI	(608) 266-0054
Deb Ornelas	WY	(307) 777-4815

## **17. CURRENT APPLICABLE USES AND EXPERIENCES OF OTHERS**

### **17.1. United States**

#### **Indiana**

Indiana is not specifically considering Smart Card technology for their motor vehicle applications. The jurisdiction is, however, considering using a Smart Card for a multi-agency government benefits card, but believes some barriers must be eliminated before this idea can be successful. The barriers they are most concerned with are ownership/issuance of the card, replacement cards, and implementing government multi-services offices where customers can have “one-stop shopping.” They have, however, formed a task force (made up of representatives from several jurisdiction agencies) that will discuss the multi-agency Smart Card and hope to have a pilot between the Bureau of Motor Vehicles and the Family and Social Services Agency within 4 years.

#### **New Jersey**

New Jersey, at present, is considering Smart Card technology for their motor vehicle applications. They plan to use a digitized photo license as the platform for several, as yet undetermined, applications. At present, they are considering a 5-year Smart Card. New Jersey hopes to offset some of the cost of the card by allowing others (vendors) to use it. They estimate that they will need only 4 of 100 “slots” of the Smart Card for DL/ID information and other jurisdiction programs, allowing plenty of space for other non-jurisdiction programs. They have titled this project “Access New Jersey” and plan to have an Request for Proposal (RFP) out in the near future.

#### **Ohio**

In late 1996, Ohio commissioned a study on the feasibility of Smart Card use in motor vehicle applications and whether there was justification to build a Smart Card application around the Driver License/Identification Card. Ohio thought that by issuing a DL or ID Smart Card that could be used with other applications, persons in their jurisdiction would only have to carry one card regardless of how many jurisdiction services they used, resulting in a significant savings for the jurisdiction. However, the initial and replacement cost of the cards, as well as confusion over which agency would be responsible for replacement of the card and the large overlap between DL/ID holders and recipients of jurisdiction benefits were considered to be significant barriers in adopting this new technology for the DL/ID.

Ohio has not entirely rejected the idea of using Smart Cards for their motor vehicle applications.

Other Ohio jurisdiction agencies are either considering or implementing other applications using a Smart Card. For example, Ohio is implementing a Food Stamp Smart Card and plans to migrate the Women, Infant, Children (WIC) program to the Food Stamp Smart Card within a couple of

years. Other applications in Ohio will also be pursued and in two or three years, the Smart Card will again be reviewed as a Jurisdiction Identification/Benefit card which includes a driver license or identification card. A copy of Ohio's Executive Summary is included with this document for reference.

## **Utah**

Utah introduced legislation in January of 1996 to their House of Representatives which included an amendment which would provide for the addition of a smart chip to jurisdiction's driver license. The intent was to allow the vendor to supply an IC chip in return for use of 75% of the chip's space. This would allow Utah to use the card as a driver license, storing all driver license data on the chip in an effort to improve security and curb fraud. Utah anticipated being able to buy more space from the vendor in the future to use for other jurisdiction programs such as voter registration and public assistance programs. This legislation passed the House of Representatives only to be placed on the interim study calendar by the Senate, and the issue was never re-visited. There are no plans at this time to revive this legislation in the near future.

The bill was unsuccessful due to strong opposition from both religious and an anti-government groups. Religious groups were concerned with the Biblical implications of the card - the Bible refers to the "Mark of the Beast," without which people would be unable to buy food or other necessities. These religious groups saw the card as the "Mark of the Beast." The government opposition groups were concerned with the card for a different reason. These groups claimed the cards would be a way for the government to keep track of their every move.

Utah's jurisdiction government is still in support of this technology and may entertain the idea again in the future.

