American Association of Motor Vehicle Administrators (AAMVA)

Date: 2003-09-25

AAMVA Uniform ID Subcommittee - UID7 Task Group

Secretariat: AAMVA

Personal Identification — AAMVA International Specification — DL/ID Card Design

Contents

Page

Foreword

The American Association of Motor Vehicle Administrators is a tax-exempt, nonprofit organization striving to develop model programs in motor vehicle administration, police traffic services and highway safety. The association serves as an information clearinghouse for these same disciplines, and acts as the international spokesman for these interests.

Founded in 1933, AAMVA is a voluntary, nonprofit, tax exempt, educational organization. AAMVA represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.

The association's programs encourage uniformity and reciprocity among the states and provinces, and liaisons with other levels of government and the private sector. Its program development and research activities provide guidelines for more effective public service.

AAMVA understands its unique positioning and the continuing role identification security will play in helping the general public realize a safer North America. The association believes ID security will help increase national security, increase highway safety, reduce fraud and system abuse, increase efficiency and effectiveness, and achieve uniformity of processes and practices.

This specification was developed as one part of an extensive program to improve the security of the DL/ID card conducted by AAMVA's Uniform Identification Subcommittee. To accomplish this program, the Subcommittee created a number of task groups, including the Card Design Specification Task Group that developed this specification. The Task Group surveyed and met with many stakeholders during the development effort. The Task Group gathered information from government and non-government users of the DL/ID card to determine their uses for the DL/ID card and how they believed the card should function. In addition, the Task Group surveyed and met with industry experts in the area of card production and security to gather their advice, especially about the physical security of the card.

The intermediate work of the Task Group was repeatedly reviewed by the UID Subcommittee as a whole and approved by the AAMVA Board.

0 Introduction

This document provides specifications for the design of driver license (DL) and identification (ID) cards issued by AAMVA member jurisdictions. The intent of the specification is to improve the security of the DL/ID cards issued by AAMVA's members and to improve the level of interoperability among cards issued by all jurisdictions.

0.1 Functional Requirements

At its August 2002 meeting, the AAMVA Board of Directors approved the following list of functional requirements for the DL/ID card:

- Evidence of the privilege to drive
- Identification
- Age verification
- Address/residence verification*
- Automated administrative processing

Originally the DL satisfied only the first of these proposes. It has long since become the identity document of choice for satisfying the other four. A clear indication of this is the fact that virtually every motor vehicle administration in the US and Canada issues a non-driver ID card to serve these needs for those who do not have a DL.

The mobility of the driving population has made it necessary for AAMVA's members to focus increasingly on issues affecting the interoperability of the driver licensing system. Jurisdictions routinely process large number of DL applicants who are transferring from one jurisdiction to another. In addition, drivers regularly drive in jurisdictions other than the one in which they are licensed. In order to effectively manage this mobile driving population, AAMVA has long stressed the one driver, one license, and one driver control record concept. In order to implement this concept, AAMVA has placed increasing emphasis on interoperability of driver licensing systems, including the DL itself. Many of the details of this specification are intended to improve the interoperability of the Dl cards, particularly the machine readable technology (MRT) used on the card.

The increased use of the card for purposes other than proof of the privilege to drive have greatly increased the motivation to alter or counterfeit the DL/ID card. Therefore, this specification places great emphasis on improving the security requirements for these cards.

0.2 Interoperability

The AAMVA National Standard for the Driver License/Identification Card, AAMVA DL/ID-2000 did not require the use of any MRT on the DL/ID card. The AAMVA DL/ID-2000 provided instructions for the contents and format for a number of different types of MRT. A jurisdiction could choose one or more of these, or choose to have no MRT at all. In addition, jurisdictions using the same MRT did not always interpret or implement the instructions in AAMVA DL/ID-2000 in the same manner. As a result of these variances, the desired level of interoperability has never been achieved.

Jurisdictions that follow this specification will all implement a common MRT on their cards. In addition, much effort has been made to reduce confusion about the contents and format of the common MRT. Furthermore, space has been allotted in the layout for an additional MRT should a jurisdiction choose to have one on its card.

Jurisdictions are strongly encouraged to coordinate implementation efforts within the AAMVA community to resolve any interpretation issues and insure a high level of commonality in their implementations.

0.3 Commonality

Closely related to the issue of interoperability is the issue of commonality. AAMVA DL/ID-2000 did not provide guidance on the physical layout of the card. As a result, the graphic design and layout of DL/ID cards varied greatly from jurisdiction to jurisdiction. In addition, since jurisdictions rarely if ever replace all existing cards as soon as they begin issuing a card with a new design, great variations have been possible even within a single jurisdiction. Some estimates place the number of design variations for valid DL/ID cards among AAMVA members well in excess of 200. This makes it extremely difficult for law enforcement, or anyone else, to recognize a valid license, especially if it comes form another jurisdiction. This specification calls for the use of a zoned layout that will increase the commonality of appearance of the cards from all jurisdictions.

0.4 Security

AAMVA DL/ID-2000 provided only basic guidance in the area of security features that would prevent alteration or counterfeiting of the card. This specification provides a much more comprehensive set of requirements for the security features of the DL/ID card. Jurisdictions that follow this specification will all have a common security feature on their DL/ID card. In addition, each jurisdiction will choose several other security features to address a variety of threats to the security of the card.

0.5 Replacement of AAMVA DL/ID Card 2000

This specification replaces the existing AAMVA National Standard for the Driver License/Identification Card, AAMVA DL/ID-2000. Since at the time of publication of this specification and for some time after, many jurisdictions will continue to issue licenses based on AAMVA DL/ID-2000, that document will continue to be available. . However, when a jurisdiction develops new card designs, it should use this document for guidance instead of AAMVA DL/ID-2000.

0.6 Compatibility with ISO Standard for International Driver License

This specification generally follows the draft ISO/IEC 18013-1: ISO compliant driving license – Part 1: Physical Characteristics and Basic Data Set. This specification starts a move toward compatibility with the ISO standard, but does not fully comply with the current draft. In order to satisfy certain requirements, this specification departs from draft ISO standard in several areas. For example, this specification describes a vertical format for a driver under the age of twenty-one, but the draft ISO standard has no provision for a vertical format. It is hoped that these differences eventually will be resolved, possibly before the ISO standard is approved and published. However, AAMVA felt it needed to go forward with this specification to deal with serious security problems and interoperability issues with the cards currently issued by its members.

Personal Identification — AAMVA International Specification — DL/ID Card Design

1 Scope

This specification was developed by AAMVA for the production and use of government-issued diving license / identification card documents (DL/IDs). Private institutions and other organizations may benefit from DL/ID uniformity established by this specification, but the functional requirements are primarily for the benefit of motor vehicle agencies and law enforcement.

This specification supersedes the AAMVA DL/ID 2000 Standard published June 6, 2000. Requests for interpretation, suggestions for improvement or addenda, or defect reports are welcome. They should be sent to AAMVA Standards Program, 4301 Wilson Boulevard, Suite 400, Arlington, VA 22206.

A DL/ID is in conformance with this standard if it meets all mandatory requirements specified directly or by reference herein, including requirements contained in annexes A, B, C, D, and E. There are additional requirements of other standards as referenced in Annexes F and G that may be adopted by issuing authorities.

2 Normative reference(s)

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this AAMVA specification. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

European Commission Directive 2000/56/EC of 14 September 2000 O.J. EC No. L 237/45

European Union Council Directive 97/26/EC of 2 June 1997 O.J. EC No. L 150/41

European Union Council Directive 91/439/EEC of 29 July 1991 O.J. EC No. L 237/1

European Union Council Directive 96/47/EC of 23 July 1996 O.J. EC No. L 235/1

European Union Council Directive 96/C 204/07 O.J. EC No. C 204/20

European Union Council Directive A-0123/96 O.J. EC No. C 181/16

European Union Council Common Position No. 14/96 of 26 February 1996 O.J. EC No. C 120/1

European Union Council Directive 96/C – 54/06 of 23 February 1996

ANSI D-20: *Data Element Dictionary – Traffic Records System*

ISO/IEC 18013-1: *ISO compliant driving licence – Part 1: Physical Characteristics and Basic Data Set*

ISO/IEC 7810: *Identification cards - Physical characteristics*

ISO/IEC 7811: *Identification cards – Recording Techniques*

ISO/IEC 7812: *Identification cards – Registration Numbers*

ISO/IEC 7816: *Identification cards – Integrated Circuit Cards with contacts*

ISO/IEC 10373: *Identification cards - Test methods*

ISO/IEC 10536: *Identification cards – Integrated Circuits – Close–Coupling*

ISO/IEC 10918: JPEG 2000

ISO/IEC 11693: *Identification cards – Optical Memory – General Characteristics*

ISO/IEC 11694: *Identification cards – Optical Memory – Linear Recording Method*

ISO/IEC 14443: *Identification cards – Integrated Circuit - Proximity*

ISO/IEC 15693: *Identification cards – Integrated Circuit Vicinity*

ISO/IEC 15438: *Automatic Identification and Data Capture Techniques – International Two-dimensional Symbology Specification – PDF417*

ISO/IEC 15444-1: *JPEG 2000 image coding system -- Part 1*

ANSI/ASQZ Z1.4: *Military standard, sampling procedures and tables for inspection by attributes*

MIL-L-61002 *Labels, Pressure Sensitive Adhesive, for Bar-Codes and other Markings*

UN Convention on Road Traffic *(Geneva – 19 September 1949), amended 22 October 1964*

UN Convention on Road Traffic *(Vienna – 8 November 1968), Amendment 1 amended 3 September 1993 (E/CONF.56/16/REV.1/Amend.1)*

ICAO Machine Readable Travel Documents. Part 1 – Machine Readable Passports. Fifth Edition – 2003.

3 Term(s) and definition(s)

For the purposes of this AAMVA specification, the terms and definitions given in the following apply:

4.1
alphabetic (A)
Apha characters (UPPERCASE letters from A to Z).

3.2
alphanumeric (ANS)
Alpha characters (UPPERCASE letters from A to Z), numeric characters, space, and special characters.

3.3
cardholder
An individual to whom a driver license or identification card is issued.

3.4
country distinguishing sign
Abbreviation used on the license document (human-readable) for countries that issue driver license.

3.4
customer record
Information pertaining to the cardholder that is stored in a jurisdiction database. Such records commonly include biographical and demographical data, address information, driving privileges, traffic convictions, driving restrictions, and information from prior jurisdictions of record. Customer records may also be linked to vehicle registration data.

3.5
data element
An item of data that may appear on the license in either human or machine-readable form.

3.6
digital
Any data that is composed of a discrete sample or collection of discrete samples that are represented as finite numbers.

3.7
document recognition
The educational knowledge and ability to recognize the validity of the driver license card of both national and international jurisdictions including data elements, formatting, visual images (e.g. photo image, signature), electronic readable features and document security features.

3.8
driver license (DL)
A document issued to a driver license cardholder by a driver license issuing authority, or their designated agent, granting the individual the right or privilege to operate a motor vehicle within its jurisdiction. The document may facilitate driver license transactions and provide input data for such transactions. This issued document incorporates several elements and qualifications regarding the driver license card holder: positive identification of the individual applicant; evidence of knowledge of laws and practices; practical driving proficiency in specific motor vehicle class categories; and, the individual's health and driving privilege restrictions (e.g. corrective eye lenses) and endorsements enabling special or extra categories of driving privileges. NOTE: The ISO term for this document is :driving license" and appears in some places in this document.

3.9
DL/ID
Refers generally to both or either driver licenses (DL) and identification cards (ID).

3.10
first line inspection (level 1)
Examination done without tools or aids that involves easily identifiable visual or tactile features for rapid inspection at point of usage.

3.11
human-readable
Data or information that is printed or engraved that is visually present on a driver license.

3.12
identification card (ID)
A document issued to an individual by an authorized government issuing authority, or their designated agent, for the purpose of identification not related to the operation of motor vehicles. The document may facilitate identity transactions and provide input data for such transactions. Such documents may include, but are not limited to, non-driver identification cards, senior citizen cards, handgun permits, and employee identification cards.

3.13
image
Digital data that represents the visual likeness of its subject, such as a portrait, finger print, or signature. Images may be collected, stored, and rendered for visual inspection using a variety for digital formats.

3.14
informative
Describes a section of the standard that provides supplementary information intended to assist in the understanding and use of this standard.

3.15
issuing authority
A statutorily authorized agent organization that issues driver licenses and/or identification cards such as a Ministry of Transport, Department of Motor Vehicles, or Police Agency.

3.16
machine-readable
Data or information that is encoded into a machine-readable medium, such as a magnetic stripe, bar code, optical memory, or integrated circuit card.

3.17
mutual recognition agreements
Reciprocal agreements between governments of two nations, regions, states, provinces, or territories for the right of its citizens to drive an eligible vehicle in each others jurisdictions without the requirement of undergoing additional practical and/or written testing.

3.18
non-portrait side of card
The opposite face from the portrait side.

3.19
numeric (N)
Digits 0 to 9.

3.20
portrait side of card
Face of the card carrying visual information containing the reproduction of the portrait of the card holder and card holder identifiers.

3.21
second line inspection (level 2)
Examination that requires the use of a tool or instrument (e.g., UV light, magnifying glass, or scanner) to discern.

