American Association of Motor Vehicle Administrators (AAMVA)

Date: 2011-July

AAMVA Driver Standing Committee – Card Design Committee

Secretariat: AAMVA

Personal Identification – AAMVA North American Standard – DL/ID Card Design

Contents

Page

Foreword

The American Association of Motor Vehicle Administrators, AAMVA, founded in 1933 is a voluntary, nonprofit, educational 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, acts as the international spokesman for these interests, and 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 standard was originally 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 the 2005 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.

A Special Task Force was reconstituted in late 2008 to undertake this revision and to provide specific guidance for those jurisdictions seeking to comply with programs like REAL ID and the Western Hemisphere Travel Initiative (WHTI). The option of issuing an International Organization for Standardization (ISO) compliant driving licence (IDL) is also supported and explained.

0 Introduction

This document provides a standard for the design of driver licenses (DL) and identification (ID) cards issued by AAMVA member jurisdictions. The intent of the standard 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. AAMVA respects the fact that each jurisdiction's laws and regulations determine its driver license issuance process and its associated card requirements. As a result, the intent of this document is to provide jurisdictions with guidance on the driver license/ID card design standards in order to provide a reliable source of identification and, at the same time, reduce a cardholder's exposure to identity theft and fraud.

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 requirements. 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 numbers 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 standard are intended to improve the interoperability of DL/ID cards, particularly by standardizing 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 increased the motivation to alter or counterfeit the DL/ID card. Therefore, this standard 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 was not achieved.

Jurisdictions that follow this standard 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 ensure 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, 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 from another jurisdiction. This standard 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 standard provides a much more comprehensive set of requirements for the security features of the DL/ID card. 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 2010

This standard replaces the existing AAMVA North American Standard for the Driver License/Identification Card, AAMVA DL/ID-2010. Since at the time of publication of this standard and for some time after, many jurisdictions will continue to issue licenses based on AAMVA DL/ID-2010, 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-2010.

0.6   Compatibility with ISO Standard for International Driver License

This standard generally follows the ISO/IEC 18013-1: ISO compliant driving license – Part 1: Physical Characteristics and Basic Data Set; and, Part 2:Machine-readable technologies. The ISO standard (which was developed under leadership of the US) specifies requirements for a card that is aligned with the UN Conventions on road traffic (covering among others domestic and international driving permits), and also addresses security and interoperability issues in general. Taking advantage of the investment already made by ISO in the ISO standard and of the international expertise embodied therein, this standard continues to move toward full compatibility with the ISO standard while at the same time making adaptations to accommodate local requirements. An example of such an adaptation is the specification of a vertical card format for a driver under the age of twenty-one (optional for Canada). As far as the regularly oriented card is concerned, this standard does not prevent a jurisdiction from designing a card that is compliant with this standard as well as with the ISO

standard (thus enabling the jurisdiction to issue one document acting as both a State driver's license and as an international driving permit).

0.7   DHS's standards for driver's licenses and enhanced driver's licenses

Since the publication of the AAMVA National Standard for the Driver License/Identification Card, AAMVA DL/ID-2000 and the AAMVA International Standard for the Driver License/Identification Card, AAMVA DL/ID-2005, the REAL ID Act was signed into law on May 11, 2005[1] and the Department of Homeland Security (DHS) subsequently issued a regulation on the "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes"[2].   The AAMVA standard is consistent with the requirements identified in the DHS regulation. Through implementation of REAL ID Act, DHS's goal is to improve the security of state-issued driver's licenses by requiring:

(1) Information and physical security features that must be incorporated into each card;

(2) Specific application information to establish an applicant's identity and lawful presence in the United States before a card can be issued;[3]

(3) Verification of certain source documents provided by an applicant with the document issuing agencies; and

(4) Issuance and physical security standards for locations where licenses and identification cards are issued.

The Enhanced Driver's License (EDL) programs have been developed to provide U.S. (and Canadian) citizens with an alternative cross-border travel document that meets the requirements of the Western Hemisphere Travel Initiative (WHTI).   The EDLs are being developed consistent with the requirements of REAL ID; the programs have some important similarities and distinctions.   Similarities include:

- EDLs can be used for official purposes, such as: accessing Federal facilities, boarding Federally-regulated commercial aircraft, or entering nuclear power plants.

- EDLs will utilize the capabilities developed for REAL ID (such as the electronic verification of vital records and state-to-state verification of existing DLs/IDs) as they are implemented.

- Both REAL ID licenses and EDLs include (1) information and security features that must be incorporated into each card; (2) specific application information to establish the identity and citizenship of an applicant before a card can be issued; (3) ability to verify certain source documents provided by an applicant with the document issuing agency where applicable; and (4) physical security standards for locations where licenses and identification cards are issued.

---

[1] *See,* Public Law 109–13, 119 Stat. 231, 302 (May 11, 2005) (codified at 49 U.S.C. 30301 note).

[2] Federal Register / Vol. 73, No. 19 / Tuesday, January 29, 2008, pp. 5272-5340

[3] EDLs are only issued to U.S. citizens by states or Canadian citizens by provinces.

Although the goal of enhancing driver's license security is shared by both programs, there are some distinctions:

- In order to be eligible for a REAL ID compliant license, the applicant must demonstrate proof of legal status in the U.S., to be eligible for an EDL the applicant must be a U.S. citizen.

- The EDL serves as a limited-use international travel document, under the Western Hemisphere Travel Initiative (WHTI).) that denotes both identity and citizenship. REAL ID compliant licenses may not be used for international travel.

- An EDL includes a vicinity Radio Frequency Identification (RFID) chip to facilitate border crossing and verification by U.S. Customs and Border Protection (CBP) at a land or sea port of entry. REAL IDs are not prohibited from including this technology, but it is not a requirement.

- An EDL also includes a machine readable zone (MRZ), which complies with travel document standards, to allow CBP officers to read the card electronically if RFID is not available. A REAL ID includes a 2D PDF417 barcode, primarily to allow State and local law enforcement to verify the document's validity.

Personal Identification – AAMVA North American Standard – DL/ID Card Design

1   Scope

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

This standard supersedes the <u>AAMVA DL/ID 2010 Standard</u>. Requests for interpretation, suggestions for improvement, addenda, or defect reports are welcome. They should be sent to AAMVA Identification Standards Program, 4301 Wilson Boulevard, Suite 400, Arlington, VA 22203.

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, and D. There are additional requirements of other standards as referenced in Annexes E, F, G, H, I and J that may be adopted by issuing authorities.