## **17.2. Overseas**

### **Malaysia**

Malaysia has designed a concept for the design and use of a Multi-Purpose Card that will have the capability to perform a variety of functions. Malaysia will test the Multi-Purpose Card at the 1998 Commonwealth Games in Kuala Lumpur and would like a full commercial release by the year 2000. The Multi-Purpose Card will be rolled-out with eight initial applications; the National ID, the Driving License, Immigration Card, Health card and electronic cash and other financial transactions. All of these applications will initially begin in a two-card approach. The first card will be a government card combining a national identity card, a driver's license, and immigration re-entry card, and a medical application with an optional electronic purse. The second card will be a payment card combining debit, ATM and credit card applications. Malaysia is emerging as a world smart card technology leader. This new Multi-Purpose card will drastically improve the ease by which citizens of Malaysia conduct routine transactions with both the government and private business.

## 18. SMART CARD WORKING GROUP MEMBERS

### CHAIR

Terry Dillinger  
Director  
Office of Driver Services  
Motor Vehicle Division  
Park Fair Mall  
100 Euclid Avenue  
P.O. Box 10382  
Des Moines, IA 50306-0382

(515) 237-3153  
FAX (515) 237-3071  
Email: ussia8g8@ibmmail.com

### MVIS REPRESENTATIVE

Michelle Moore  
Project Manager  
Bureau of Motor Vehicles  
100 N. Senate Avenue, #N420  
Indianapolis, IN 46204

(317) 232-0661  
FAX (317) 233-1696

Donald Cort  
Deputy Administrator  
Bureau of Motor Vehicles  
4300 Kimberly Parkway  
Columbus, OH 43266-0020

(614) 752-7692  
FAX (614) 752-4749  
or (614) 752-7220  
Email: cort@dps.state.oh.us

William Donahue  
Administrative Analyst II  
Division of Motor Vehicles  
222 East Jurisdiction Street  
Trenton, NJ 08666

(609) 633-3678  
FAX (609) 292-7040  
Email: williamdonahue@dot.state.nj.us

### DL REPRESENTATIVES

Joseph Sanders  
Director  
Driver Systems  
Department of Motor Vehicles  
Empire Jurisdiction Plaza  
Albany, NY 12228

(518) 474-2955  
FAX (518) 474-2596

G. Barton Blackstock  
Chief  
Control/Driver Improvement/DWI Programs  
Driver License Division  
Department of Public Safety  
4501 South 2700 West  
Salt Lake City, UT 84119

(801) 965-4405  
FAX (801) 965-4496

### **LEGAL SERVICES REPRESENTATIVE**

Michael J. Alderman  
Assistant General Counsel  
Department of Highway Safety and Motor Vehicles  
2900 Apalachee Parkway  
Neil Kirkman Building  
Tallahassee, FL 32399

(904) 488-1606  
FAX (904) 922-6784  
Email: aldermm@hsmv.state.fl.us

### **PTS REPRESENTATIVE**

Lt. Paul Krisavage  
Commander, Headquarters Traffic Unit  
Connecticut Jurisdiction Police  
P.O. Box 2794  
Middletown, CT 06457

(860) 685-8060  
FAX (860) 685-8349

### **RTVDM/MOTOR CARRIER REPRESENTATIVE**

Art Lemon  
Department of Highway Safety & Motor Vehicles  
2900 Apalachee Parkway, Room A108  
Neil Kirkman Building  
Tallahassee, FL 32399

(904) 921-0066  
FAX (904) 487-2328

### **INDUSTRY REPRESENTATIVES (To be invited when appropriate)**

John Harker  
Account Manager  
Symbol Technologies, Inc.  
401 Hackensack Avenue  
Hackensack, NJ 07601

(914) 277-2234  
FAX (914) 277-2235

Tate Preston  
Government Marketing Representative  
Datacard, Inc.  
11111 Bren Road West  
P.O. Box 9355  
Minneapolis, MN 55440

(612) 988-1827  
FAX (612) 988-2996  
Email: tate\_preston@datacard.com

Dino Redmond  
VP, Technology  
NBS Imaging Systems, Inc.  
1530 Progress Road  
Fort Wayne, IN 46808