3.22
signature panel
Area used for cardholder signature that is receptive to writing instruments.

3.23
third line inspection (Level 3)
Inspection by forensic specialists conducting detailed examination allows for more in-depth evaluation and may require special equipment to provide true certification.

3.23
visual special characters (S)
! “ # $ % & ‘ ( ) * + , - . / : ; < = > ? [\ ] ^ _ @. A special character is removed from this category when it is used as a delimiter between data elements in machine-readable technology.

4 Human-readable data elements

4.1 Data element tables

Table 1 in section 5.2 describes the mandatory data elements that must visually appear on compliant DL/ID documents. Jurisdictions may go beyond these minimum mandatory requirements, as long as each mandatory requirement is met. Table 2 in section 5.3 describes optional data elements that may visually appear on compliant DL/ID documents. Jurisdictions may include additional data elements and features on their compliant DL/ID document. However, if any of the optional data elements are included on the document, they should appear as descried by the rules in this specification.

4.2 Mandatory data elements

Column 1 (**Data Ref.**): serves as a reference indicator for citation elsewhere in this standard and in other documents.

Column 2 (**On card reference**): The reference number may be visibly included as text on the DL/ID to identify the data element for purposes of interpreting the data and other international interchange requirements.

Column 3 (**Zone placement**): indicates the location on the DL/ID where the data element must be placed. Location of the zones is provided in Annex A of this specification. In some cases, data elements may appear in a choice of zones, or be repeated in another zone. Such data elements are marked with the appropriate multiple zone placements. If no zone is listed for a data element, it may be placed anywhere on the card as long as it does not interfere with the required placement of other data elements.

Column 4 (**Data element**): common name or phrase that designates what information is to be inscribed on the card. If **on card reference numbers** are not used, then these **data elements** must be labeled using text on the card. When abbreviations are provided in bold, they are available for use by jurisdictions. If a jurisdiction uses an abbreviation to designate a data element, the abbreviation must conform to the bold abbreviations when provided. Unless otherwise specifically stated, formatting rules of *ANSI D20 Data Dictionary for Traffic Record Information Systems* must be followed. Data elements must appear in upper case.

Column 5: (**Definition**): description of the data element, including any exceptions.

Column 6: (**Card type**): identifies the applicability of the data element. DL = driver license only; ID = non-driver identification card only; Both = both the driver license and the non-driver identification card.

Column 7: (**Field maximum length/type**): valid field length (i.e., the number of characters) for each data element. The following refer to the valid characters or image used (A=alpha A-Z, N=numeric 0-9, S=special, F=fixed length, V=variable length) in the related application.

Table 1 — Mandatory data elements

Data ref.	On card reference	Zone placement	Data element	Definition	Card type	Field maximum length/type
a.	1	Zone II	Family Name[1]	Family name (commonly called surname or last name), or primary identifier, of the individual that has been issued the driver license or identification document. If the individual has only one name, it will be placed in this data element.	Both	V40AS
b.	2	Zone II	Given names[1]	Given name or names (includes all of what are commonly referred to as first and middle names), or secondary identifier, of the individual that has been issued the driver license or identification document. If Suffix follows (see below), the Given Names and the Suffix must be separated by a comma and a space.	Both	V80AS

[1] Family name, given names, and suffix may be concatenated into a single element for placement on the card in Zone II. If a jurisdiction chooses this option, the element will consist of the family name followed by a comma and then the given names followed by any suffix. Such a concatenated name element will use the data element tag “Name”.

Data ref.	On card reference	Zone placement	Data element	Definition	Card type	Field maximum length/type
c		Zone II	Name suffix[1]	Name suffix of the individual that has been issued the driver license or identification document.	Both	V5AS
d.	3	Zone II	Date of birth **DOB**	Month, day, year (If unknown, approximate DOB). Format: MM/DD/CCYY	Both	F10NS
e.	4a	Zone II	Date of Issue **Iss**	Date DL/ID was issued. Format: MM/DD/CCYY	Both	F10NS
f.	4b	Zone II	Date of expiry **Exp**	Date DL/ID expires. Format: MM/DD/CCYY	Both	F10NS
g.	4d	Zone II	Customer identifier	The alphanumeric string assigned or calculated by the issuing authority.	Both	V25ANS
h.	5	Zone II	Document discriminator	Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.	Both	V25ANS
i.	6	Zone III	Portrait	A reproduction of the license holder's photograph. The portrait must be in color unless laser engraving card production is used.	Both	- (Image)

Data ref.	On card reference	Zone placement	Data element	Definition	Card type	Field maximum length/type
j.	7	Zone II / III	Signature	A reproduction of the license holder's signature. The signature may overlap the portrait image. If the signature does not overlap the portrait, it should remain in Zone II.	Both	- (Image)
k.	8	Zone II	Cardholder address[2]	The place where the cardholder resides and/or may be contacted (street/house number, municipality etc.). The issuing jurisdiction may choose to use either the mailing or physical address.	Both	V108ANS
l.	9	Zone II / Zone IV	Vehicle classifications / categories	Vehicle types the driver is authorized to operate.. Each vehicle classification / category denoted on the DL/ID must be described in Zone IV.	DL	V4ANS
m.	9a	Zone II / Zone IV	Endorsements **End**	Additional privileges granted to the cardholders, such as hazardous materials, passengers, doubles/triples trailers, motorcycle, chauffeur, emergency vehicles, and farm vehicles. Each endorsement denoted on the DL/ID must be described in Zone IV.	DL	V4ANS

[2] Address: Regardless of the type of address used for the production of the DL/ID, the issuing jurisdiction must store the driver's physical address as part of the customer record.

Data ref.	On card reference	Zone placement	Data element	Definition	Card type	Field maximum length/type
n.	12	Zone II / Zone IV	Restrictions / conditions / information codes	Codes used by the issuing jurisdiction to indicate restrictions or conditions that apply to the cardholder (shown as alphanumeric codes or pictographs). Other medical, administrative, or legal limitations applying to the cardholder are also to be displayed in this area. Restrictions or conditions denoted in Zone II must be described in Zone IV. If no restrictions or other conditions apply to the cardholder, "NONE" shall be indicated.	DL	V4ANS (Image)
o.	14	Zone II	Cardholder sex **Sex**	Cardholder's sex: M for male, F for female.	Both	F1A
p.	15	Zone II	Height **Hgt**	Inches (in): number of inches followed by " in" ex. 6'1" = " 73 in" Centimeters(cm): number of centimeters followed by " cm" ex. 181 centimeters="181 cm"	Both	F6AN
q.	16	Zone II	Weight **Wgt**	Indicates the approximate weight range of the cardholder: 0 = up to 31 kg (up to 70 lbs) 1 = 32 – 45 kg (71 – 100 lbs) 2 = 46 - 59 kg (101 – 130 lbs) 3 = 60 - 70 kg (131 – 160 lbs) 4 = 71 - 86 kg (161 – 190 lbs) 5 = 87 - 100 kg (191 – 220 lbs) 6 = 101 - 113 kg (221 – 250 lbs) 7 = 114 - 127 kg (251 – 280 lbs) 8 = 128 – 145 kg (281 – 320 lbs) 9 = 146+ kg (321+ lbs)	Both	F1N

Data ref.	On card reference	Zone placement	Data element	Definition	Card type	Field maximum length/type
r.	17	Zone II	Eye color **Eyes**	Blue, brown, black, hazel, green, gray, pink, dichromatic. If the issuing jurisdiction wishes to abbreviate colors, the three-character codes provided in ANSI D20 must be used.	Both	V12A
s.	20	-	Audit information	A string of letters and/or numbers that identifies when, where, and by whom a driver license/ID card was made.	Both	V25ANS
t.	-	Zone I	Issuing jurisdiction	The state, province, or territory responsible for the issuance of the DL/ID, and has the power to revoke or restrict the holder's driving and identification privileges. The appropriate two-character code in ANSI D20, Annex B, must be used.	Both	F2A

4.3 Optional data elements

Table 2 — Optional data elements

Data ref	On card reference	Zone placement	Data element/label	Definition	Card Type	Field Length/Type
a.	18	Zone II	Hair color **hair**	Brown, black, blonde, gray, red/auburn, sandy, white. If the issuing jurisdiction wishes to abbreviate colors, the three-character codes provided in ANSI D20 must be used.	Both	V12A
b.	19	Zone II	Place of birth	Country and municipality and/or state/province	Both	V33A

Data ref	On card reference	Zone placement	Data element/label	Definition	Card Type	Field Length/Type
c.	21	-	Inventory control number	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licenses and ID cards.	Both	V25ANS
d.	10	Zone II / Zone IV	Date of first issue per category [3]	The date of first issue for a specific class of vehicle if it is before the date of issue of the license document (same format as DOB). If this information is not available, indicate "**unavail. **"	DL	F10ANS
e.	11	Zone II / Zone IV	Separate expiry dates for vehicle classifications	If driving privilege for certain vehicle classifications expire before the base document, the date(s) must be noted on the document as indicated in Annex A. Format: MM/DD/CCYY	DL	F10NS

[3] Date of first issue per category is a mandatory data element for compliance with the ISO standard. Other countries require this information to be displayed on the license document to convey additional data about driving experience of the cardholder. It is generally understood that the jurisdictions of North America do not maintain this information and the data will generally be unavailable.

Annex A
(normative)

Card Design

A.1 Introduction

This annex contains the requirements with regard to the human readable content and layout of the data elements on DL/ID documents.

The main ideology for defining the design of the DL/ID is the minimum acceptable set of requirements to guarantee global interoperability. Sufficient freedom is afforded to the issuing authorities of driver licenses to meet their national (domestic) needs (existing standards, data contents, security elements, etc).

A.2 Scope

Annex A defines the specifications of the card layout, together with informative examples for ease of understanding.

A.3 Dimensions and character set

The dimensions of the DL/ID shall be in conformance with ISO/IEC7810 ID-1.

All mandatory human readable data elements shall be printed in ANS characters, i.e. the extended Latin character set, including characters such as ß, ä, ã, ç, è, é, ö and ü.

A.4 Definitions

The basis of the visual card design is to meet the minimum common mandatory set of data elements in the following areas of function:

- Common recognition of the DL/ID document by law enforcement agencies and users outside of the jurisdiction of issue.
- Layout of the human readable data elements and the machine-readable components.
- Text and or pictographs of the human readable data elements.
- Security of the card as a separate topic to avoid confusion between common recognition and integrity issues.

A.5 Common recognition

To assist law enforcement agencies in recognizing a driver license presented by a driver outside the country of issue as an DL/ID, the following shall appear on the card:

- The common security element, as prescribed by AAMVA, shall be included in Zone 4 of the card.

- For driver license documents, the background color of Zone 1 of the card shall be predominantly pink and the color of the background, which may be a printed image, shall be matched as closely as possible to a 30% tint of Pantone reference 198. This is a specific requirement of ISO/IEC CD 18013-1 for ISO compliant driver licenses.

- For non-driver license identification card documents, the background color of Zone 1 of the card shall be predominantly green and the color of the background, which may be a printed image, shall be matched as closely as possible to a 30% tint of Pantone reference 368.

- The reproduction of the portrait of the holder of the license is depicted on the left side on the portrait side of the card as shown by the position of Zone III in figure A.2 and A.3.

A.6 Layout

Flexibility is built into the specification to accommodate the needs of the many issuing jurisdictions. There are two principle formats – vertical and horizontal. Within both of these formats, zones divide the layout and options for the zones are delineated in this Annex. Zone placement will vary between the two formats for the portrait side of the cards. The non-portrait sides will be consistent between the two formats.

The portrait and non-portrait side of the vertical and horizontal cards shall carry the following:

Portrait side

Data Element Set of text, digitally printed reproduction of portrait and signature.

Zones I, II and III.

Non-portrait side

Data Element Set of text (optional) and machine-readable technologies.

Zones IV and V.

A.7 Contents of the zones

A.7.1 General

This section addresses the placement of data elements in various zones on the card. In some cases, it is mandatory that a data element be placed in the given zone. In other cases, the placement of a data element may be optional for the given zone. The issue of the mandatory or optional *placement* of data elements is different than the issue of whether the data element is required to appear on the card at all. For example, the use of a data element, e.g., date of expiry of each vehicle category, may be optional, but if it is used it is mandatory to place it in the given zone.

A.7.2 Zone I

A.7.2.1 Document type indicator

For driver licenses, the words “DRIVING LICENSE” in English must be included as text or, alternatively, the words "DRIVING LICENSE" may be incorporated in the background graphic design of Zone I. The words may also be repeated in French or Spanish. NOTE: “The term “driving license” is use for compatibility with the ISO draft standard.

Other types of driving licenses may be indicated in the same manner, such as commercial driving licenses and instruction/learning permits.

For non-driving identification cards, the words "IDENTIFICATION CARD" must be included as text or, alternatively, the words "IDENTIFICATION CARD" may be incorporated in the background graphic design of Zone I.

A.7.2.2 Issuing jurisdiction information

The name of the issuing jurisdiction must be included as text.

The distinguishing sign of the issuing country, as prescribed below, must be included in Zone I:

U.S. jurisdictions shall use: **USA**

Canadian jurisdictions shall use: **CDN**

A full list of issuing country codes may be obtained from ISO/IEC 18013-1, Annex F (*Distinguishing Signs of Countries*).