2   Reference(s)

The following documents contain provisions, which, through reference in this text, constitute provisions of this AAMVA standard or were consulted in the compilation of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this 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 96/47/EC of 23 July 1996 O.J. EC No. L 235/1

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

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

ANSI INCITS 385:– *Digital Image Attributes, Face Interchange Format (Human and Automated)*

ISO 1831: *Printing Specifications for Optical Character Recognition*

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*

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

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

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

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

ISO/IEC 18013-2: *ISO compliant driving licence – Part 2: Machine-readable technologies*

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 9303 Part 3 - Machine Readable Official Travel Documents, Volume 1 – MRtds with Machine Readable Data Stored in Optical Character Recognition Format, Third edition – 2008

EPCglobal Tag Data Standards Version 1.3

3   Term(s) and definition(s)

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

3.1
alphabetic (A)
alpha characters/letters from A to Z and a to z

3.2
ANS
any combination of A, N, or S 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 licenses describes a section of the standard that provides supplementary information intended to assist in the understanding and use of this standard

3.5
customer record
Information pertaining to the cardholder that is stored in a jurisdiction database. Such records commonly include biographical and demographic 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.

3.6
data element
an item of data that may appear on the license in either human or machine-readable form

3.7
digital
any data that is composed of a discrete sample or collection of discrete samples that are represented as finite numbers

3.8
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

3.9
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 cardholder: 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 licence" and appears in some places in this document.

3.10
DL/ID
refers generally to both or either driver licenses (DL) and identification cards (ID)

3.11
EDL
enhanced driver license

3.12
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

3.13
human-readable
data or information that is printed or engraved that is visually present on a driver license

3.14
identification card (ID)
a card issued to a person whose identity is verified in the same manner as required for the issuance of a driver license by a licensing authority for identification purposes only, excluding other identification provided by the issuing authority, such as state employee identification, senior citizen cards, handgun permits, etc.

3.15
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 of digital formats

3.16
informative
describes a section of the standard that provides supplementary information intended to assist in the understanding and use of this standard

3.17
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

3.18
machine-readable technology (MRT)
machine-readable mediums, such as a magnetic stripe, bar code, optical memory, or integrated circuit card that carry data

3.19
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

3.20
non-portrait side of card
the opposite face from the portrait side

3.21
normative
describes a section of the standard that is mandatory and must be implemented in the prescribed way for compliance

3.22
numeric (N)
digits 0 to 9

3.23
portrait side of card
face of the card carrying visual information containing the reproduction of the portrait of the cardholder and cardholder identifiers

3.24
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

3.25
third line inspection (Level 3)
inspection by forensic specialists conducting detailed examination that allows for more in-depth evaluation and may require special equipment to provide true certification

3.26
visual special characters (S)
! " # % & ' ( ) * + , - . / : ; < = > ? [\ ] ^ _ @ "space". Visual special characters do not include characters used as delimiters between data elements in a machine-readable technology

4   Human-readable data elements

4.1   Data element tables

Table 1 in section 4.2 describes the mandatory data elements that must visually appear on DL/ID documents. Jurisdictions may go beyond these minimum mandatory requirements, as long as each mandatory requirement is met. Table 2 in section 4.3 describes optional data elements that may visually appear on 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 described by the rules in this standard.

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 shall 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. If no on card reference number is listed in this standard, then no number should be used.

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 standard. 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. These **data elements, if used,** must be labeled using text on the card (If the jurisdiction uses French, the French translations of the data elements and their abbreviations are provided). 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.

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 and type) 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).

4.2   Mandatory data elements

Table 1 — Mandatory data elements

Data ref.	On card reference	Zone placement	Data element English/ Français	Definition	Card type	Field maximum length/type
a.	1	Zone II	Family Name[4] / Nom de famille	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. Collect full name for record, print as many characters as possible on portrait side of DL/ID.	Both	V40ANS

---

[4] 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 English/ Français	Definition	Card type	Field maximum length/type
b.	2	Zone II	Given names[2] / Prénoms	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 is used, the Given Names and the Suffix must be separated by a comma and a space. Collect full name for record, print as many characters as possible on portrait side of DL/ID.	Both	V80ANS
c.	3	Zone II	Date of birth **DOB** / Date de naissance **DDN**	Month, day, year (If unknown, approximate DOB). Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
d.	4a	Zone II	Date of Issue **Iss** / Date de délivrance **Dél.**	Date DL/ID was issued. Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
e.	4b	Zone II	Date of expiry **Exp** / Date d'expiration **Exp.**	Date DL/ID expires. Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
f.	4d	Zone II	Customer identifier / Identificateur de client	The alphanumeric string assigned or calculated by the issuing authority.	Both	V25ANS
g.	5	Zone II	Document discriminator **DD** / Discriminateur de document **Réf**	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

Data ref.	On card reference	Zone placement	Data element English/ Français	Definition	Card type	Field maximum length/type
h.		Zone III	Portrait / Portrait	A reproduction of the cardholder's photograph/image. The portrait must be in color unless laser engraving card production is used.	Both	- (Image)
i.		Zone II / III	Signature / Signature	A reproduction of the cardholder's signature. The signature may overlap the portrait image. If the signature overlaps the portrait, it may be in Zone III. Otherwise, it must be in Zone II.	Both	- (Image)
j.	8	Zone II	Cardholder address[5] / Adresse du détenteur/de la détentrice	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. If a mailing address such as a P.O. Box is used on portrait side of document, the residence address must be collected for the electronic record.	Both	V108ANS
k.	9	Zone II / Zone IV	Vehicle classifications / categories / Classifications/ca tégories de véhicules	Vehicle types the driver is authorized to operate. Each vehicle classification / category denoted on the DL/ID must be described or illustrated in Zone IV.	DL	V6ANS or image
l.	9a	Zone II / Zone IV	Endorsements **End** / Mentions **Ment.**	Jurisdiction-specific codes denoting 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 or illustrated in Zone IV.	DL	V5ANS or image

---

[5] 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 English/ Français	Definition	Card type	Field maximum length/type
m.	12	Zone II / Zone IV	Restrictions / conditions / information codes / Codes d'information sur les restrictions/conditions	Jurisdiction-specific 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	V12ANS (Image)
n.	15	Zone II	Cardholder sex **Sex** / Sexe du détenteur/de la détentrice **Sexe**	Cardholder's sex: M for male, F for female.	Both	F1A
o.	16	Zone II	Height **Hgt** / Taille **Taille**	U.S. : feet and inches ex. 6 foot 1 inch = "6'-01"" Canada: centimeters (cm), number of centimeters followed by " cm" ex. 181 centimeters="181 cm"	Both	F6ANS
p.	18	Zone II	Eye color **Eyes** / Couleur des yeux **Yeux**	Blue, brown, black, hazel, green, gray, pink, maroon, dichromatic. If the issuing jurisdiction wishes to abbreviate colors, the three-character codes provided in ANSI D20 must be used.	Both	V12A