(219) 484-8611  
FAX (219) 482-2428  
Email: dinor@nbstech.com

Peter J. Ognibene  
1127 Cresthaven Drive  
Silver Spring, MD 20903-1607

(301) 434-8572  
FAX (301) 434-8573  
Email: pjsmart@aol.com

Steve Zullo  
3-G International  
Loisdale Court  
Suite 100  
Springfield, VA 22150

(703) 922-3448  
FAX (703) 922-4603  
Email: szullo@3gi.com

### **FHWA REPRESENTATIVE**

Kate Hartman  
Department of Transportation  
Office of Motor Carriers  
400 7<sup>th</sup> Street SW, HSA-20  
Washington, DC 20590

(202) 366-2742  
FAX (202) 366-3518  
Email: kate.hartman@fhwa  
.dot.gov

### **NHTSA REPRESENTATIVE**

Ellen Ross  
Department of Transportation  
400 7<sup>th</sup> Street SW, NTS 32  
Washington, DC 20590

(202) 366-4800  
FAX (202) 366-2746  
Email: eross@nhtsa.dot.gov

**AAMVA REPRESENTATIVE**

Mike Calvin  
Vice President Driver Services  
4301 Wilson Boulevard, Suite 400  
Arlington, VA 22203

(703) 908-8262  
FAX (703) 522-1553  
Email: [mikec@aamva.org](mailto:mikec@aamva.org)

**AAMVAnet REPRESENTATIVE**

Sonja Freeman  
Systems Analyst  
4301 Wilson Boulevard, Suite 400  
Arlington, VA 22203

(703) 908-5842  
FAX (703) 522-1553  
Email: [sonjaf@aamva.org](mailto:sonjaf@aamva.org)

## **21. FURTHER INFORMATION**

## APPENDIX A

1. OH Executive Summary (May 1997)..... **Insert 1**  
**State of Ohio Identification/Benefit Card Feasibility Study**
  
2. Purchasing “Group Drafts Smart Card Plan” Federal ID cards would include Biometrics, encryption keys, Elana Varon, FCW Policy and Procurement, October 6, 1997.....  
**The Electronic Processing Initiatives Committee (EPIC), an interagency task, is working on a federal policy for smart cards to be deployed government-wide.**  
**[Article not attached - Copyrights not granted free of charge]**
  
3. Smart Card Chip Reads fingerprints, Andrew Craig, Tech Web, February 17, 1998. ....  
**Siemens, a Germany technology company, has recently revealed a smart card chip that doubles as a fingerprint reader to verify the user’s identity. The Fingertop Sensor chip was demonstrated at the SmartCard ’98 show.**  
**[Article not attached - Copyrights not granted free of charge]**
  
4. Websites: [Public domain]
  - MSC...Flagship Applications, <http://mdc.cinenet.net/flagship/index.html> .....  
**Multimedia Super Corridor effort in Malaysia. “The ‘Multimedia Environment’ Flagship Applications will provide both Malaysian and international companies with the opportunity to operate in an environment of close co-operation with leaders in the multimedia industry, research and academic institutions, and customers, in one of the world’s most attractive business regions. These applications will also allow companies to build centres of excellence for their R&D activities, create hubs to efficiently deliver value-added services to companies throughout the region, and innovate entire businesses by taking full advantage of the MSC’s unique environment and infrastructure.”**
  
  - ITS 101 Technology Closeup: Smart Cards for ITS and Beyond, Peter Harrop, <http://www.itsworld.com/ITS101/tc0198.html>.....  
**“This Flagship Application seeks to develop a single and common platform for a Multi-Purpose Card (MPC) that will enable the Government and private application providers to implement smart card solutions without duplication of effort and investment.”**  
**[Article not attached - Copyrights not granted free of charge]**