The full name of the issuing country may also be included, as well as other images, such as the flag or logo of the issuing country and/or jurisdiction.

A.7.3 Zone II

Zone II contains the following data elements:

- Family name (or concatenated Name)
- Given name(s) (or concatenated Name)
- Suffix
- Date of birth
- Date of issue
- Date of expiry
- Customer number
- Document discriminator
- Signature (unless in Zone III)
- Cardholder address

- Vehicle classifications (if codes are used, they should be explained in Zone IV; overflow information may be placed in Zone IV)
- Vehicle restrictions and endorsements (if codes are used, they should be explained in Zone IV; overflow information may be placed in Zone IV)
- Cardholder sex
- Cardholder height
- Cardholder weight
- Cardholder eye color
- Audit information
- Issuing jurisdiction
- Cardholder signature (may be in Zone III instead)
- Cardholder hair color (optional)
- Cardholder place of birth (optional)
- Date of expiry per vehicle classification / category (optional – may be in Zone IV instead)
- Date of issue per vehicle classification / category (optional – may be in Zone IV instead)
- Date of first issue per vehicle classification / category (optional – may be in Zone IV instead)

Other data fields for national or jurisdictional purposes in human readable format (optional).

A.7.4 Zone III

Zone III contains the following:

- Portrait
- Signature (May be in Zone II instead)

A.7.5 Zone IV

Zone IV contains the following:

- Common security device
- Explanations of codes used in Zone II categories, restrictions, and/or endorsements
- Overflow from categories, restrictions, and/or endorsements in Zone II
- Date of expiry of each vehicle category (if used)
- Date of first issue of each vehicle category (if used)

Jurisdiction-specific information in human-readable format for purposes of administration of the license or related to road safety may also be included in this zone.

A.7.6 Zone V

The PDF417 2-dimensional bar code must be included in Zone V. Other optional machine-readable technologies may co-exist with the PDF417 2-dimensional bar code in Zone V. This specification contains requirements for PDF417 2-dimensional bar codes, 3-track magnetic stripes, and optical memory cards. No other machine-readable technologies, including IC chips, are supported in this specification. Issuing jurisdictions wishing to implement other non-proprietary technologies, such as integrated circuit cards (also known as "smart cards"), are

asked to work with AAMVA prior to implementation, so that future iterations of this specification will properly include these technologies to insure future interoperability with other jurisdictions.

The positions of the zones for the optional jurisdiction-specific human readable fields and optional machine-readable technologies are presented in figures A.4 and A.5 of the annex. The position and size of Zones IV and V may be adjusted in accordance with the machine readable technologies incorporated on the card.

A.7.7 Reproduction of images

A.7.7.1 Portrait

Measures shall be taken by the issuing authority to ensure that the digitally printed reproduction of the portrait of the holder on the card is resistant to forgery and substitution. The portrait shall meet the following requirements:

Pose. The portrait shall depict the face of the rightful holder of the card in a full-face frontal pose with both eyes visible; i.e. captured perpendicular to an imaginary plane formed parallel to the front surface of the face. The portrait may only show the holder with headgear, if the holder is a member of a religion requiring the wearing thereof and provided that the headgear does not render the portrait inadequate for the identification of the holder. Jurisdictions that incorporate facial recognition biometric technology may wish to insure eyeglasses are removed as well, to aid in consistent identification of the cardholder.

Depth of Field. The full-face frontal pose shall be in-focus from the crown (top of the hair) to the chin and from the nose to the ears.

*Orientatio*n. The crown (top of the hair) shall be nearest the top edge of Zone III as defined in figure A.2 and A.3; i.e. the crown to chin orientation covering the longest dimension defined for Zone III.

Face Size. The crown to chin portion of the full-face frontal pose shall be 70 to 80 percent of the longest dimension defined for Zone III, maintaining the aspect ratio between the crown-to-chin and ear-to-ear details of the face of the holder.

*Lightin*g. Adequate and uniform illumination shall be used to capture the full-face frontal pose; i.e. appropriate illumination techniques shall be employed and illumination used to achieve natural skin tones (and avoid any color cast) and a high level of detail, and minimize shadows, hot spots and reflections (such as sometimes caused by spectacles).

*Backgroun*d. A uniform light blue color background shall be used to provide a contrast to the face and hair.

Centering. The full-face frontal pose shall be centered within Zone III.

*Borde*r. A border or frame shall not be used to outline the digitally printed reproduction of the portrait.

Color. The digitally printed reproduction of the portrait shall be a true color representation of the holder, unless laser engraving is used to produce the DL/ID document. If laser engraving is used, a true color representation of the cardholder must be stored by the issuing jurisdiction with the cardholder's record.

Printing resolution. The digitally printed reproduction shall yield an accurate recognizable representation of the rightful holder of the license. The quality of a digitally reproduced portrait shall be visually comparable to an

acceptable photograph. To achieve this comparable quality in a digital reproduction, care must be given to the image capture, processing, digitization, compression and printing technology and the process used to reproduce the portrait on the card, including the final preparation of the DL/ID.

A.7.7.2 Signature

The signature of the holder shall be a digitally printed reproduction of an original. Measures shall be taken by the issuing authority to ensure that the digitally printed reproduction of the signature is resistant to forgery and substitution. The signature displayed shall meet the following requirements:

Orientation. The digitally printed reproduction of the signature shall be displayed in either Zone II or Zone III with its A-dimension parallel to the Top Reference Edge of the horizontal format cards identified in figure A.2. In the case of vertical format cards, the A-dimension will be perpendicular to the top reference edge. (See figure A.2.1 for an example of the horizontal format and figure A.3.1 for an example of the vertical format..)

Figure A.1

Size. The signature displayed shall be of such dimensions as to be discernible by the human eye and maintain the aspect ratio (A-dimension to B-dimension) of the original signature.

Scaling. In the event the signature displayed is scaled-up or scaled-down, the aspect ratio (A-dimension to B-dimension) of the original signature shall be maintained. In the case of a scaled-down image, the image shall not be smaller than 50% of the original signature.

Cropping. The issuing authority should take steps to eliminate or minimize cropping.

Color. The digital reproduction of the signature shall be printed in black to afford a definite contrast to the background.

*Border*s. Borders or frames shall not be permitted or used to outline the digitally printed reproduction of the signature.

Printing resolution. The digitally printed reproduction shall yield an accurate recognizable representation of the signature of the rightful holder of the license. To achieve this comparable quality in a digital reproduction, care must be given to the image capture, processing, digitization, compression and printing technology and the process used to reproduce the signature on the card, including the final preparation of the DL/ID.

A.8 Security

Aspects such as a specific background pattern, rainbow printing, holograms and special inks relate to the minimum security requirements of the card and should not be confused with common recognition of the DL/ID. The security requirements are addressed in Annex B.

Figure A.2: Portrait side of Horizontal DL/ID (not to scale)

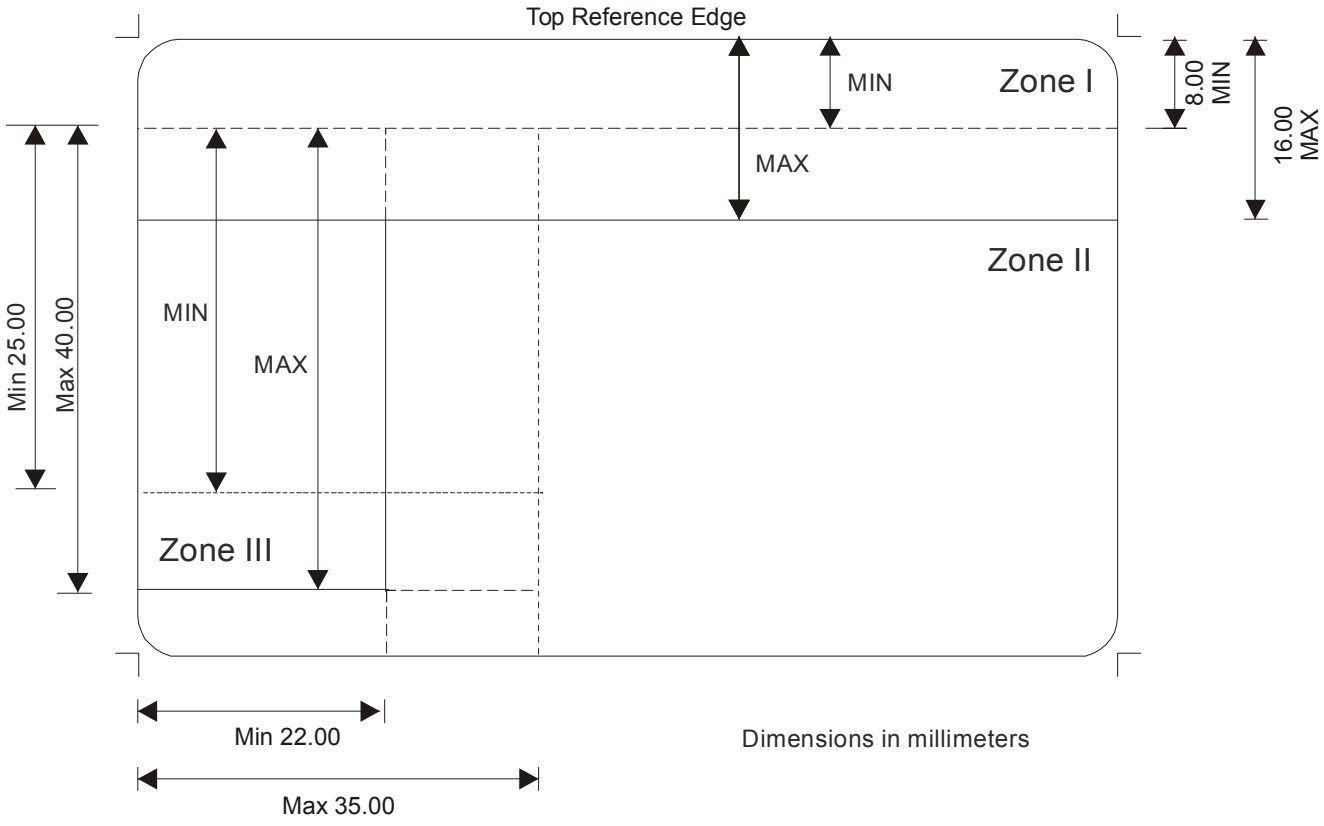


Figure A.2.1: Horizontal DL/ID - Informative Example (not to scale)

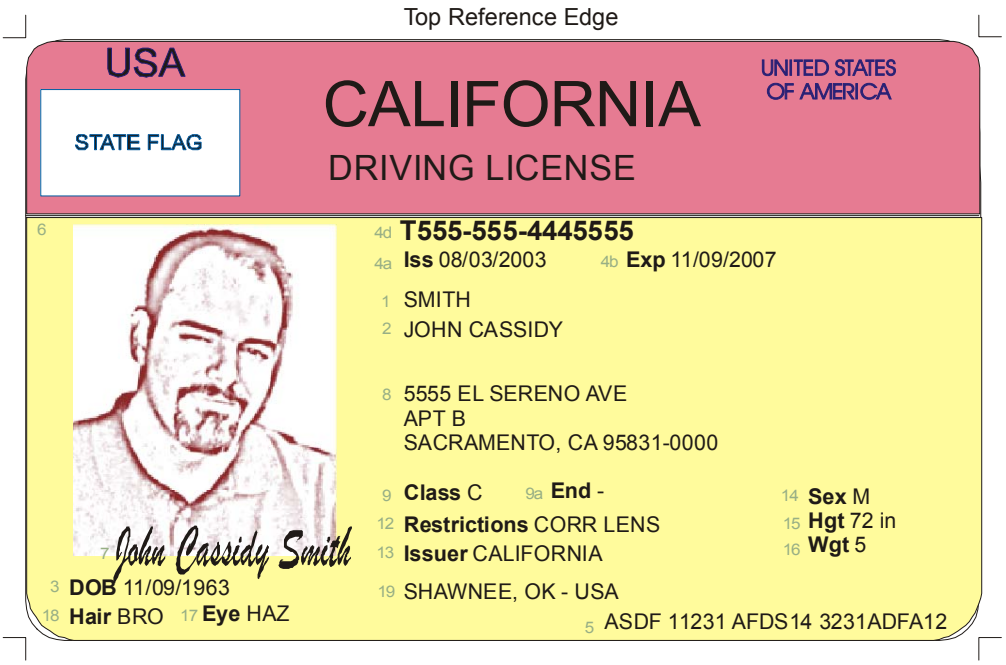


Figure A.3: Portrait side of Vertical DL/ID (not to scale)