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.	19	Zone II	Hair color **hair** / Couleur des cheveux **cheveux**	Bald, black, blonde, brown, gray, red/auburn, sandy, white, unknown. If the issuing jurisdiction wishes to abbreviate colors, the three-character codes provided in ANSI D20 must be used.	Both	V12A
b.	3a	Zone II	Place of birth / Lieu de naissance	Country and municipality and/or state/province	Both	V33A
c.	21	-	Inventory control number / Numéro de contrôle d'inventaire	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 or bar code
d.	10	Zone II / Zone IV	Date of first issue per category [6] / Date de délivrance pour la première fois, par catégorie	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

---

[6] 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.

Data ref	On card reference	Zone placement	Data element/label	Definition	Card Type	Field Length/Type
e.	11	Zone II / Zone IV	Separate expiry dates for vehicle classifications / Dates d'expiration séparées pour les catégories de véhicule	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 U.S., CCYY/MM/DD Canadian	DL	F10NS
f.	17	Zone II	Weight **Wgt** / Poids **Poids**	Indicates the approximate weight range of the cardholder: U.S.: pounds ex. 185 pounds = "185 lb" Canada: kilograms ex. 84 kilograms = "084 kg"	Both	F6ANS

Data ref	On card reference	Zone placement	Data element/label	Definition	Card Type	Field Length/Type
g.		Zone II	Name suffix[2] / Suffixe	Name suffix of the individual that has been issued the driver license or identification document. If Suffix is used, the Given Names and the Suffix must be separated by a comma and a space. Collect full name for record, print as many characters as possible on portrait side of DL/ID. • JR (Junior) • SR (Senior) • 1ST or I (First) • 2ND or II (Second) • 3RD or III (Third) • 4TH or IV (Fourth) • 5TH or V (Fifth) • 6TH or VI (Sixth) • 7TH or VII (Seventh) • 8TH or VIII (Eighth) • 9TH or IX (Ninth)	Both	V5ANS
h.	20	-	Audit information / Renseignements de vérification	A string of letters and/or numbers that identifies when, where, and by whom a driver license/ID card was made. If audit information is not used on the card or the MRT, it must be included in the driver record.	Both	V25ANS

Data ref	On card reference	Zone placement	Data element/label	Definition	Card Type	Field Length/Type
i	-	Zone I	Issuing jurisdiction / Administration délivrante	The state, province, or territory responsible for the issuance of the DL/ID, and has the power to revoke or restrict the cardholder's driving and identification privileges. The appropriate two-character code in ANSI D20 must be used.	Both	F2A
j	-	Zone II	Under 18 Until	Date DL/ID cardholder turns 18 years old. Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
k	-	Zone II	Under 19 Until	Date DL/ID cardholder turns 19 years old. Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
l	-	Zone II	Under 21 Until	Date DL/ID cardholder turns 21 years old. Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
m	-	Zone II	Organ Donor	An indicator that denotes that the card holder is an organ donor. A red heart icon is required "♥". The issuer has the option of adding text – recommendation is for the words "ORGAN DONOR" to be used.	Both	Image and V20ANS

5   Quality Control

5.1   Quality Control Inspections

It is <u>highly recommended</u> that jurisdictions make regular quality control inspections of the DL/ID cards they are producing. These quality control inspections should continue throughout the life of the card production system. The production of DL/ID cards is essentially a manufacturing operation, and the need for effective quality control is the same as for any other manufacturing operation that seeks to produce a quality product.

5.2   Quality Control Guidelines

The following guidelines will help jurisdictions establish an effective quality control program:

Basic quality control testing. Ideally, basic quality control testing should be performed on every card produced. The purpose of this testing is to ensure that the cards conform to the design and includes all required elements (bar code, security devices, digital image, etc.) This could be as simple as a visual inspection prior to releasing

the card to the cardholder. In high volume printing operations, it may be necessary to use statistical sampling or automated quality control testing.

Comprehensive quality control testing. In addition, more comprehensive quality control testing should be conducted on a regular basis. This testing should determine that not only are the required design elements present but also that they perform as intended. This testing should include a check of the format of the data in the bar code and a test of bar code print quality.

Frequency of testing. The frequency of testing that is needed depends on the actual design of the card production system. At a minimum, testing of sample cards from each printer in operational use should be done on a weekly basis. It is the responsibility of the DMV to ensure testing is done. If the DMV hires a vendor to print the cards for them, then the DMV should ensure that quality control testing is required as part of the contract with the vendor.

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.

A.4 Functions

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 jurisdiction or country of issue as a DL/ID, the following apply:

A.5.1 Background color

Distinctly different colors should be used for the background of Zone 1 of the driver license and non-driver identification cards. The Zone 1 background color should be predominantly a high security color chosen to make copying or duplication of the document difficult. The background of Zone 1 may utilize any type of design. The use of the following colors for the background of Zone 1 is recommended, but not required:

- For DL documents, it is recommended that the background color of Zone 1 be predominantly a 30% tint of Pantone reference 198 as specified in ISO/IEC CD18013-1 for ISO Compliant Driver Licenses

- For ID cards, it is recommended that the background color be predominantly a 30% tint of Pantone reference 368

A.5.2 Portrait position

The reproduction of the portrait of the cardholder of the license shall be 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 standard to accommodate the needs of the many issuing jurisdictions. There are two principal formats – vertical (under 21, mandatory for US, optional for Canada) 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 the same for the two formats.

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

Portrait side

    Zones I, II and III

Non-portrait side

    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 and identification cards, the following options exist:

- DRIVING LICENSE

- DRIVING LICENCE (ISO-compatible)

- DRIVER LICENSE

- DRIVER'S LICENSE

- DRIVER LICENCE

- COMMERCIAL DRIVER'S LICENSE; COMMERCIAL DRIVER LICENSE; or CDL

- NONRESIDENT COMMERCIAL DRIVER'S LICENSE or NONRESIDENT CDL

- IDENTIFICATION CARD

The words "DRIVING LICENSE" or "DRIVER LICENSE" may be incorporated in the background graphic design of Zone I. The words may also be in French ("PERMIS de CONDUIRE"). NOTE: The term "driving licence" is used for compatibility with the ISO standard. If a version is to be used other than "license" or "licence," the jurisdiction must apply for an exception. You may also use a bilingual version of both French and the ISO compliant English. Other types of driving licenses may be indicated in the same manner, such as commercial driving licenses and instruction/learning permits.