- License Plate Recognition Systems, Lee J. Nelson,  
<http://www.itsworld.com/97article/9701article.htm>.....  
**“Video-based automatic vehicle identification is carving a niche for itself in applications such as road tolling and access control.”**  
[Article not attached - Copyrights not granted free of charge]
- Smart Cards for ITS and Beyond, Peter Harrop, ITS World, February 1998. ....  
**“Smart cards are becoming increasingly popular in Europe, Asia, and around the world and are poised for widespread use in smart parking, electronic toll collection, fleet management, traveler, information, and other ITS applications.”**  
[Article not attached - Copyrights not granted free of charge]
- 5. ITS Taking Hold in Malaysia, Michael J. Avery, South Korea,  
ITS World, February 1998.....  
**“Malaysia and South Korea are two of the Asia-Pacific countries where rising incomes are fueling vehicle sales - and traffic growth. To address the worsening congestion, the countries are applying ITS more widely than ever.”**  
[Article not attached - Copyrights not granted free of charge]
- 6. Fear, trembling and smart cards, Lavarr Webb, Desert News Science Technology,  
Wednesday, August 13, 1997. ....  
**“Like it or not smart cards are in almost everyone’s future...Smart cards will provide security and control over money, data and information far beyond what is possible today.”**  
[Article not attached - Copyrights not granted free of charge]
- 7. Utah firm advances technology, Brooke Adams, Desert News Science Technology,  
Wednesday, August 13, 1997. ....  
**“But while the politicians distance themselves from the technology, a private company in Utah is plowing ahead with it, and smart card projects are popping up across the United States.”**  
[Article not attached - Copyrights not granted free of charge]
- 8. China Contract Awarded, Corporate News, Law Enforcement Technology, July 1997.....  
**“Viisage Technology has signed an agreement with China Jon Son groups to develop and produce smart cards to be used in the Driver “Penalty Card” program. As drivers are stopped for violations, any resulting fines can be paid on the spot, using the smart card driver’s license as a debit card.”**  
[Article not attached - Copyrights not granted free of charge]

9. Tiny chip not just a token, Springs firm coins transit pay card, Leyla Kokmen, Denver Post, July 21, 1997.....  
**“The Go Card ...The size of a credit card, the Go Card pays the fare each time a rider swipes it about 2 inches near the target reader. The card is integrated with regional rail, bus, toll road and parking authorities for acceptance of fares.”**  
[Article not attached - Copyrights not granted free of charge]
10. Looking for The Pot of Gold, Pete Hisey, Credit Card Management, July 1997. ....  
**“Multiple-use smart cards promise to revolutionize the payments industry---and earn issuers and acquirers a transaction-fee bonanza. But with several incompatible schemes entering the marketplace, the threats, in the form of wasted investments, balance out the opportunities. And more important, do consumers even want the things?”**  
[Article not attached - Copyrights not granted free of charge]
11. The Search for A Compelling Case, Pete Hisey, Credit Card Management, July 1997. ....  
**“American Express Co. and the Hilton Hotel chain are undertaking an aggressive smart card test through the end of the year aimed at the population segment most consider primed for smart card adoption: frequent travelers.”**  
[Article not attached - Copyrights not granted free of charge]
12. Differing Takes on MasterCard’s Multos, Pete Hisey, Credit Card Management, July 1997.....  
**“MasterCard International has leapt into the front of the smart card pack with the introduction of its Multos multiple-application operating system. Critics, however, charge that the system is at least partly proprietary and unnecessarily cumbersome.”**  
[Article not attached - Copyrights not granted free of charge]
13. PCs and Smart Cards Are Starting to Talk, techwatch, Card Technology, March/April 1997.....  
**“Smart cards and personal computers will be talking to each other a lot more by the end of this year than they do now, technology experts agree. The only question is what type of interface devices will be most widely used to accomplish the task and who will be the first to push the price of such PC/smart-card readers low enough to enable them to become standard PC peripherals.”**  
[Article not attached - Copyrights not granted free of charge]
14. Atlanta Visa Cash Issuers Look to Long-term Efforts, techwatch, Card Technology, March/April 1997.....  
**“Card issuers involved in last year’s Visa Cash pilot during the Atlanta Olympics are now turning their attention to creating a solid smart card foundation in the city.”**  
[Article not attached - Copyrights not granted free of charge]
15. Escheatment Issues Could Impact Stored-Value Cards, techwatch, Card Technology, March/April 1997.....