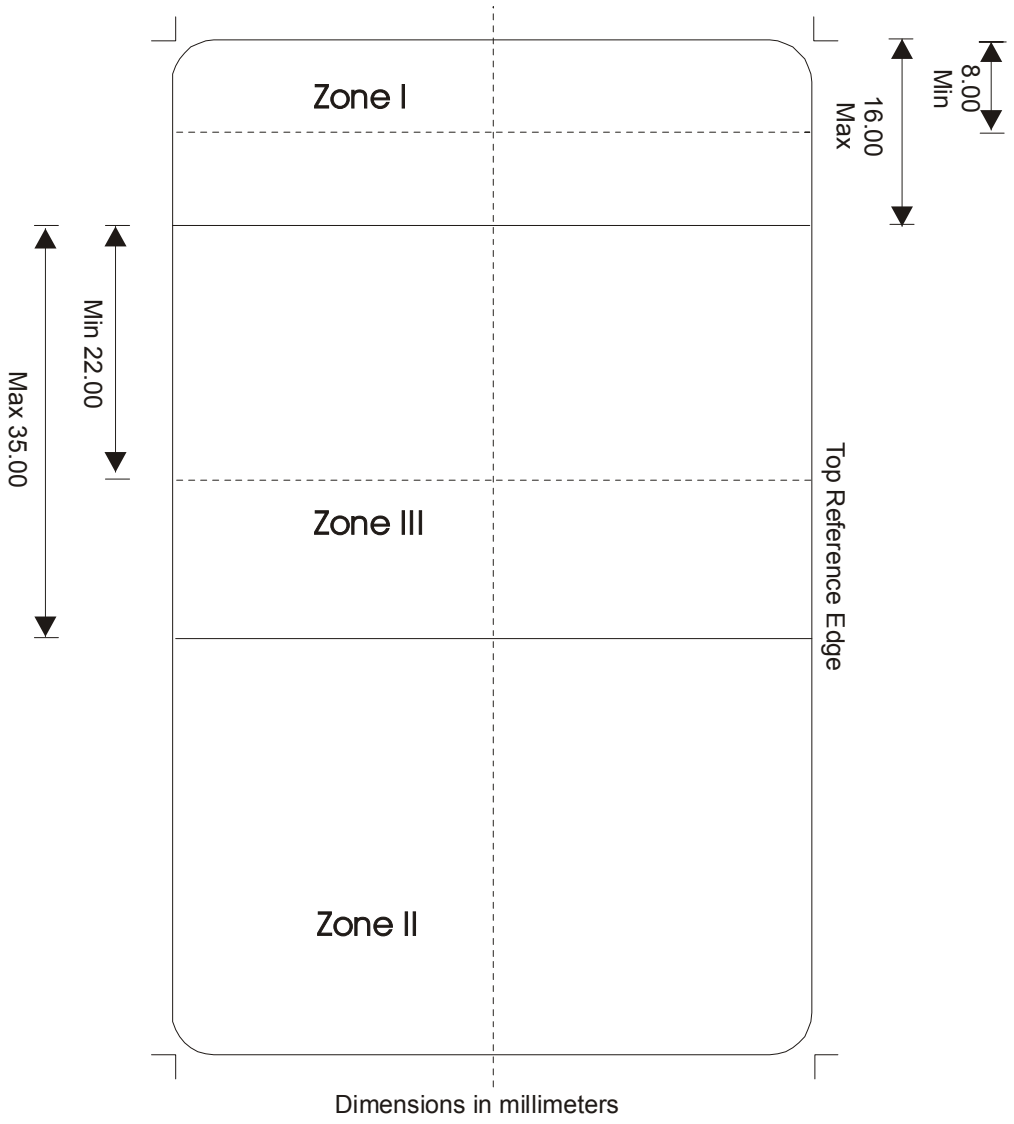
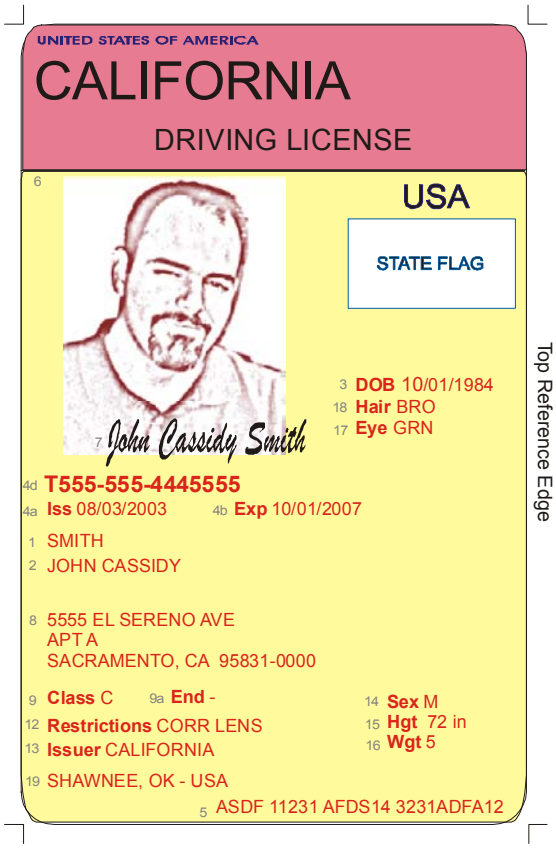


Figure A.3.1: Vertical DL/ID - Informative Example (not to scale)



Dimensions in millimeters

Figure A.4: Non-portrait side of Horizontal and Vertical DL/ID

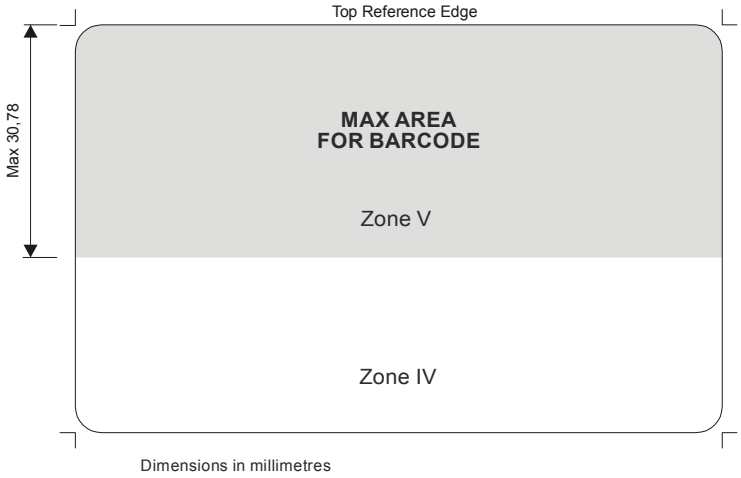
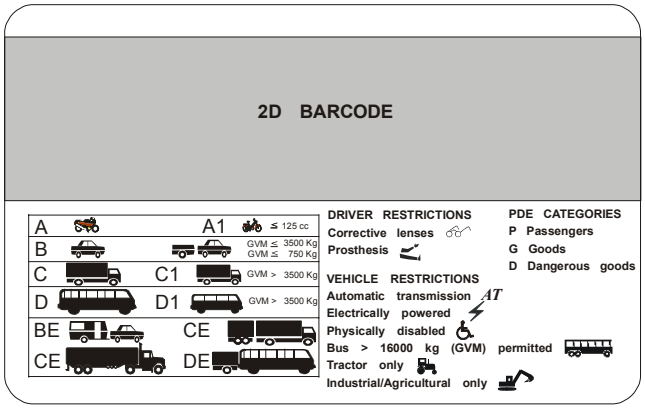
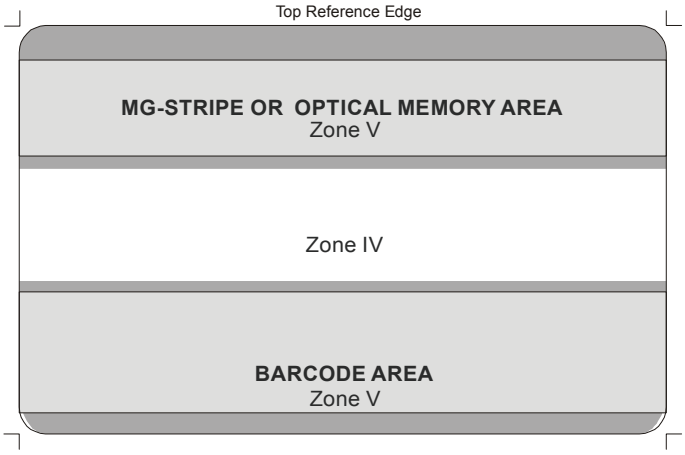


Figure A.4.1: Informative Example



Note: Pictographs / icons used in this informative example are samples taken from the ISO/IEC standard for ISO compliant driving licenses (ISO/IEC 18013-1). Jurisdictions may wish to consider the use of icons to convey driving privileges, endorsements, and restrictions.

Figure A.5: Non-portrait side of Horizontal and Vertical DL/ID – magnetic stripe and bar code



Annex B
(normative)

Physical Security

B.1 Scope

This normative annex specifies the security requirements for AAMVA compliant DL/IDs. The purpose is to discourage forgery, counterfeiting and other fraud related to the misuse of DL/IDs used as identity documents and to establish an adequate level of confidence in the authentication of genuine documents and the detection of fraudulent ones. This normative annex also specifies some minimum requirements for the materials used in the card, and the security printing and copy protection techniques to be employed, including personalization and the protection of the biographical data in the cards.

B.2 Introduction

The growth in international crime and identity fraud have led to increasing concerns over the security of driving licenses as well as all other kinds of personal identification documents and what may be done to help improve their resistance to attack or misuse. The DL/ID is one of the most commonly used, and most commonly counterfeited, forms of identification in North America.

This annex draws heavily upon ISO IEC CD 18013-1, Annex C. This approach recognizes that a feature or technique that may be necessary to protect one Issuer's cards may be superfluous or of minor importance to another Issuer using different production systems and vice versa. A targeted approach that allows issuing authorities flexibility to choose from different card technologies (pure plastic cards or combined structures incorporating other materials in the core of the card-body) and a combination of security features and/or techniques most appropriate to their particular needs is therefore preferred to a "one size fits all" philosophy. However, to help ensure that a balanced set of security features and/or techniques is chosen, it is first necessary for each issuing authority to conduct a risk assessment and select optional features and/or techniques that are appropriate to the particular issuing environment and to meeting any specific security concerns. All this must serve the objective of facilitating the task of card verification as easy as possible under all practical circumstances.

The aim of this annex is to establish a security baseline. Nothing within these recommendations shall prevent or hinder issuing authorities from implementing additional security features beyond the minimum features and techniques required in this annex.

B.3 Definitions

The glossary of terms in this card is included to assist the reader with understanding the general meanings of such terms within the context of this card. This glossary is not intended to be authoritative or definitive.

Biographical data (biodata): The personalized details of the holder of the card.

Card core: The opaque or translucent inner layers of a laminated card upon which the security design is usually printed

Counterfeit from cannibalized cards. Creation of a fraudulent document using card components from legitimate DL/ID cards.

*Card blank*s: A card that does not contain the biographical data and other personalized details of a cardholder.

CMYK colors: The 'process' colors, cyan, magenta, yellow and black used in combination in commercial color printing, normally in the form of half-tone images, and by digital printing devices to approximately represent the visible color spectrum and enable the printing of 'color pictures'.

Forgery: Fraudulent alteration of any part of the genuine card e.g. changes to the biographical data or the portrait.

Impersonators: People who resemble the rightful cardholder (naturally or otherwise) who then masquerade using the stolen identity.

Impostors: people who prove they are someone who they are not by using fraudulent documents and other techniques to obtain a bona fide DL/ID card.

*Laser engravin*g: A process whereby images (usually personalized images) are created by 'burning' them into the card-body material with a laser. The images may consist of text, portraits and other security features

Level 1: synonymous with "first line inspection"

Level 2: synonymous with "second line inspection"

Level 3: synonymous with "third line inspection"

Optically variable feature (OVF): An image or feature whose appearance in color and/or design changes dependent upon the angle of viewing or illumination. Examples are: features including diffraction structures with high resolution (Diffractive Optically Variable Image Devices/DOVID's), holograms, color shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.

*Personalizatio*n: The process by which the portrait, signature and biographical data are applied to the card.

*Photo-substitutio*n: A type of forgery in which the portrait on a card is substituted for a different one after the card has been issued.

Tactile feature: A surface feature giving a distinctive 'feel' to the card.

Security element: A distinct physical element or property of a document that contributes to at least one security feature. Depending on the method of verification, a single element may provide one or more security features which may apply to the same or to different categories of protection.

Security feature: A feature of a document that is linked to a specific method of verification and thus helps insure the document's integrity and/or authenticity as a properly issued document that has not been tampered with. Security features may be distinguished in different kinds of categories such as:
- for human or machine verification,
- for first line, second line, or third line inspection,
- substance features, structure features, or data features according to ICAO doc. 9303.
Security elements applied during production of a document may contribute more than one feature and therefore also cover more than one category of each kind.

Theft of card components: Theft of genuine card blanks or card components to be used with a card printer / personalization system to create counterfeit DL/ID cards.

B.4 Basic Principles

B.4.1 Card Production

Production of IDL cards, including the personalization processes, should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. Centralized card production and personalization is recommended wherever possible. If the personalization process is decentralized, or if personalization is carried out in a location geographically separated from where any card blanks are made, appropriate precautions should be taken when transporting the blank cards and any associated security materials to safeguard their security in transit.

B.4.2 Accountability and auditing

There should be full accountability over all the security materials used in the production of good and spoiled cards and a full reconciliation at each stage of the production process with records maintained to account for all material usage. The audit trail should be to a sufficient level of detail to account for every unit of material used in the production and should be independently audited by persons who are not directly involved in the production. Certified records should be kept of the destruction of all security waste material and spoiled cards.

Materials used in the production of the cards should be of controlled varieties and obtained only from bona fide security materials suppliers. Materials whose use is restricted to high security applications should be used within the card construction and materials that are available to the public on the open market should be avoided.