Pursuant to Title 49 CFR Subpart J – Commercial driver's license document, §383.153 Information on the document and application, (a) All CDLs shall contain the following information: (a)(1) The prominent statement that the license is a "Commercial Driver's License" or "CDL," except as specified in §383.153(b).

(b) If the CDL is a Nonresident CDL, it shall contain the prominent statement that the license is a "Nonresident Commercial Driver's License" or "Nonresident CDL." The word "Nonresident" must be conspicuously and unmistakably displayed, but may be noncontiguous with the words "Commercial Driver's License" or "CDL."

For ID 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. The words may also be in French ("CARTE D'IDENTITÉ").

A.7.2.2   Issuing jurisdiction information

The name of the issuing jurisdiction must be included as text (full name or abbreviation).

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: **CAN**

A full list of issuing country codes may be obtained from ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes*.

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:

- Table 1/Ref. a. Family name (or concatenated Name)
- Table 1/Ref. b. Given name(s) (or concatenated Name)
- Table 2/Ref. g. Suffix (optional)
- Table 1/Ref. c. Date of birth
- Table 1/Ref. d. Date of issue
- Table 1/Ref. e. Date of expiry
- Table 1/Ref. f. Customer number
- Table 1/Ref. g. Document discriminator
- Table 1/Ref. i. Signature (unless in Zone III)
- Table 1/Ref. j. Cardholder address
- Table 1/Ref. k. Vehicle classifications (if codes are used, they should be explained in Zone IV; overflow information may be placed in Zone IV)
- Table 1/Ref. l. Vehicle restrictions and endorsements (if codes are used, they should be explained in Zone IV; overflow information may be placed in Zone IV)
- Table 1/Ref. n. Cardholder sex
- Table 1/Ref. o. Cardholder height
- Table 2/Ref. f. Cardholder weight (optional)
- Table 1/Ref. p. Cardholder eye color
- Table 2/Ref. h Audit information (optional)
- Table 2/Ref. a. Cardholder hair color (optional)
- Table 2/Ref. b. Cardholder place of birth (optional)
- Table 2/Ref. e. 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)
- Table 2/Ref. d. 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:

- Table 1/Ref. h. Portrait
- Table 1/Ref. i. Signature (May be in Zone II instead)

A.7.5 Zone IV

Zone IV contains the following:

- Explanations of codes used in Zone II categories, restrictions, and/or endorsements
- Overflow from categories, restrictions, and/or endorsements in Zone II
- Table 2/Ref. e. Date of expiry of each vehicle category (if used)
- Table 2/Ref. d. Date of first issue of each vehicle category (if used)
- Optical character recognition text & RFID for enhanced DL/ID (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 – details can be found in Annex D. Other optional machine-readable technologies may co-exist with the PDF417 2-dimensional bar code in Zone V. This standard contains additional details concerning how to use 3-track magnetic stripes, optical memory cards, and optical character recognition text & RFID for enhanced DL/ID. Issuing authorities wishing to implement other non-proprietary technologies, such as integrated circuit cards (also known as "smart cards") beyond how that technology is reflected for the enhanced DL/ID, are asked to work with AAMVA prior to implementation, so that future iterations of this standard will properly include these technologies to ensure 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. 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 Truncation of name

If information has to be truncated to fit in the available space then this is the way to do it. For all name fields, characters are eliminated from a field in the following order until the name fits into the field:
- Starting from the right and moving to the left, eliminate spaces adjacent to hyphens
- Starting from the right and moving to the left, eliminate apostrophes
- Starting from the right and moving to the left, eliminate any remaining characters, excluding:
  - Hyphens
  - Remaining spaces
  - Characters immediately following a hyphen or a space

For example, in the case where a person's middle names are "V'Erylongmiddlename01 V'Erylongmiddlename02 Marie - Louise" (58 characters), the truncation sequence will progress as follows:
- Remove spaces adjacent to hyphens, resulting in "V'Erylongmiddlename01 V'Erylongmiddlename02 Marie-Louise" (56 characters)

- Remove apostrophes, resulting in "VErylongmiddlename01 VErylongmiddlename02 Marie-Louise" (54 characters)
- Remove other characters as allowed, resulting in "VErylongmiddlename01 VErylongmi M-L" (35 characters)

A.7.8 Reproduction of images

A.7.8.1   Portrait

Measures shall be taken by the issuing authority to ensure that the digitally printed reproduction of the portrait of the cardholder 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 cardholder 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 cardholder with headgear, if the cardholder is a member of a religion requiring the wearing thereof and provided that the headgear does not present as an obstruction or present a shadow and render the portrait inadequate for the identification of the cardholder. Jurisdictions that incorporate facial recognition biometric technology may wish to ensure 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.

Orientation. 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 cardholder.

Lighting. 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).

Background. A uniform light blue color or white background shall be used to provide a contrast to the face and hair. Note: Preference is for uniform light blue color, such as Pantone 277 (though the specific Pantone color is not a requirement – a uniform light blue color or white background is a requirement).

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

Border. 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 cardholder, 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 cardholder 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.7.8.2   Signature

The signature of the cardholder 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.)
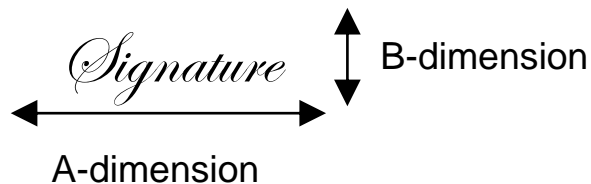
Figure A.1

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 reduced to a size where it is no longer a discernible representation of the original. The resulting signature must be a smooth representation of the original signature without such distortions such as stair stepping, stretching and/or squishing being apparent to the human eye.

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

Color. The digital reproduction of the signature shall be printed or laser engraved in definite contrast to the background color of the license. Either use a light signature on a dark background or a dark signature on a light background if printed. The ink of the signature must be printed entirely in the same shade or of a color, not varying shades (i.e., grey scale printing).

Borders. Borders or frames shall not be 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 cardholder 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.

A.9 DHS Compliance Indicators

The markings on both compliant and non-compliant cards should be secured in the same way that other personalization data on the card must be secured. For example, if the name and photo/image are secured using a high security overlay then the marking should also be secured by the security overlay.