**“Admst the discussions on bringing stored-value smart cards to the United States, one area that’s received relatively little attention is the fairly esoteric topic of escheatment-the legal concept that allows states to take over unclaimed or abandoned property.”**

**[Article not attached - Copyrights not granted free of charge]**

16. Smart Card Marketing Needs to Stress Convenience, techwatch, Card Technology, March/April 1997.....

**“With smart-card marketing still in its infancy, those in the industry differ on what media they find most effective. But they all agree on one thing-whatever you do, don’t say you’re replacing cash.”**

**[Article not attached - Copyrights not granted free of charge]**

17. Smart Cards Hit the Trade-Show Circuit, techwatch, Card Technology, March/April 1997.....

**“Trade show exhibitors always are hungry for information about potential customers. As a result, they’ll do everything from giving away premiums in return for business cards to scanning show-issued mag strip cards to collect key attendee demographic data.”**

**[Article not attached - Copyrights not granted free of charge]**

18. Mondex USA’s Internet Bet, techwatch, Card Technology, March/April 1997.....

**“The Internet will play a role in Mondex USA’s smart-card strategy. So will multi-application cards. But is all this, and a possible \$100 million investment, really necessary? Competitors doubt it.”**

**[Article not attached - Copyrights not granted free of charge]**

19. Half of Mondex Cardholders Active in Swindon Test, techwatch, Card Technology, March/April 1997.....

**“To date, roughly 13,000 cards have been distributed to customers of Mondex founder National Westminster Bank and Midland Bank. Of those, about half are being used regularly...”**

**[Article not attached - Copyrights not granted free of charge]**

20. Less Than Stellar Debut for Smart Cards in NYC, The Financial Times, Date ? . . . . .

**“STORE CLERKS have emerged as the biggest obstacles preventing American shoppers from paying with ‘smart cards’ - stored-value cards embedded with a computer chip.”**

**[Article not attached - Copyrights not granted free of charge]**

21. Uncle Sam May be Getting Serious About Smart Cards, Card Technology, April 1998.....  
**“Uncle Sam has seen the future, and it apparently includes smart cards. The General Services administration, the purchasing arm of the federal government, recently approved six vendors how now can sell card systems for purchasing, travel and fleet use to more than 120 federal agencies. Included in many of those sales plans will likely be smart card applications, vendors involved and government watchers agree.”**  
 [Article not attached - Copyrights not granted free of charge]
22. Alliances Growing in Contactless Card Arena, Card Technology, April 1998 .....  
**“The world of contactless smart cards is getting more attention thanks to a series of major alliances announced in recent months. The new pacts demonstrate that major players such as Motorola Inc. and Japan’s Hitachi Lid. Realize contactless cards are poised to move beyond their transit market and will be used for such applications as building security, to pay road tolls and for pay telephone use, industry analysts agree. More alliances are likely before the industry analysts agree. More alliances are likely before the industry analysts agree. More alliances are likely before the industry settles on a contactless standard, ...”**  
 [Article not attached - Copyrights not granted free of charge]
23. Late-Breaking Card News, Card Technology, April 1998 .....  
**“...The state of New Jersey next year plans to begin issuing AccessNJ smart card licenses.”**  
 [Article not attached - Copyrights not granted free of charge]
24. Building the Multiapplication Business Case, Card Technology, April 1998 .....  
**“When smart card seers gather, talk invariably turns to multiapplication smart cards. Putting more than one application on a card is touted as the wave of the future, a way to deal with high card costs while seemingly answering consumers’ desire to cut down on the number of cards carried in the average purse or wallet.”**  
 [Article not attached - Copyrights not granted free of charge]
25. What is a Multiapplication Card? Card Technology, April 1998 . .....  
**“A card that allows a cardholder to do more than one thing isn’t necessarily multiapplication, it may only be multifunction.”**  
 [Article not attached - Copyrights not granted free of charge]