B.4.3 Graphics design

Sole dependence upon the use of publicly available graphics design software packages for originating the security backgrounds should be avoided. (Such software packages may however be used in conjunction with specialist security design software.)

B.4.4 Security over time

The combination of security features, materials and techniques must be well chosen to ensure full compatibility and protection for the lifetime of the card.

B.4.5 Covert features

Although this annex deals mainly with security features that help officials to detect counterfeiting and fraudulent alteration of cards, there is another class of security features that are covert (secret) features, designed to be authenticated either by forensic examination or by specialist verification equipment. It is evident that knowledge of the precise substance and structure of such features must be restricted to very few people on a "need to know" basis. The purpose of these features is to enable authentication of cards where unequivocal proof of authenticity is a requirement (e.g. in a Court of Law). DL/ID cards shall contain at least one covert level 3 security feature. The feature must have absolute consistency of characteristics, be difficult to discover, be invisible to the human eye, and require special equipment and training not commonly available in order to discover. The issuing jurisdiction must insure that information about the covert feature is not made part of public record. Information about the covert feature should be known to the absolute minimum number of people, but should be shared with law enforcement laboratories that are accredited by the American Society of Crime Laboratory Directors (ASCLD) and/or ISO 9000.

B.4.6 Common security element

All compliant DL/ID documents must include the common security element prescribed by AAMVA in Zone 4 of the card (see Annex A, paragraph A.5). Although the common security element contains advanced security features, it should not be considered as helping fulfill the requirements of this annex. The common recognition feature, while being highly resistant to counterfeit, will be the primary focus of fraudsters. Its primary goal is to establish an easily recognizable common security feature, similar to the concept introduced for major credit cards, to aid in the recognition of DL/ID documents. Additional security features are needed to fully protect the card from counterfeit and alteration.

B.5 Risk Assessment

Each issuing jurisdiction should conduct a risk assessment of their own DL/ID documents to determine how and to what extent the threats of counterfeit/simulation, counterfeit from cannibalized cards, alteration, photo/signature substitution, theft of card components, and impersonators / impostors pertain to their documents. Jurisdictions must also determine whether their cards are at risk to some threats more than others, or if there are additional threats unique to their region. The constantly changing nature of counterfeiting requires continued vigilance and periodic risk assessments. It is recommended that risk assessments be performed by third parties not affiliated with the issuing jurisdiction's primary contractor.

B.6 General Requirements

This specification provides minimum guidelines for that compliant DL/ID documents must adhere to for protection against a variety of common threats to their fraudulent use. In general, jurisdictions should insure that their selected security devices:

- Do not conflict with each other and should be planned for maximum effectiveness.

- Do not interfere with the operation of machine-readable technology(ies) on the document.
- Are layered in order to benefit from the combined protection of multiple features and leverage the card production process.

Jurisdictions may benefit from a non-biased third party verification of the compatibility of the selected security devices and the manner in which they intend to integrate them into the DL/ID document.

B.7 Use of the *DL/ID Security Device Index*

Annex C contains the *DL/ID Security Device Index*. This index is to be used as a guideline for security feature selection. The index is an inclusive list of security devices that includes a general description of the device and a guideline for determining what threats each device protects against at levels 1 and 2. The *DL/ID Security Device Index* will assist issuing jurisdictions to make educated decisions about the security design of their DL/ID document system.

The properties of the security devices identified in Annex C should be considered generally and as a beginning of discussion. Security device vendors may offer new approaches to established security devices that provide protection above and beyond those listed in Annex C. Security devices may be combined and implemented in a manner that offers protection against more threats than when the devices are considered individually. The DL/ID Security Device Index indicates coverage against various threat types at different levels of inspection (level 1 and level 2). The levels of inspection and threat types are as follows:

B.7.1.1 Level 1: first line inspection

Examination without tools or aids that involves easily identifiable visual or tactile features for rapid inspection at point of usage.

B.7.1.2 Level 2: second line inspection

Examination requires the use of a tool or instrument (e.g., UV light, magnifying glass, or scanner) to discern .

B.7.1.3 Type 1: Counterfeit / simulation

An unauthorized copy or reproduction of a genuine security card made by whatever means

B.7.1.4 Type 2: Alteration

Deletion, modification, masking, tampering with biographical data concerning the original or rightful cardholder.

B.7.1.5 Type 3: Photo / signature substitution

Substitution of an impostor's photograph and/or signature in place of the photograph / signature of the original or rightful cardholder.

B.7.1.6 Type 4: Counterfeit from cannibalized cards

Creation of a fraudulent document using card components from legitimate DL/ID cards.

B.7.2 Minimum requirements

Each DL/ID document must have a minimum of four security features. Physical security devices must cover all threat types, as defined above, at level 1, and all threat types at level 2. The four features may be unevenly split between levels 1 and 2.

The minimum features mandated elsewhere in the card design specifications (the common security feature, document discriminator, 2D bar code, etc.) may not contribute toward the minimum four devices and threat type coverage.

Annex C
(informative)

DL/ID Security Device Index

C.1 Introduction

The security device index was developed by AAMVA as a tool to aid in the security design of DL/ID documents and to insure full coverage of common threats to document integrity in North America. The index is designed to be inclusive of security devices available for DL/ID documents. The terms used in the index are written to the extent possible in generic terms rather than using trademarked names. Suggestions for updates should be sent to AAMVA's Standards Program for inclusion in subsequent iterations of this specification.

C.2 Threat Levels

Level 1 - A Level 1 security device supports first line inspection.

Level 2 – A Level 2 security device supports second line inspection.

C.3 Threat Types

Type 1 – Counterfeit/Simulation

Type 2 – Alteration

Type 3 – Photo Substitution

Type 4 – Cannibalization

(Refer to Annex B, section 7.1 for definitions of these terms.)

C.4 Printing

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
a. Deliberate Errors/known flaws A feature is purposely made with an intentional mistake known only to the manufacturer or inspection officials.						X			
b. Duplex Patterns A design made up of an interlocking pattern of small irregular shapes, printed in two colors and requiring very close register printing in order to preserve the integrity of the image.		X	X		X	X	X		
c. Fine line background (Guilloche pattern)		X	X	X	X	X	X	X	X

PHYSICAL SECURITY FEATURE / Threat Type	LEVEL 1				LEVEL 2			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**
A pattern of continuously fine lines constructed by using two or more lines in overlapping bands that repeat a lacy, web-like curve.								
d. Fine line foreground A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve.	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
e. Front to back (see through) register A design printed on both sides of a card that forms an interlocking image when held to a light source.	**x**							
f. Ghost Image Half tone reproduction of the original image that is typically printed in the same area as, and behind, personal data.		**x**	**x**	**x**	**x**			**x**
g. Layered printing (on lamination) Printing separate elements of the secure design on different layers of the laminated card body materials so that no single layer contains all of the security features and the entire products is only apparent after lamination.	**x**	**x**		**x**				
h. Micro optical imaging Text, line art, gray scale images and multi—reflectivity images are engineered into optical WORM media at high resolution (over 12,000 dpi). Difficult to simulate the printing resolution.	**x**	**x**			**x**	**x**	**x**	
i. Microprinting / nanoprinting Miniature lettering which is discernible under magnification. Incorporated into fine line backgrounds or placed to appear as bold lines. Continues to decrease in size as technology improves. Difficult to duplicate.					**x**			**x**
j. Moiré pattern (anti-scan/VOID pattern) A new pattern formed by the super positioning of two patterns who periodicities are not identical. Security designs can be developed so that a scanner or copier will only display part of the pattern and/or word VOID or COPY appears instead of the pattern.					**x**	**x**	**x**	**x**

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
k. Non standard type fonts Special type that is not available on the commercial market and is reserved for security card use only.	x	x			x	x		
l. Rainbow printing A subtle shift of color across a document. Accurately designed patterns cannot be easily copied. It is often used with a fine line or medallion pattern in the background of a card.	x							
m. Security code High-resolution color printing systems print a security code within the body of the color printed photo image. The code can be printed in a non-proportional font that can imbed characters on the edge or bottom of the printed picture.					x			

C.5 Inks

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Chemically Reactive Contains a security agent that is sensitive to chemicals, i.e., polar and non-polar solvents and bleach, commonly used to alter documents. The chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.		x				x		
b. Infrared fluorescent Forms a visible image when illuminated with light in the infrared / red visible part of the spectrum.					x	x		
c. Infrared drop-out Forms a visible image when illuminated with light in the visible part of the spectrum, but cannot be detected in the infrared region.					x	x		
d. Metallic, pearlescent, and iridescent Inks that fluctuate in brilliance depending on the angle of illumination of	x	x	x					

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
the viewing. Difficult to mimic the luster and hard to copy or scan.								
e. Metameric The use of a pair of ink colors that differ in spectral composition but match one another under certain lighting conditions. Under incandescent light that may appear the same, but under colored light they appear as different colors.					x			
f. Optically variable (color shifting) This overt security ink can be printed as a semi-transparent or opaque color shifting security feature. Advanced multi-layer light interference structures create noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc	x	x						
g. Phosphorescent Contains a pigment that glows when exposed to a light source of appropriate wavelength. The reactive glow decays after the light source is removed.					x	x		
h. Tagged Contains taggants or compounds that are not naturally occurring and that can be detected using special equipment that reacts to electromagnetic energy identifying the grouping or type.					x			
i. Thermochromatic Ink that exhibits a sharp, reversible color change when exposed to heat, i.e., finger rubbing or hot air.	x				x	x		
j. Ultraviolet fluorescence Invisible inks that emit visible color under exposure to ultraviolet light. Colors can be formulated that are not commercially available, making resistance to counterfeiting higher.					x	x	x	x

C.6 Substrate Inclusion

PHYSICAL SECURITY FEATURE	LEVEL 1	LEVEL 2

	Threat Type	1	2	3	4	1	2	3	4
a. Core inclusion The manufacture of card stock with different layers. A colored core material may be placed inside to create a colored edge along the card.		x							
b. Embedded thread, fiber or planchette Small, often fluorescent particles or platelets incorporated into a card material at the time of manufacture that can be seen later under certain lighting conditions. The embedded elements may have magnetic or other machine-readable properties that may be used to enhance the levels of security provided.						x	x		
c. Opacity mark Similar to a watermark, it is a plastic that contains a unique translucent mark.		x							
d. Security bonding The card periphery incorporates a security bonding material that bonds all of the layers together. Tamper evidence is seen if access is attempted to obtain the internal structures of the card.						x	x		x
e. Ultraviolet features Card bodies are made UV dull or possess a controlled response to UV light so they exhibit fluorescence that can be distinguished in color from the “blue” used in commonly available fluorescent materials.						x	x		

C.7 Optically Variable Devices (OVD)

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
a. De-Metalized OVD A combination of metal and transparency on the same foil or laminate. Hi resolution OVD has selective de-metallization, either transparent or opaque, as defined above.		x	x	x		x		x	x
b. Non-transparent OVD Printed opaque, OVD's advanced multilayer light interference structures		x				x		x	

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
create noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc. similar to what is seen on many global identification documents including driver licenses, banknotes, passports, and visas. The color shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications.								
c. Personalized OVD OVD that is personalized for each card based upon biographical data, portrait, or signature of the card holder.	x	x	x	x	x	x	x	x
d. Transparent OVD Printed on transparent lamination overlay material, advanced multilayer light interference structures create noticeable, reflecting color shifts, i.e., gold to green, green to blue, etc. When incorporated into a driver license design, feature will not interfere with photo or data information. Transparent OVD color shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications, i.e., driver licenses, passports, visas, etc. The OVDs are digitally mastered and created using computer-guided lasers or electron beams.	x	x	x	x	x	x	x	x

C.8 Additional Features

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Biometric feature (template) A biometric template of the customer's physical characteristics.					x	x	x	x
b. Covert variable pixel manipulation Covert dot matrix images that are converted to visible text with a special reader or lens.					x	x	x	x
c. Digital Seal A method of securing and validating data by electronic means using					x	x		x

PHYSICAL SECURITY FEATURE / Threat Type	LEVEL 1				LEVEL 2			
	1	2	3	4	1	2	3	4
digital signature technology. The issuing authority "signs" the information contained in the MRT .								
d. Embedded Image (e.g., digital watermark) An image or information that is embedded or encoded within a primary visual image.					x	x	x	x
e. Laminates (security) Transparent layers or films with an integrated security feature(s) are applied to the card with an adhesive or fused by heat. Available in a number of forms, security laminates are designed to be tamper evident and carry other security features to the card.	x	x	x	x				
f. Laser encoded optical image Image and text files are placed to an optical WORM media as a visible diffraction pattern image that is eye-readable under a variety of lighting conditions.	x	x	x					
g. Laser engraving The information cannot be mechanically or chemically removed without surface damage to the card. Can be used for photos, characters, bar codes, OCR, etc.	x	x	x			x		
h. Laser perforation Holes are made with the laser beam of images or objects. The image is visible when held up to a light source. It has a tactile feel with conical holes that are larger at the entrance than exit.	x	x	x	x				
i. Machine readable technology (MRT) Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc. Verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other information.					x	x	x	x
j. Magnetic media fingerprinting Tracks unique, random patterns of magnetic media formed as a by-product manufacture of card. The pattern is recorded at the time the					x	x		x