A.9.1 Materially Compliant

The mark for Materially Compliant is a star.

Specifications

> • Printed on portrait side, in the top third of the DL/IDs, both landscape and portrait

> • Mark Size is .25 inch square

> • Mark Color is Gold Pantone 117 or CMYK equivalent: C: 0.0 M: 18.5 Y: 100.0 K: 15.0

A.9.2 Fully Compliant

The mark for Fully Compliant is a circle with a star cut out to reveal the background.

Specifications

> • Printed on portrait side, in the top third of the DL/IDs, both landscape and portrait

> • Mark Size is .25 inch square

> • Mark Color is Gold Pantone 117 or CMYK equivalent: C: 0.0 M: 18.5 Y: 100.0 K: 15.0

A.9.3 Non-Compliant Card

The text "NOT FOR REAL ID PURPOSES" or "NOT FOR FEDERAL IDENTIFICATION" is the marking for a Non-Compliant Card.

Specifications

> • The Non-Compliant text is on the portrait side of the DL/ID where portrait/personalization is captured

> • Printed in the top third of DL/IDs, both landscape and portrait

> • The Non-Compliant text is recommended in a font size of 9 points and an acceptable minimum of 7 points

> • The Non-Compliant text should be capitalized

> • The Non-Compliant text is set in a san serif font (straight line) such as Helvetica and Arial, and set **bold**.

> • The Non-Compliant text tracking* should be set to 100 based on a tracking unit of 1/1,000th of an em[7]. Tracking can be adjusted to fit and look.

> • It is suggested that the Non-Compliant text be placed above all personalization data

> • Recommend one space above and one space below text to separate words from other personalization on the card

*Tracking creates an even spacing between multiple characters in a line of text, widening out or tightening up.

A.10 DHS Limited Duration of Stay Document Indicator

States shall only issue a temporary or limited-term DHS Compliant DL/ID to an individual who has temporary lawful status in the United States. These cards should clearly indicate on their face and in the machine readable zone that they are temporary or limited-term DL/IDs compliant with DHS standards.

The temporary or limited-term compliant DL/ID should be marked on the portrait side with the phrase "Temporary" or "Limited-Term" within the top third of the card. The specified font is Helvetica Bold with a recommended font size of 9 points, however not less than a 7 points font in regular black ink. This phrase should be secured in the same way that other personalization data on the card is secured.

---

7 An em is a unit of measurement in the field of typography, equal to the point size of the current font.

Figure A.2: Portrait side of Horizontal DL/ID (not to scale)[8]
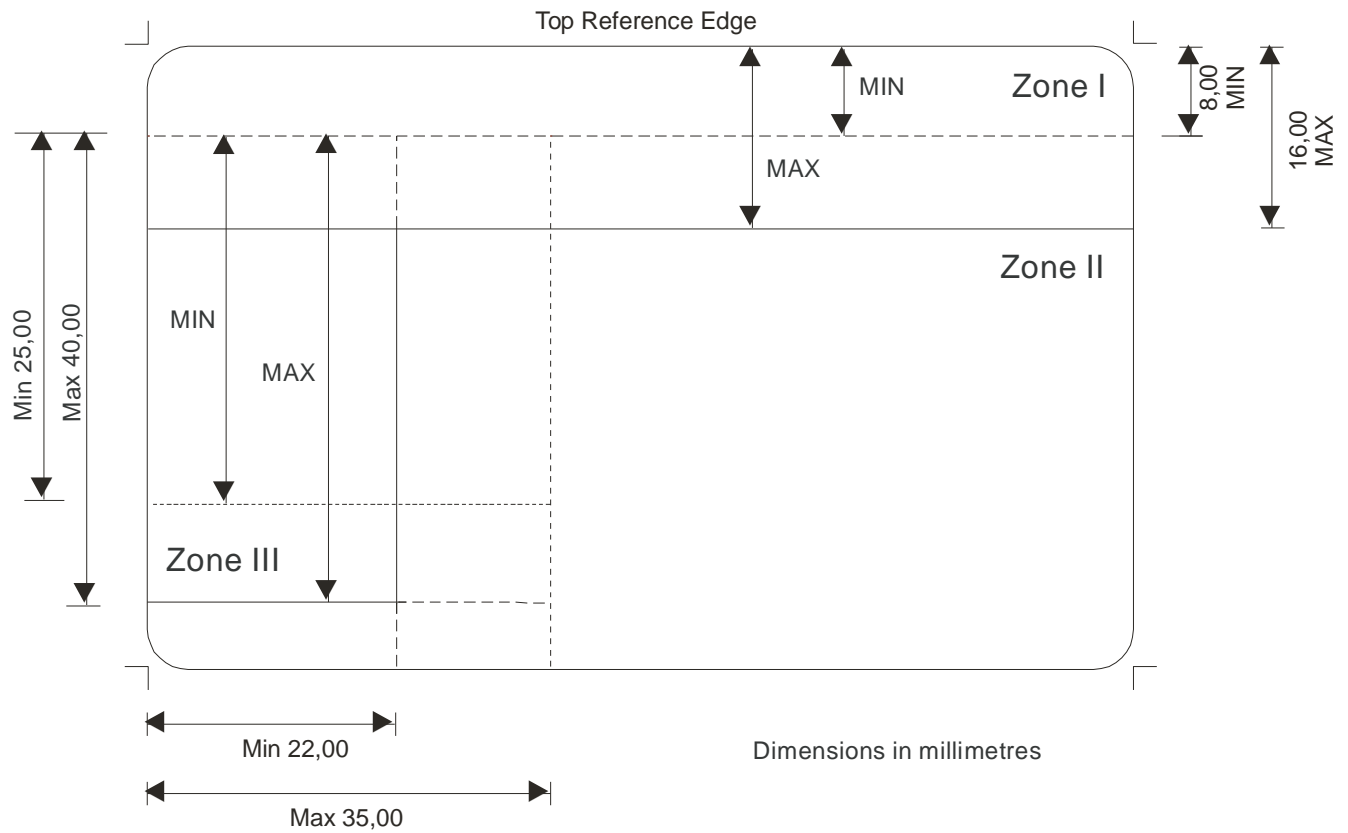
Top Reference Edge

Zone I

MIN

MAX

Zone II

8,00
MIN

16,00
MAX

Min 25,00

Max 40,00

MIN

MAX

Zone III

Min 22,00

Max 35,00

Dimensions in millimetres

Figure A.2.1: Horizontal DL/ID - Informative examples (not to scale) – intended to show what could be done within this standard. (See NOTE on page 27)