26. Spain Dances to a One Card Beat, Anne-Sophie Bolon, Card Technology, April 1998. ....  
**“Multiple programs are using the same card technology to propel Spain to the forefront of smart card users.”**

[Article not attached - Copyrights not granted free of charge]

**Report on Smart Cards can be visited at this site: [www.tr.com](http://www.tr.com)**

[All “Report on Smart Card” articles are not attached - Copyrights not granted free of charge]

27. Report on Smart Cards, January 20, 1997, Volume 11, Number 1. ....
- **GSA to Award Contracts for Smart Cards, Issues Draft Statement of Work**
  - **France Moves Toward Chip Card Future**
  - **Visa Delays ‘SET’ Rollout While MasterCard Completes First Transaction**
  - **Excerpts From GSA Draft Statement**
  - **HFN Finds ‘Unbridled Enthusiasm’ For Smart Cards Among Users**
28. Report on Smart Cards, February 3, 1997, Volume 12, Number 2. ....
- **Olympic Committee, Visa Cash Trashed by Small Firm With Big Claim**
  - **Hometown Smart Cards To Boost Main Street Sales**
  - **Analysts’ New Study Predicts Explosion, In the use of E-Money**
  - **A Little ‘Musical Chairs’ For the Smart Card Industry**
  - **Federal Smart Card User Group Sets Consortium Meeting Feb. 13**
  - **Items of Interest**
  - **Appeals Court Remands Encryption Export Case**
29. Report on Smart Cards, February 17, 1997, Volume 12, Number 3. ....
- **Mondex Launches its First Canadian Trial**
  - **To Tax or Not to Tax the Internet?**
  - **Administration Moving to Coordinate Electronic Commerce, Internet Policies**
  - **Gemplus, Schlumberger Announce New Age of Togetherness**
  - **Visa to Expand Chinese ATM Service**
  - **DataCard, Racal Forge Card Security Agreement**
  - **Motorola to Supply Chips for Visa Card, Hits Japanese Smart Card Market**
  - **Items of Interest**
30. Report on Smart Cards, August 4, 1997, Volume 11, Number 15. ....
- **Multiapplication Smart Cards Get Boost With Gemplus, IBM Venture**
  - **Siemens Will Execute Java Instruction Set Directly to Hardware, Making Java Systems Faster, Cheaper**

**U.S. Government Update:**

New EFT Rule Will Address Unbanked, Vendor Payments Information

Tough Challenges, SIMple Solution? GSM Must Overcome Strong Competitors,  
Demanding Users to Win the PCS Wars

**Business Ventures:**

Discount Investment Corp., Paz Buy Mondex Franchise in Israel  
Hewlett-Packard, AT&T Team For Electronic Commerce  
Racom Provides Contactless Cards To Manufacturer of Printed Circuit Boards

**Industry News:**

Forum Work Group Focuses On Industry Interoperability  
New Division for Transactions, Chip Tests at Schlumberger  
CommerceNet Looks East To Expand Its Reach

**SET:**

Concentric Network Will Participate In U.S. Government Pilot  
SET Mark Unveiled At Consortium Showcase

31. Report on Smart Cards, September 1, 1997, Volume 11, Number 17.....

- **TTI Acquires EDS Smart Card System Could Be Makings of Major Competitor, Experts Say**
- **ATM CardPay Plans to License New ATM?EFT Infrastructure to Banks**
- **Sun Microsystems Acquires Integrity Arts to Help Develop JAVA**
- **Orga Will Introduce Over-the-Air, Add-On Application Service for SIM Cards**

**Products:**

Scotiabank 'Chip Farm' Add-On Accepts VISA Cash and Mondex  
NetChannel's Internet Service Uses Smart Cards in Set-Top Boxes  
Philips Semiconductors' Smart Card Chip Chosen for New Visa Merchant Card  
Orga Offers Newest Addition To Smart Card Personalization Printer Line  
Oki's Value-Checker Smart Card Readers To Be Used With Banksys' Proton