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
cad is encoded and this pattern can later be compared to the pattern detected when the card is scanned.								
k. Optical media fingerprinting Tracks unique, random patterns of optic media (e.g., fibers) on card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.					x	x	x	x
l. Optical watermark Fine line images that are engineered into optical WORM medial with a very high resolution (12,000 dpi). The watermark is overwritten with a laser-encoded optical image, locking together a preformatted document security feature with a laser encoded personalization security feature.	x	x			x	x		x
m. Overlay An ultra-thin film or protective coating that may be applied to the surfaced of a card in place of a security laminate and which may contain optically variable features.	x	x	x	x				
n. Overlapping data Variable data, such as digitized signature, seals or text can be placed over another field such as a photo image. Both fields must be altered if a substitution is to take place making it more difficult.		x	x	x	x	x	x	x
o. Redundant data Display of data in more than one location on the card. A visual inspection may determine if all of the fields match. Usually, the data is displayed in a variety of colors and forts to further deter alteration.		x						
p. Retroreflective device Optical constructions that reflect light such that covert logos become visible over the entire document when viewed using a focused light source or retroreflective viewer. Level 1 capability is based on a distinctive tactile quality.	x	x	x	x	x	x	x	x

PHYSICAL SECURITY FEATURE	Threat Type	LEVEL 1				LEVEL 2			
		1	2	3	4	1	2	3	4
q. Security threads Metal or plastic, these threads are seen on currency. With special metallized film, demetallized text is invisible in reflected light and therefore is difficult to copy. When viewed in transmitted light, the opaque aluminum letters are clearly visible.		x	x	x		x	x	x	x
r. Thin film interference filters Multiple layer structures that produced color effects by interference.						x			
s. Tactile feature A feature which is apparent to touch or feel without requiring a special instrument. This could include texture, flexibility, or weight of the document and/or a feature incorporated in the card structure or card components.		x	x						

Annex D
(normative)

Mandatory PDF417 Bar Code

D.1 Scope

This annex defines mapping of the driving license/identification (DL/ID) card machine-readable information elements onto a two dimensional bar code. This annex expands upon, corrects minor errors in, and intends to supersede the requirements of AAMVA DL/ID-2000 Annex E – *Mapping of driving license/identification card information to 2 dimensional bar codes* (June 6, 2000).

D.2 Functional requirements

The primary function of the driver license document is to provide evidence of driving privileges and restrictions. The remaining functions of the DL/ID documents are to aid in: identity and age verification, automation of administrative processing, and address verification. The mandatory and optional data elements defined in this annex, and the mapping of the elements to the machine-readable technology, flow from these functional requirements. This specification primarily seeks to support the needs of the law enforcement community and their interaction with DL/ID documents.

All mandatory and optional data must be unencrypted. Issuing jurisdictions may encrypt jurisdiction-specific data in a separate subfile or within a different storage media.

D.3 Mandatory machine-readable technology – PDF417

The PDF417 two dimensional bar code symbology is the minimum mandatory machine-readable technology that must be present on compliant DL/ID documents.

D.4 Optional machine-readable technologies

This specification does not preclude a jurisdiction from integrating additional machine-readable technologies into the DL/ID documents as long as they are compatible with the minimum mandatory requirements of this specification.

D.5 Technical requirements for PDF417

D.5.1 Conformance

A prerequisite for conformance with this standard for bar coding is conformance with ANSI X3.182, ANSI/ASQC Z1.4, ASCII/ISO 646, ASCII/ISO 8859-1, ISO/IEC 15438, and MIL-L-61002.

D.5.2 Symbology

The PDF417 symbology (see ISO/IEC 15438 *Automatic Identification and Data Capture Techniques - International Two-dimensional Symbology Specification - PDF417*) shall be used for the Drivers License applications.

The following PDF417 symbology variants as defined in the ISO/IEC 15438 *Automatic Identification and Data Capture Techniques - International Two-dimensional Symbology Specification - PDF417* shall NOT be used.

- Compact PDF417
- MicroPDF417
- MacroPDF417

D.5.3 Symbology Characteristics

The symbology characteristics shall conform to ISO/IEC 15438.

D.5.4 Dimensions and Print Quality

D.5.4.1 Narrow element dimension

The narrow element dimension (X dimension) range shall be from .170mm (.0066 inch) to .380mm (.015 inch) as determined by the printing capability of the supplier/printer. Symbols with narrow elements at the lower end of this range, i.e., .170mm (.0066 inch) to .250mm (.010 inch), may require special care to meet the print quality requirements of this standard.

D.5.4.2 Row height

The PDF417 symbol shall have a minimum row height (height of the symbol element) of three (3) times the width of the narrow element (“X” dimension). Increasing the row height may improve scanning performance but will reduce the number of characters that can be encoded in a given space.

D.5.4.3 Quiet zone

The PDF417 symbol shall have a minimum quiet zone of 1X (X = the narrow element dimension) above, below, to the left, and to the right. The quiet zone is included within the calculation of the size of the symbol.

D.5.4.4 Print Quality

The AIM^{USA} Uniform Symbology Specification PDF417 and ANSI X3.182 *Bar Code Print Quality* - Guideline shall be used to determine the print quality of the PDF417 symbol.

The minimum symbol grade shall be 3.5/10/660, where:

Recommended Print Quality grade 3.5 (A) at the point of printing the symbol before lamination and a Print Quality Grade of 2.5 (B) after lamination.

Measurement Aperture = .250mm (0.010 inch)

Light Source Wavelength = 660 nanometers (nm) ± 10 nm

The above symbol quality and measurement parameters assure scanability over a broad range of scanning environments.

It is important that the bar code be decodable throughout the system of use. For this reason, quality tests should not be limited to production inspection but also should be followed through to the end use.

D.5.4.5 Error Correction

PDF417 symbols shall use a minimum Error Correction Level of 3. Where space allows, an Error Correction Level of 5 is recommended. Error correction is important for decoding the bar code because certain security laminates interfere with the readability of bar codes, and higher error correction levels help to insure the prolonged usability of the bar code as abrasions and other damage are incurred over time.

D.6 Character sets

The AAMVA community shall use the 256 character table known as ASCII/ISO 8859-1 as the character set table when generating Hi-Density symbols and for efficiency shall use the 128 character subset TEXT COMPACTION TABLE as defined in the specification.

D.7 Compression

No specific recommendation is presented at this time. The AAMVA community has no need to employ specific Compression techniques beyond the field truncation constructs incorporated into the overall Data Structure option recommended in this standard.

D.8 Sampling

To ensure that printed on-demand bar code symbols meet the above Print Quality specification, it is recommended that a sample set of symbols, produced in their final form, be verified a minimum of once per day.

Military Standard, Sampling Procedures and Tables for Inspection by Attributes (ANSI/ASQC Z1.4), provides useful guidelines for statistically valid sampling plans. Acceptable quality levels (AQL) may be established prior to quality control inspection.

D.9 Symbol Durability

If bar code symbol durability is required, then the test method in AAMVA DL/ID-2000, Annex G, G.5, should be used.

D.10 Bar code area

The bar code area shall be located in Zone V of the DL/ID document. The maximum width of the PDF417 symbol shall be 75.565 mm (2.975”). The maximum height of the PDF417 symbol shall be 38.1 mm (1.50”).

D.11 Orientation and Placement

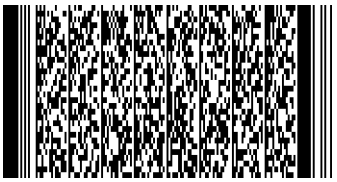
D.11.1 PDF417 Orientation

All PDF417 symbols and linear bar codes shall have the same orientation. The bars of the PDF417 symbol shall be perpendicular to the natural bottom of the card. (see Figure D.1).

The symbol skew shall not be more than ±5 degrees.

D.11.2 Designing the Card Layout

Figure D.1 — Orientation of PDF417 symbol on bottom



Plan for the maximum amount of data:

Determine the required and optional fields that will be required and the maximum anticipated length of each field. Add in the additional characters needed for formatting.

Plan for the maximum “X” dimension(s) that may be used:

Since the supplier/printer of the card ultimately determines the “X” dimension at which the symbol will be printed, it is possible that a PDF417 symbol could be printed at any “X” dimension from .0066 inch to .015 inch. The largest “X” dimension that allows all the data to fit in the maximum area available shall be used when printing the symbol.

D.12 Data encoding structure

All compliant 2D symbols shall employ a file header that allows interested parties to interpret the encoded data. Subfiles shall be employed to carry the specific information. The combination of a header and one or more subfile designators shall make up a compliant 2D symbol.

Each 2-dimensional bar code shall begin with a file header that will identify the bar code as complying with the standard. The header shall be followed by a subfile designator “DL” to identify the DL/ID data type stored in the file. Each data element contained in a subfile shall be prefaced by a data element identifier (Element ID) as defined in Tables D.3 and D.4. The use of a field separator character shall serve to both terminate a field and indicate the presence of a following field identifier.

D.12.1 Header

Compliant 2D Symbol's must begin with a Header in the following format:

Table D.1 — 2D symbols header format

Field	Bytes	Contents
1	1	**Compliance Indicator:** A 2D symbol encoded according to the rules of this standard shall include a Compliance Indicator. The Compliance Indicator as defined by this standard is the Commercial At Sign ("@") (ASCII/ISO 646 Decimal "64") (ASCII/ISO 646 Hex "40"). The Compliance Indicator is the first character of the symbol.
2	1	**Data Element Separator:** The Data Element Separator is used in this standard to indicate that a new data element is to follow, *and* that the current field is terminated. Whenever a Data Element Separator is encountered (within a Subfile type which uses Data Element Separators), the next character(s) shall either be a Segment Terminator or shall define the contents of the next field according to the template of the specific Subfile. The Data Element Separator as defined by this standard is the Line Feed character ("$^{L}_{F}$" ASCII/ISO 646 Decimal "10") (ASCII/ISO 646 Hex "0A"). The Data Element Separator is the second character of the symbol.
3	1	**Record Separator:** The Record Separator as defined by this standard is the Record Separator character ("$^{R}_{S}$" ASCII/ISO 646 Decimal "30") (ASCII/ISO 646 Hex "1E"). As this report is presented for ratification, there is no special case defined for when this field will be used. It is embodied within the recommendation for future growth. The Record Separator is the third character of the symbol and shall always be reflected within the header in a compliant symbol.
4	1	**Segment Terminator:** As used in this standard the Segment Terminator is used to end Subfiles where Field Identifiers are employed. The Segment Terminator as defined by this standard is the Carriage Return character ("$^{C}_{R}$" ASCII/ISO 646 Decimal "13") (ASCII/ISO 646 Hex "0D"). The Segment Terminator is the fourth character of the symbol.
5	5	**File Type:** This is the designator that identifies the file as an AAMVA compliant format. The designator is defined as the 5 byte upper character string "ANSI ", with a blank space after the fourth character .
6	6	**Issuer Identification Number (IIN):** This number uniquely identifies the issuing jurisdiction and can be obtained by contacting the ISO Issuing Authority (AAMVA).

Field	Bytes	Contents
7	2	**AAMVA Version Number:** This is a decimal value between 00 and 99 that specifies the version level of the PDF417 bar code format. Version “0” and "00" is reserved for bar codes printed to the specification of the American Association of Motor Vehicle Administrators (AAMVA) prior to the adoption of the AAMVA DL/ID-2000 standard. All bar codes compliant with the AAMVA DL/ID-2000 standard are designated Version “01.” All barcodes compliant with this current AAMVA specification shall be designated Version “02.” Should a need arise requiring major revision to the format, this field provides the means to accommodate additional revision.
8	2	**Jurisdiction Version Number:** This is a decimal value between 00 and 99 that specifies the jurisdiction version level of the PDF417 bar code format. Notwithstanding iterations of this specification, jurisdictions implement incremental changes to their bar codes, including new jurisdiction-specific data, compression algorithms for digitized images, digital signatures, or new truncation conventions used for names and addresses. Each change to the bar code format within each AAMVA version (above) must be noted, beginning with Jurisdiction Version 00.
9	2	**Number of Entries:** This is a decimal value between “01 and 99” that specifies the number of different Subfile types that are contained in the bar code. This value defines the number of individual subfile designators that follow. All subfile designators (as defined below) follow one behind the other. The data related to the first subfile designator follows the last Subfile Designator.

D.12.2 Subfile Designator

All compliant 2D bar code symbols must contain the “DL” subfile structure as defined below immediately after the Header as defined in D.7.6.

Table D.2 – Subfile designator format

Field	Bytes	Contents
1	2	**Subfile Type:** This is the designator that identifies what type of data is contained in this portion of the file. The 2-character uppercase character field “DL” is the designator for DL/ID subfile type containing mandatory and optional data elements as defined in tables D.3 and D.4. Jurisdictions may define a subfile to contain jurisdiction-specific information. These subfiles are designated with the first character of “Z” and the second character is the first letter of the jurisdiction's name. For example, "ZC" would be the designator for a California or Colorado jurisdiction-defined subfile; "ZQ" would be the designator for a Quebec jurisdiction-defined subfile.
2	4	**Offset:** These bytes contain a 4 digit numeric value that specifies the number of bytes from the head or beginning of the file to where the data related to the particular sub-file is located. The first byte in the file is located at offset 0.
3	4	**Length:** These bytes contain a 4 digit numeric value that specifies the length of the Subfile in bytes. The segment terminator must be included in calculating the length of the subfile. A segment terminator = 1.