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

Zone I

MIN

MAX

8,00
MIN

16,00
MAX

Min 25,00

Max 40,00

MIN

MAX

Zone III

Dimensions in millimetres

Min 22,00

Max 35,00

Zone II

26
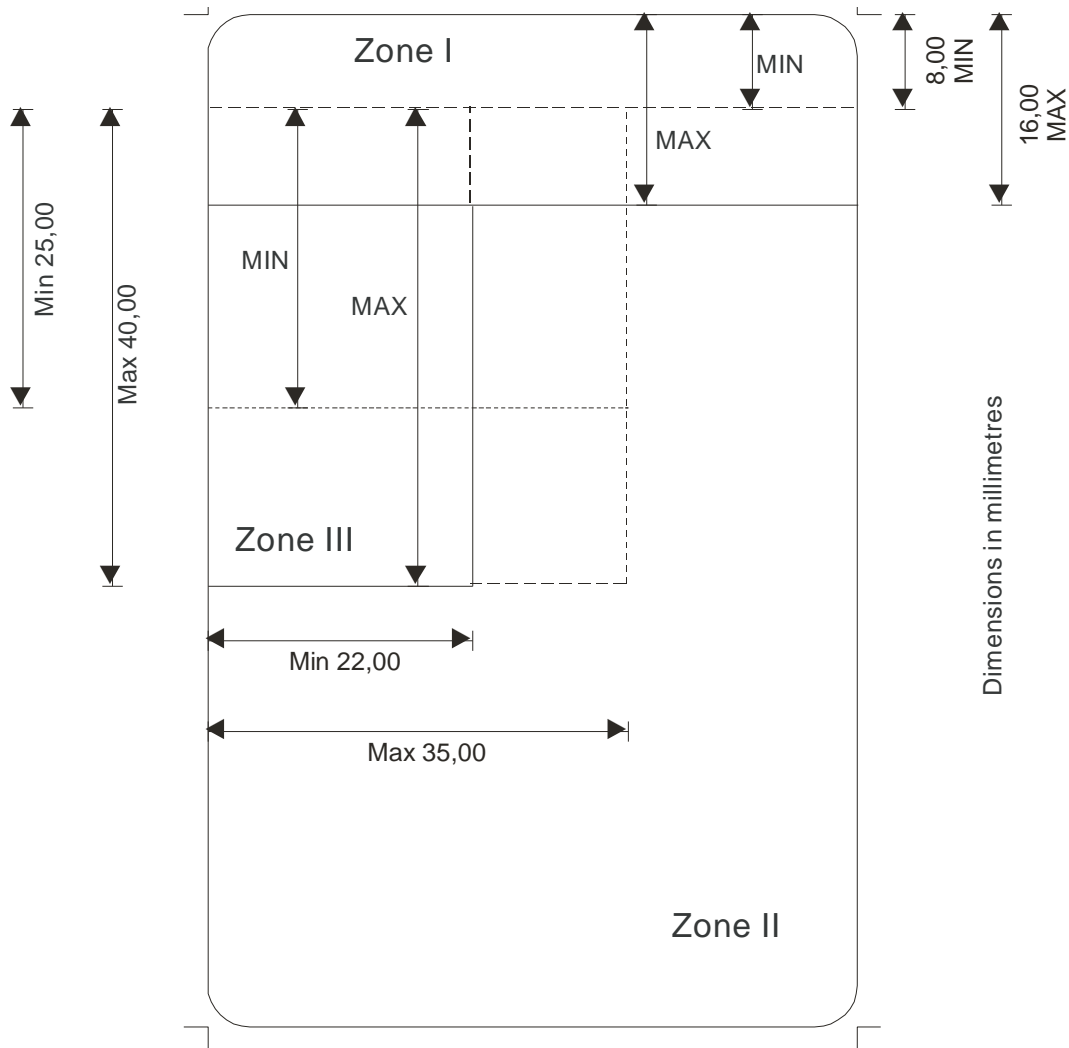
Figure A.3.1: Vertical DL/ID - Informative examples (not to scale) – intended to show what could be done within this standard
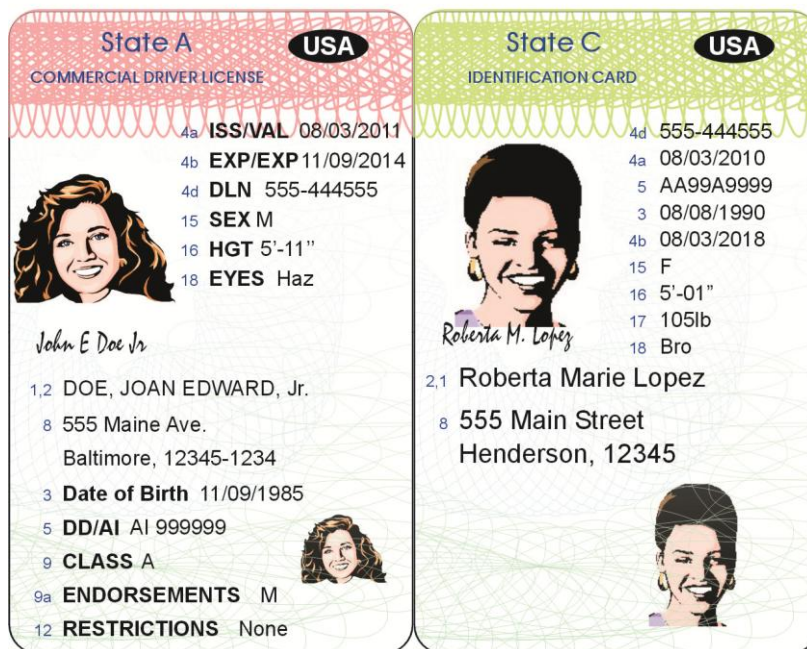
NOTE: The background colors in Zone 1 of the sample cards (which are specified as Pantone reference 198 and 368) may not appear as the true shade due to variations between individual monitors and printers on which they are viewed or printed. It is for this reason the Pantone reference numbers are used to specify the colors to be used on the actual cards.