**Pilot:**

Smart Card Pilot Started In Northern California

**International:**

Hong Kong Supermarket Chain To Accept VISA Cash  
SET Comes to Germany in Pilot By Commerzbank and Karstadt

**Security:**

Federal Encryption Rules Unconstitutional, Judge Says

32. Report on Smart Cards, September 29, 1997, Volume 11, Number 19.....

- **Netscape Hopes to Expand Smart Cards Beyond Browser and E-Mail**
- **Smart Card Forum Elects Officers, New Board**
- **ABA Helps Banks Comply With EFT '99, Provides EDI Services**
- **Future for Encryption Bill Appears to Be Bleak**

**Partnerships:**

Oberthur, Bull, Schlumberger To Supply French Health Cards  
CSI Receives \$3 Million in Funding To Develop CardBASE2000 System

**Products:**

Digital's Microprocessor Makes Smart Phone Functions Faster

Comsat Releases Smart Card Personal Communications Service  
 Schlumberger's New Smart Card To Add Applications to Wireless Phones  
 Philips' Add-On Feature Turns Digital Phones Into 'Smart' Phones  
 CTT Will Help With Marketing NTRU's New Public Key System  
 Lucent Technologies' Inferno to Be Used On Small Devices, Including Smart Cards

**Industry News:**

DANMONT Card Reaches 10 Million-Transactions Mark  
 Visa Executives Say Checks, Cash Will Become Extinct  
 Industry News Briefs

**Letter to the Editor:**

Last Chance for Bank Brands

33. Report on Smart Cards, October 13, 1997, Volume 11, Number 20.....

**U.S. Government to Introduce Navy, Western Health Multi-Application Card**

**Regulation:**

Industry Mixed Over Whether Stored-Value Card Issuers Must Register With U.S. Treasury  
 EFT Proposal Says Benefits Have to Go Through Federally Insured Accounts

**Pilots:**

Motorola Is Supplying Chips For N.Y., Smart Card Project  
 Seattle to Use Contactless Transit Smart Card

**Products:**

ImagineCard Gives Corporations Secure Use of Networks  
 Gemplus, Far Point Offer Electronic Gift Certificate  
 Verifone, HAN Let Bank Customers Use Smart Cards for Business  
 Schlumberger's New Products Support Microsoft Windows

**Standard:**

Java-Enabler Cyberflex Kits Are Popular, Says Schlumberger

**Partnership:**

Syntellect Application Lets Banks Process Over the Phone

**Industry News:**

Lucent to License/Sell Its Smart Card Property  
 SCIA Adds Two Members To Its Board of Directors  
 Retailers Enjoy the Switch to Smart Cards But U.S. Market Is Difficult  
 Convenient Stores Are Logical Retail Environment For Cards, But Retailers Still Hesitate, Says Survey

34. Report on Smart Cards, October 27, 1997, Volume 11, Number 21.....

- **Schlumberger Releases First JAVA SIM Card**
- **Motorola, Matsushita Will Develop FeRAM Chips for Faster Cards That Store More Money**
- **Oki Provides Personal Card Readers, Schlumberger Provides VISA Cash for N.Y., Pilot**
- **VeriFone Provides N.Y., Project With Terminals, Personal ATM Devices**
- **Gemplus Releases Card to Generate Key Cryptography and Contain Electronic Purse**
- **Gemplus to Supply 60,000 Smart Cards to University of Toronto**

- **Four Firms Team for Test of Student Application of E-Commerce Via Wireless PCS System**

**Pilots:**

- Bank of America, Visa Test First U.S. 'Combi,' Two-Chip Card
- DOD Contractors to Receive E-Money Through Smart Cards
- **Intellect Wins Award for Card Terminal '8590'**
- **Set 1.0 Experiences Two 'First' Transactions**
- **Visa, Gemplus Announce Products Based on Java Card 2.0 API**
- **Ascom Monetel, Schlumberger Win SESAMEs For Best Application, Innovation**

**INSERT PAGE**  
**[This page left intentionally blank]**