D.12.3 Data elements

Tables D.3 and D.4 define mandatory and optional data elements that are accommodated in the “DL” subfile type. Jurisdiction-specific data elements may also be encoded, provided the bar code ID is a 3-character uppercase character field beginning with “Z*X*” where "*X*" is the first letter of the jurisdiction. Each data element field within the jurisdiction-defined subfile should follow consecutively in alphabetic order. For example, data elements in a Virginia subfile would be ZV*A, ZV*B, etc.; a Delaware subfile would be ZD*A*, ZD*B*, etc.).

Mandatory data elements for which no data exists for a given cardholder are to be encoded with the word "none." In the event data is *not available* for a mandatory data element, "unavail" is to be encoded.

For variable length fields, the field should be padded if you do not utilize the maximum field length. For alpha or alphanumeric fields, spaces should be padded to the right of the data. For numeric fields, zeros should be added to the left of the data.

D.12.3.1 Minimum mandatory data elements

Column 1 (**Data Ref.**): serves as a reference indicator for citation elsewhere in this standard and in other documents.

Column 2 (**Element ID**): three letter bar code element identifier corresponding to the data element. The three letter identifier must precede the encoded data element.

Column 3 (**Data element**): common name or phrase that designates what information is to be encoded in the 2D bar code.

Column 4: (**Definition**): description of the data element, including any exceptions.

Column 5: (**Card type**): identifies the applicability of the data element. DL = driver license only; ID = non-driver identification card only; Both = both the driver license and the non-driver identification card.

Column 6: (**Length/type**): valid field length (i.e., the number of characters) for each data element. The following refer to the valid characters or image used (A=alpha A-Z, N=numeric 0-9, S=special, F=fixed length, V=variable length) in the related application.

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
a.	DCA	Jurisdiction-specific vehicle class	Jurisdiction-specific vehicle class / group code, designating the type of vehicle the cardholder has privilege to drive.	DL	V4ANS
b.	DCB	Jurisdiction-specific restriction codes	Jurisdiction-specific codes that represent restrictions to driving privileges (such as airbrakes, automatic transmission, daylight only, etc.).	DL	V10ANS
c.	DCD	Jurisdiction-specific endorsement codes	Jurisdiction-specific codes that represent additional privileges granted to the cardholder beyond the vehicle class (such as transportation of passengers, hazardous materials, operation of motorcycles, etc.).	DL	V5ANS
d.	DBA	Document Expiration Date	Date on which the driving and identification privileges granted by the document are no longer valid.	Both	F8N
e.	DCS	Customer Family Name	Family name of the cardholder. (Family name is sometimes also called “last name” or “surname.”)	Both	V40ANS
f	DCT	Customer Given Names	Given names of the cardholder. (Given names include all names other than the Family Name. This includes all those names sometimes also called “first” and “middle” names.)	Both	V80ANS
g	DCU	Name Suffix	Name Suffix	Both	V5ANS

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
h.	DBD	Document Issue Date	Date on which the document was first issued. (MMDDCCYY)	Both	F8N
i.	DBB	Date of Birth	Date on which the cardholder was born. (MMDDCCYY)	Both	F8N
j.	DBC	Physical Description – Sex	Gender of the cardholder. 1 = male, 2 = female.	Both	F1N
k.	DAY	Physical Description – Eye Color	Color of cardholder's eyes. (ANSI D-20 codes)	Both	F3A
l.	DAU	Physical Description – Height	Height of cardholder. Inches (in): number of inches followed by " in" ex. 6'1" = " 73 in" Centimeters (cm): number of centimeters followed by " cm" ex. 181 centimeters="181 cm"	Both	F6AN
m.	DCE	Physical Description – Weight Range	Indicates the approximate weight range of the cardholder: 1 = 0 – 31 kg (0 – 70 lbs) 2 = 32 – 45 kg (71 – 100 lbs) 3 = 46 - 59 kg (101 – 130 lbs) 4 = 60 - 70 kg (131 – 160 lbs) 5 = 71 - 86 kg (161 – 190 lbs) 6 = 87 - 100 kg (191 – 220 lbs) 7 = 101 - 113 kg (221 – 250 lbs) 7 = 114 - 127 kg (251 – 280 lbs) 8 = 128 – 145 kg (281 – 320 lbs) 9 = 146+ kg (321+ lbs)	Both	F1N
n.	DAG	Address – Street 1	Street portion of the cardholder address.	Both	V35ANS
o.	DAI	Address – City	City portion of the cardholder address.	Both	V20ANS
p.	DAJ	Address – Jurisdiction Code	State portion of the cardholder address.	Both	F2A
q.	DAK	Address – Postal Code	Postal code portion of the cardholder address. If the trailing portion of the postal code in the U.S. is not known, zeros will be used to fill the trailing	Both	F11N

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
			set of numbers.		
r.	DAQ	Customer ID Number	The number assigned or calculated by the issuing authority.	Both	V25ANS
s.	DCF	Document Discriminator	Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.	Both	V25ANS
t.	DCG	Country Identification	Country in which DL/ID is issued. U.S. = USA, Canada = CDN.	Both	F3A
u.	DCH	Federal Commercial Vehicle Codes	Federally established codes for vehicle categories, endorsements, and restrictions that are generally applicable to commercial motor vehicles. If the vehicle is not a commercial vehicle, "NONE" is to be entered.	DL	F4AN

D.12.3.2 Optional data elements

Column 1 (**Data Ref.**): serves as a reference indicator for citation elsewhere in this standard and in other documents.

Column 2 (**Element ID**): three letter bar code element identifier corresponding to the data element. The three letter identifier must precede the encoded data element.

Column 3 (**Data element**): common name or phrase that designates what information is to be encoded in the 2D bar code.

Column 4: (**Definition**): description of the data element, including any exceptions.

Column 5: (**Card type**): identifies the applicability of the data element. DL = driver license only; ID = non-driver identification card only; Both = both the driver license and the non-driver identification card.

Column 6: (**Length/type**): valid field length (i.e., the number of characters) for each data element. The following refer to the valid characters or image used (A=alpha A-Z, N=numeric 0-9, S=special, F=fixed length, V=variable length) in the related application.

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
a.	DAH	Address – Street 2	Second line of street portion of the cardholder address.	Both	V35ANS
b.	DAZ	Hair color	Brown, black, blonde, gray, red/auburn, sandy, white	Both	V12A
c.	DCI	Place of birth	Country and municipality and/or state/province	Both	V33A
d.	DCJ	Audit information	A string of letters and/or numbers that identifies when, where, and by whom a driver license/ID card was made.	Both	V25ANS
e.	DCK	Inventory control number	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licenses and ID cards.	Both	V25ANS
f.	DBN	Alias / AKA Name	Other name by which cardholder is known.	Both	V35ANS
g.	DCL	Race / ethnicity	Codes for race or ethnicity of the cardholder, as defined in ANSI D20.	Both	F2N
h.	DCM	Standard vehicle classification	Standard vehicle classification code(s) for cardholder. This data element is a placeholder for future efforts to standardize vehicle classifications.	DL	F4AN
i.	DCN	Standard endorsement code	Standard endorsement code(s) for cardholder. This data element is a placeholder for future efforts to standardize endorsement codes.	DL	F5AN
j.	DCO	Standard restriction code	Standard restriction code(s) for cardholder. This data element is a placeholder for future efforts to standardize restriction codes.	DL	F10AN
k.	DCP	Jurisdiction-specific vehicle classification description	Text describing the jurisdiction-specific code(s) for types of vehicles cardholder is authorized to drive.	DL	V50ANS
l.	DCQ	Jurisdiction-specific endorsement code	Text describing the jurisdiction-specific code(s) that indicates additional driving privileges granted to the cardholder beyond the vehicle	DL	V50ANS

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
		description	class.		
m.	DCR	Jurisdiction-specific restriction code description	Text describing the jurisdiction-specific restriction code(s) that curtail driving privileges.	DL	V50ANS

D.12.3.3 Additional data elements

Jurisdictions wishing to encode data elements in their PDF-417 bar codes other than those described in the above lists of mandatory and optional data elements should coordinate with AAMVA on the format and Data Element ID to use for that data. This will prevent the introduction of conflicts and variances across the jurisdictions.

Annex E
(normative)

Test Methods

Introduction (informative)

Driver license jurisdictions need some level of assurance about card service life. Therefore, jurisdictions are requiring card durability test results when requests for proposal (RFP) are made. The RFPs often include inadequately defined test methods that leave test details up to the test laboratory's discretion. The result is that test data will often be significantly affected by the discretionary details.

The ANSI NCITS 322 test methods were developed by industry experts from card component suppliers, card manufacturers, and card personalization companies. The objective was to provide standardized tests capable of giving reproducible results.

These accelerated laboratory test methods are the group's best effort to simulate field failures. Relevancy and correlation between predicted card service life and ANSI NCITS 322 test data has not been established at the time of publication. Test results only provide a means of ranking or comparing one card structure to another. Future work is planned to determine relevancy of and correlation between card test methods and card service life.

E.1 Scope

This annex provides a set of precisely defined card durability test procedures based on ANSI NCITS 322. The usefulness of results obtained from these test methods is only to compare or rank the relative durability of one card structure to another.

E.2 Conformance

A test result is in conformance with this annex if it meets all the mandatory requirements specified directly or by reference herein. Test results shall not be represented as equivalent to card service life.

E.3 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this annex. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the normative document referred to applies.

ANSI NCITS 322, *For information technology-Card durability test methods: 1998*

ISO 10373-1, *Identification cards - Test methods - General characteristics tests*

E.4 Terms and definitions

For the purposes of this annex, the following terms and definitions apply:

E.4.1 card service life

period of time between card issuance and expiration date

E.5 Test methods and sample size

Only the test methods described in ANSI NCITS 322 shall be used. Performing multiple tests on the same card shall not be done. Sample size is not specified, however some tests require more than 1 card in order to obtain a single result.

Note (Informative) Test precision is unknown for the individual test methods. Therefore, caution should be taken when determining if the test result differences between card types is large enough to be statistically significant. It is strongly recommended that one laboratory perform comparison testing for all card types being evaluated. If possible, cards from different vendors should also be tested simultaneously to minimize test variability. Sample sizes necessary to reach statistical confidence are unknown. Typical sample sizes used by industry are shown in the tables below.

ANSI NCITS 322 recommended sample size (Informative)

Clause	Test description	Card orientation NA = not applicable	Typical sample size # cards
5.1	Delamination-90 degrees	NA	6
5.2	Delamination-180 degrees	NA	6
5.3	Delamination-Cross Hatch Tape Test (for heat transfer film layers)	NA	6
5.4	ID-1 Card Flexure	axis A, face up	4
		axis A, face down	4
		axis B, face up	4
		axis B, face down	4
5.5	ID-1 Card Static Stress	axis A, face up	25
		axis A, face down	25

		axis B, face up	25
		axis B, face down	25
5.6	ID-1 Card Stress and Plasticizer Exposure	axis A, face up	4
		axis A, face down	4
		axis B, face up	4
		axis B, face down	4
5.7	Impact Resistance	NA	25
5.9	Surface Abrasion	NA	6
5.10	Bar Code Abrasion	NA	6
5.11	Magnetic Stripe Abrasion	NA	6
5.12	Image Abrasion	NA	6
5.13	Temperature and Humidity Induces Dye Migration	NA	6
5.14	Plasticizer Induced Dye Migration	NA	6 sets of 5
5.15	Ultraviolet (UV) Light Exposure Stability	test both sides of card	6
5.16	Daylight Exposure Image Stability-Xenon Arc	test both sides of card	6
5.17	Laundry Test	NA	6
5.18	Embossed Character Retention-Pressure	NA	6
5.19	Embossed Character Retention-Heat	NA	6
5.20	Corner Impact Test	NA	6
5.21	Wet Abrasion and Impact	NA	6 – 16
5.22	IC Card with Contacts Micromodule Adhesion	NA	6
6.1	Card Structure Integrity Test Sequence	NA	6 – 16

ISO 10373-1 recommended sample size (Informative)

clause	Test description	Card orientation NA = not applicable	Typical sample size # cards
5.9	Dynamic torsional stress (torsion)	NA	6

E.6 Test report

For each test performed, the following information shall be included in the test report:

- ANSI NCITS 322 or ISO 10373-1 date and clause number
- test method title
- sample size used
- date when testing was completed
- identifying name or number to describe the type/color/style of card tested
- result for each card tested (numeric and/or qualitative)

Annex F
(normative)

Optional Magnetic Stripe

F.1 Scope

This annex defines mapping of the driver license/identification card machine-readable information elements onto a 3-track magnetic stripe. This annex expands upon, corrects minor errors in, and intends to supersede the requirements of AAMVA DL/ID-2000 Annex D – *Mapping of driver license/identification card information to optical memory cards* (6 June 2000).

F.2 Introduction

This annex defines mapping of the DL/ID card machine-readable data elements onto a magnetic stripe. For the purposes of this specification, AAMVA has adopted the magnetic stripe annex from the AAMVA DL/ID-2000 standard (Annex A). The minimum mandatory data elements of the new specification (see paragraph 5.2 of this specification) will not fit within a 3-track magnetic stripe. The AAMVA DL/ID-2000 magnetic stripe annex was grandfathered in its entirety in the interest of smoothing a transition from legacy DL/ID documents and legacy readers that are designed to interact with cards issued under the AAMVA DL/ID-2000 standard.