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

Top Reference Edge

Max 38.1

**MAX AREA
FOR BARCODE**

Zone V

Zone IV

Dimensions in millimetres
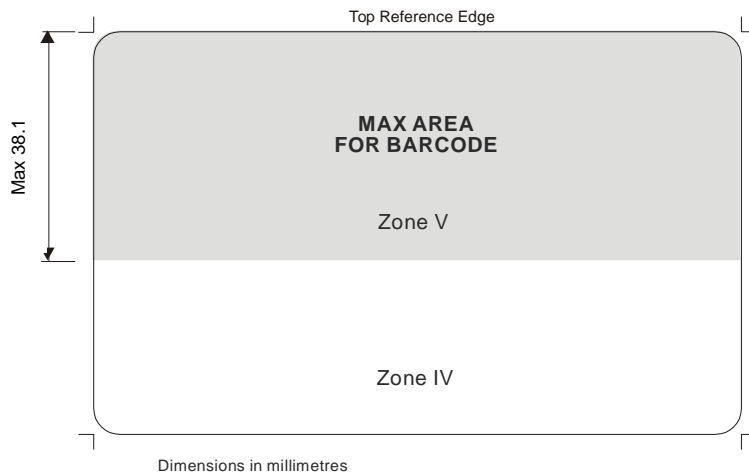
Figure A.4.1: Informative Example

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, and use appropriate vehicle class codes.

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

Top Reference Edge

MG-STRIPE OR OPTICAL MEMORY AREA
Zone V

Zone IV

BARCODE AREA
Zone V
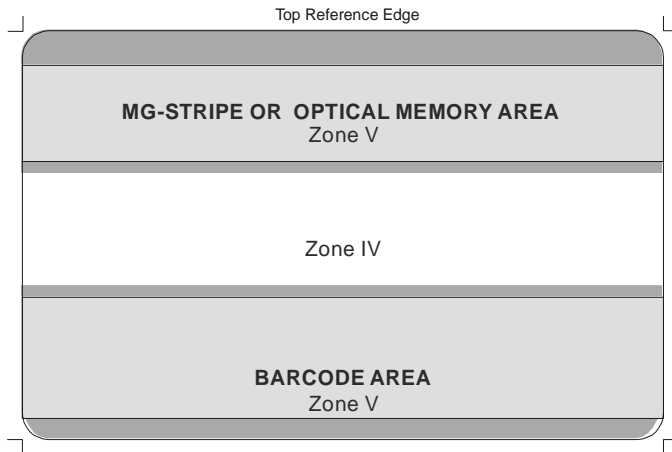
Figure A.6: Non-portrait side of Horizontal and Vertical DL/ID – integrated circuit with contacts

Top Reference Edge

Zone V

Zone IV
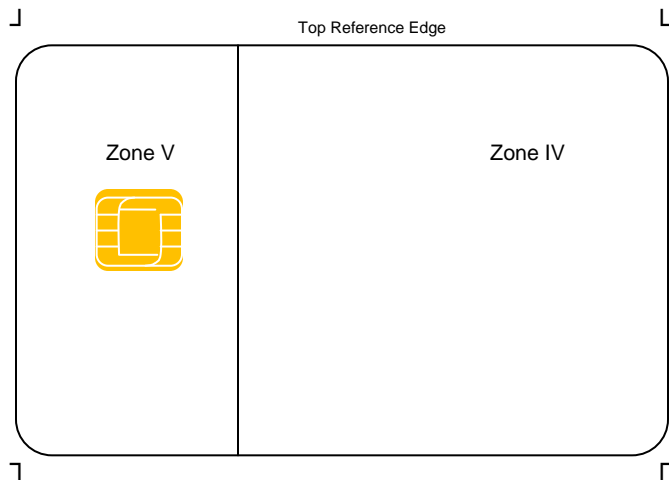
Annex B
(normative)

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.

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.2 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 cardholder.

Card core: The opaque or translucent inner layers of a card construction upon which the security pre-print 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 dye diffusion thermal transfer and color printing personalization methods, normally in the form of personalized data and images, and by digital printing devices to approximately represent the visible color spectrum and enable the printing of 'color portrait images'.

*Forger*y: 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(s) or feature that appear under a lens structure and whose appearance in color and/or design changes dependent upon tilting 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, biographical data, and other machine-readable features and technologies are applied to the card.

*Photo/Image-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 featur*e: 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 ensure 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.3 Basic Principles

B.3.1 Card Production

Production of DL/ID 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.3.2 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.3.3 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.3.4 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.3.5 Forensic 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 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 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 ensure 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 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/image/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.5 General Requirements

This standard 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 ensure 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.6 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. Note – that a number of security features are not compatible with each other or are available only on specific card structures or using certain personalization methods such as multiple Optically Variable Devices on a card, multiple UV inks in the same location on a card, Central Issue only features and Laser engraving features. Asking for all the features listed to be available on one Over the Counter and/or Central Issue card structure will create very real issues around real estate and security feature contention and/or overlap issues as well.

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.

B.6.1 Levels and Types

The DL/ID Security Device Index indicates coverage against various threat types at different levels of inspection (level 1 and level 2). Specifying the number of threats covered at level 1 and level 2 making sure that pre-print, personalization and lamina layers contain level 1 and level 2 features is an effective method to properly secure a card structure. The levels of inspection and threat types are as follows:

B.6.1.1   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.6.1.2   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.6.1.3   Level 3: third line inspection

Examination done at a forensic level and not specifically addressed by this standard.

B.6.1.4   Type 1: Counterfeit / simulation

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

B.6.1.5   Type 2: Alteration

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

B.6.1.6   Type 3: Photo / image and signature substitution

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

B.6.1.7   Type 4: Counterfeit from cannibalized cards

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

B.6.2 Minimum requirements

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

The minimum features mandated elsewhere in the card design standard (level 3 feature, document discriminator, 2D bar code,) 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 ensure 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 standard.

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.

Level 3 – A Level 3 security device supports third line inspection (as previously stated specifics for Level 3 are not covered in this standard).