F.3 Conformance

Conformance with all parts of ISO/IEC 7811-6 is required with the exception of data content and coded character sets as defined in Table A.1 and A.1.

F.4 Card characteristics

The physical characteristics and dimensions shall conform to ISO/IEC 7810. The magnetic stripe area shall conform to ISO/IEC 7811-6 for tracks 1, 2, and 3.

F.5 Coded character set

Tables F.1 and F.2 define characters for tracks 1, 2, and 3. The coded character sets for 5 bit numeric and 7 bit alphanumeric are the same as those described in ISO/IEC 7811-6. However, the use of the characters for data or control purposes may be different.

Table F.1 — Coded character set for 5 bit numeric

ASCII	Hex	Binary					ASCII	Hex	Binary				
		P	2^3	2^2	2^1	2^0			P	2^3	2^2	2^1	2^0
0	30	1	0	0	0	0	8	38	0	1	0	0	0
1	31	0	0	0	0	1	9	39	1	1	0	0	1
2	32	0	0	0	1	0	:	3A	1	1	0	1	0
3	33	1	0	0	1	1	;	3B	0	1	0	1	1
4	34	0	0	1	0	0	<	3C	1	1	1	0	0

ASCII	Hex	Binary					ASCII	Hex	Binary				
5	35	1	0	1	0	1	**=**	3D	0	1	1	0	1
6	36	1	0	1	1	0	**>**	3E	0	1	1	1	0
7	37	0	0	1	1	1	**?**	3F	1	1	1	1	1
The 3 characters **: < >** are available for hardware control purposes and shall not be used for information (data content).													
The 3 characters **; = ?** shall have the following meaning: **;** start sentinel **=** field separator **?** end sentinel													

Table F.2 — Coded character set for 7 bit alphanumeric

ASCII	Hex	Binary							ASCII	Hex	Binary						
		P	2^5	2^4	2^3	2^2	2^1	2^0			P	2^5	2^4	2^3	2^2	2^1	2^0
space	20	1	0	0	0	0	0	0	@	40	0	1	0	0	0	0	0
!	21	0	0	0	0	0	0	1	A	41	1	1	0	0	0	0	1
“	22	0	0	0	0	0	1	0	B	42	1	1	0	0	0	1	0
#	23	1	0	0	0	0	1	1	C	43	0	1	0	0	0	1	1
$	24	0	0	0	0	1	0	0	D	44	1	1	0	0	1	0	0
%	25	1	0	0	0	1	0	1	E	45	0	1	0	0	1	0	1
&	26	1	0	0	0	1	1	0	F	46	0	1	0	0	1	1	0
‘	27	0	0	0	0	1	1	1	G	47	1	1	0	0	1	1	1
(	28	0	0	0	1	0	0	0	H	48	1	1	0	1	0	0	0
)	29	1	0	0	1	0	0	1	I	49	0	1	0	1	0	0	1
*****	2A	1	0	0	1	0	1	0	J	4A	0	1	0	1	0	1	0
+	2B	0	0	0	1	0	1	1	K	4B	1	1	0	1	0	1	1
,	2C	1	0	0	1	1	0	0	L	4C	0	1	0	1	1	0	0
-	2D	0	0	0	1	1	0	1	M	4D	1	1	0	1	1	0	1
.	2E	0	0	0	1	1	1	0	N	4E	1	1	0	1	1	1	0
/	2F	1	0	0	1	1	1	1	O	4F	0	1	0	1	1	1	1
0	30	0	0	1	0	0	0	0	P	50	1	1	1	0	0	0	0
1	31	1	0	1	0	0	0	1	Q	51	0	1	1	0	0	0	1
2	32	1	0	1	0	0	1	0	R	52	0	1	1	0	0	1	0
3	33	0	0	1	0	0	1	1	S	53	1	1	1	0	0	1	1
4	34	1	0	1	0	1	0	0	T	54	0	1	1	0	1	0	0
5	35	0	0	1	0	1	0	1	U	55	1	1	1	0	1	0	1
6	36	0	0	1	0	1	1	0	V	56	1	1	1	0	1	1	0
7	37	1	0	1	0	1	1	1	W	57	0	1	1	0	1	1	1
8	38	1	0	1	1	0	0	0	X	58	0	1	1	1	0	0	0
9	39	0	0	1	1	0	0	1	Y	59	1	1	1	1	0	0	1
:	3A	0	0	1	1	0	1	0	Z	5A	1	1	1	1	0	1	0
;	3B	1	0	1	1	0	1	1	**[**	5B	0	1	1	1	0	1	1
<	3C	0	0	1	1	1	0	0	\	5C	1	1	1	1	1	0	0
=	3D	1	0	1	1	1	0	1	**]**	5D	0	1	1	1	1	0	1
>	3E	1	0	1	1	1	1	0	**^**	5E	0	1	1	1	1	1	0
?	3F	0	0	1	1	1	1	1	**_**	5F	1	1	1	1	1	1	1
The 14 characters **! “ & ‘ * + , : ; < = > @ _** are available for hardware control purposes and shall not																	

ASCII	Hex	Binary	ASCII	Hex	Binary
be used for information (data content). Applies to track 1 only.					
The 3 characters **[\ ]** are reserved for additional national characters when required. They shall not be used internationally. Applies to track 1 only.					
The character **#** is reserved for optional additional graphic symbols. Applies to track 1 only.					
The 3 characters **% ^ ?** shall have the following meaning: **%** start sentinel **^** field separator **?** end sentinel					
All 64 characters may be used for information (data content). Applies to track 3 only.					

F.6 Information content and format

This standard uses additional characters and a different format for track 3 than what is described in ISO/IEC 7811-6. The following tables give the content for each track. This is unique to the AAMVA community and will require modifications to the encoding and reading devices used in conjunction with track 3. The ability to implement such modifications is a mainstay of the magnetic stripe environment and will introduce no significant problem to any jurisdiction or to any public or private sector entity wishing to use the magnetic stripe DL/ID card.

F.6.1 Track 1

Table F.3 — Track 1 information content and format

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
-	82	V-max	O	Track 1	A/N data in 7 bit binary code for state, city, name.	see Table A.2 and iv
1	1	F	R	Start sentinel	This character must be encoded at the beginning of the track.	%
2	2	F	R	State or Province	Mailing or residential code.	A-Z, see ii
3	13	V-max	R	City	This field shall be truncated with a field separator ^ if less than 13 characters long. If the city is exactly 13 characters long then no field separator is used (see i). Richfield^	A-Z **.-'** space
4	35	V-max	R	Name	Priority is as follows, spaces allowed; last name$firstname$title This field shall be truncated with a field separator ^ if less than 35 characters long. The "$" symbol is used as a delimiter between names (see i & iii).	A-Z **.-'** space

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
5	29	V	R	Address	The street number shall be as it would appear on mail. The $ is used as a delimiter between address lines. This field shall be truncated with a field separator (or padded with spaces) if less than 29 characters long but can be longer (see i). 28 Atol Av$Suite 2$^ Hiawatha Park$Apt 2037^ 340 Brentwood Dr.$Fall Estate	A-Z 0-9 .-' space
6	1	F	R	End sentinel	This character shall be after the last data character of the track.	?
7	1	F	R	LRC	Longitudinal redundancy check is generated from all other characters and is the last character encoded.	see Table A.2
I	Fields 3 and 4 may be shorter than the maximum listed. Total for fields 3,4 and 5 combined is 77 characters.					
ii	Allowable characters are further restricted to those defined in ANSI D-20.					
iii	The $ symbol is used for a delimiter rather than the @ symbol as defined in ANSI D-20. There is no @ symbol in the 7 bit character set.					
iv	For Fields 1 through 6 only the following characters from Table A.2 are allowed: A-Z 0-9 $ % ( ) - . / ^ ? space					

F.6.2 Track 2

Table F.4 — Track 2 information content and format

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
-	40	V-max	O	Track 2	Numeric data in 5 bit binary code for DL number, expiration date, birthdate.	see Table A.1
1	1	F	R	Start sentinel	This character shall be encoded at the beginning of the track.	;

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
2	6	F	R	ISO IIN	This is the assigned identification number from ISO. This number shall always begin with a "6". This number shall be obtained from the AAMVAnet Standards Program Director.	0-9
3	13	V-max	R	DL/ID#	This field is used to represent the DL/ID number assigned by each jurisdiction. Overflow for DL/ID numbers longer than 13 characters is accommodated in field number 7.	0-9
4	1	F	R	Field Separator	A field separator must be used after the DL/ID number regardless of length.	=
5	4	F	R	Expiration date	This field is in the format: YYMM If MM=77 then license is "non-expiring". If MM=88 the Expiration Date is after the last day of their birth month One Year from the Month (MM) of Field 6 and the Year (YY) of Field 5 (Expiration Date). If MM=99 then the Expiration Date is on the Month (MM) and Day (DD) of Field 6 (Birthdate) and the Year (YY) of Field 5 (Expiration Date).	0-9
6	8	F	R	Birthdate	This field is in the format: CCYYMMDD	0-9
7	5	V	O	DL/ID# overflow	Overflow for numbers longer than 13 characters. If no information is used then a field separator is used in this field.	0-9
8	1	F	R	End sentinel	This character shall be after the last data character of the track.	?

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
9	1	F	R	LRC	Longitudinal redundancy check is generated from all other characters and is the last character encoded.	see Table A.2
Rules governing DL/ID numbering format(s) will be kept by the Issuing DL/ID Agencies. DL/ID Numbers containing printed Alpha characters will be represented by two numeric positions for each Alpha character on Track 2. Example: The character (A) = a numeric (01), character (B) = a numeric (02), character Z = a numeric (26).						

F.6.3 Track 3

Table F.5 — Track 3 information content and format

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
-	82	V-max	O	Track 3	A/N data in 7 bit binary code for postal code, class, restrictions.	see Table A.2 and ii
1	1	F	R	Start sentinel	This character shall be encoded at the beginning of the track.	%
2	1	F	R	Version #	This field used to store the mag stripe version used.	02
3	1	F	R	Security v.#	This field used to store the security version being used (00-63), 00 means no security being used.	0-9
4	11	F	R	Postal code	For an 11 digit postal or zip code. (left justify fill with spaces, no hyphen)	A-Z, 0-9, space
5	2	F	R	Class	Represents the type of DL (ANSI codes modified for CDLIS).See i	A-Z, 0-9, space
6	10	F	R	Restrictions	See i, iii	A-Z, 0-9, space
7	4	F	R	Endorsements	See i, iii	A-Z, 0-9, space
8	1	F	R	Sex	M for male, F for female.	M,F
9	3	F	R	Height	See i, iii	0-9, space
10	3	F	R	Weight	See i, iii	0-9, space
11	3	F	R	Hair Color	See i, iii	A-Z, space
12	3	F	R	Eye Color	See i, iii	A-Z, space

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
13	10	V	O	ID #	Discretionary data for use by each jurisdiction.	see Table A.2
14	22	V	O	Reserved space	Discretionary data for use by each jurisdiction.	see Table A.2
15	5	V	O	Security	Discretionary data for use by each jurisdiction.	see Table A.2
16	1	F	R	End sentinel	This character shall be after the last data character of the track.	?
17	1	F	R	LRC	Longitudinal redundancy check is generated from all other characters and is the last character encoded.	see Table A.2
I	Allowable characters are further restricted to those defined in ANSI D-20.					
Ii	All 64 characters may be used in data fields; this is different from the ISO use of Table A.2 coded characters. Special hardware or software may be required for readers and encoders.					
iii	If not present pad with spaces.					

F.7 Encoding specifications

Track locations, start of encoding location, end of encoding location, average bit density, flux transition spacing variation, and signal amplitude requirements shall be as described in ISO/IEC 7811-6 for tracks 1, 2, and 3.

F.8 Error detection

Inclusion of parity and LRC as described in ISO/IEC 7811-6 is required.

Annex G
(normative)

Optional Optical Memory

G.1 Scope

This annex defines mapping of the driver license/identification card machine-readable information elements onto optical memory. This annex expands upon, corrects minor errors in, and intends to supersede the requirements of AAMVA DL/ID-2000 Annex D – *Mapping of driver license/identification card information to optical memory cards* (6 June 2000).

G.2 Introduction

This annex defines mapping of the driver license/identification card machine-readable data elements, as defined in clause 6, onto an optical memory card.

G.3 Conformance

A driver license/identification card that incorporates optical memory shall comply with the following standards; ISO/IEC 11693 and 11694 Parts 1 - 4.

G.4 File location

The Information content of the PDF417 bar code, defined in annex D of this specification, shall be written to both the first and last user data tracks of the optical memory card. The data shall be written as ASCII exactly duplicating the data format and structure defined in F.5. Unused sectors in the first and last user data tracks shall be reserved for future use.

G.5 Updating of data

The data written to the first and last user data tracks shall be read-only. If updating of the data is permitted, additional sectors in the first and last user data tracks may be used to control access for updating purposes and to specify the location of the updated data. The original data in the first and last user data tracks shall remain unchanged in order to provide an audit trail.