C.3 Threat Types

Type 1 – Counterfeit/Simulation

Type 2 – Alteration

Type 3 – Photo/Image Substitution

Type 4 – Cannibalization

(Refer to Annex B.6.1 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			

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
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) A pattern of continuously fine lines constructed by using two or more lines in overlapping bands that repeat a lacy, web-like curve.		X	X	X	X	X	X	X	X
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 A lighter reproduction of the original image that appears in the same area as the personal data such that the image appears to be in the background and the personal data can still be read without interference.			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	

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
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 whose 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
k. Non standard type fonts Special type font that is not available on the commercial market and is reserved for security card use only.		X	X			X	X		
l. Rainbow printing Must demonstrate a controlled exacting color shift subtly in a linear continuous fashion. Accurately designed patterns cannot be easily copied or duplicated via scanning. It is applied using non-commercial method of printing. 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		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			X				X		

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.									
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 the viewing. Difficult to mimic the luster and hard to copy or scan.		X	X	X					
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. 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		
g. 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			
h. Thermochromatic Ink that exhibits a sharp, reversible color change when exposed to heat, i.e., finger rubbing or hot air.		X				X	X		

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
i. Ultraviolet fluorescence Invisible inks that emit visible color under exposure to ultraviolet light. Colors should 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 in paper, 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. Metalized DOVID (Diffractive Image) Opaque metalized DOVID (diffractive optically variable image device). OVD authentication effects cannot be photo copied, scanned or digitally recreated. OVD's are holographically mastered or digitally mastered using computer-guided lasers or electron beams.		X	X	X					
b. De-Metalized OVD (Diffractive Image) 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					
c. Transparent DOVID Transparent DOVID (diffractive optically variable image device). When incorporated into a driver license design, feature will not interfere with photo/image or data information. Transparent OVD authentication effects cannot be photo copied, scanned or digitally recreated. OVD's are holographically mastered or digitally mastered using computer-guided lasers or electron beams.		X	X	X					
d. Film - Color Shifting OVD Semi-transparent, multilayer light interference film creates noticeable, reflecting color shifts, i.e., clear to blue, magenta to blue, yellow to orange, etc. When incorporated into a driver license design, feature will minimally interfere with photo/image or data information. OVD color shifting effect cannot be photo copied, scanned or digitally recreated.		X	X	X					
e. Ink - Color Shifting OVD Printed opaque, multilayer light interference ink pigment creates 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.		X	X						
f. Liquid Crystal - Color Shifting OVD Semi-transparent, liquid crystal light interference layers create noticeable,		X	X	X					

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
reflecting color shifts, i.e., orange to green. When incorporated into a driver license design, feature will minimally interfere with photo/image or data information. OVD color shifting effect cannot be photo copied, scanned or digitally recreated.									
g. Personalized OVD OVD that is personalized for each card based upon biographical data, portrait, or signature of the cardholder.		X	X	X	X	X	X	X	X
h. Virtual Image OVD Transparent or semi-transparent virtual image appears to float above or sink below the surface of the document, as the viewing angle changes. When incorporated into a driver license design, feature will not interfere with photo/image or data information. OVD virtual image effect cannot be photo copied, scanned or digitally recreated.		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 Device – Readable and Storage Technology Unique individual Near IR or IR invisible data mark, 2-dimenional encrypted bar code, capable of storing independent information or details.						X	X	X	X
c. Covert variable pixel manipulation Covert dot matrix images that are converted to visible text with a special reader or lens.						X	X	X	X
d. Digital Seal A method of securing and validating data by electronic means using						X	X		X

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
digital signature technology. The issuing authority "signs" the information contained in the MRT.									
e. Embedded Image An image or information that is embedded or encoded within a primary visual image.						X	X	X	X
f. 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				
g. 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					
h. Laser engraving The information cannot be mechanically or chemically removed without surface damage to the card. Can be used for photo/images, characters, bar codes, OCR, etc.		X	X	X			X		
i. 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				
j. 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 machine or visual information.						X	X	X	X
k. 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
card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.									
l. 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
m. 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
n. 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				
o. 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
p. 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 fonts to further deter alteration.			X						
q. 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		LEVEL 1				LEVEL 2			
	Threat Type	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
r. 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
s. Thin film interference filters Multiple layer structures that produced color effects by interference.						X			
t. 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						

<div align="center">

Annex D
(normative)

Mandatory PDF417 Bar Code

</div>

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-2009 v1.0, Annex D – *Mandatory PDF417 Bar Code* (July, 2009).

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 standard 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 standard 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 standard.

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 2.5/6/660, where:

Recommended Print Quality grade 2.5 (B) at the point of printing the symbol before lamination and a Print Quality Grade of 1.5 (C) after lamination.

Measurement Aperture = 6 mil (0.060 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 ensure 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.

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 Annex E, Table E.1 (NCITS 322 5.10), 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 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
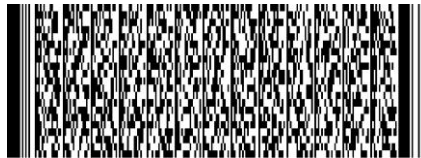
Plan for the maximum amount of data:

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 should be used when printing the symbol.

D.12 Data encoding structures

D.12.1 Structure Options

A compliant 2D symbol shall employ either the encoding structure set out in D.12.2 to D12.5 or the encoding structure set out in Annex I.

D.12.2 Overview

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 this 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.12.3 Header

Compliant 2D symbols must begin with a Fixed Header in the following format (Note: The number of bytes for each field is fixed and must be present. The numbers must be zero filled.):

<div align="center">Table D.1 — 2D symbols header format</div>

Field	Bytes (Fixed)	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.

Field	Bytes (Fixed)	Contents
6	6	**Issuer Identification Number (IIN)[9]:** This number uniquely identifies the issuing jurisdiction and can be obtained by contacting the ISO Issuing Authority (AAMVA). The full 6-digit IIN should be encoded.
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 AAMVA Card Design Specification version 1.0, dated 09-2003 shall be designated Version "02." All barcodes compliant with AAMVA Card Design Specification version 2.0, dated 03-2005 shall be designated Version "03." All barcodes compliant with AAMVA Card Design Standard version 1.0, dated 07-2009 shall be designated Version "04." All barcodes compliant with AAMVA Card Design Standard version 1.0, dated 07-2010 shall be designated Version "05." All barcodes compliant with this current AAMVA standard shall be designated "06". 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 standard, 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.

---

[9] http://www.aamva.org/KnowledgeCenter/Standards/Current/INNnumbers.htm

D.12.4 Subfile Designator

All compliant 2D bar code symbols must contain the "DL" or "ID" subfile structure as defined below immediately after the Header as defined in D.12.1. The subfile designator is a fixed element, as well as the number of bytes, and the numbers must be zero-filled. All sub file headers must follow one another.

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 subfile type and "ID" is the subfile type for non-DLs 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. In the case of a jurisdiction-defined subfile that has a first letter that could be more than one jurisdiction (e.g. California, Colorado, Connecticut) then other data, like the IIN or address, must be examined to determine the jurisdiction.
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. Each subfile must begin with the two-character Subfile Type and these two characters must also be included in the length.

D.12.5 Data elements

Tables D.3 and D.4 define mandatory and optional data elements that are accommodated in the "DL" and "ID" subfile types. 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 jurisdictions name. 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, Z*VB, 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, "unavl" is to be encoded.

D.12.5.1 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). **Use of padding for variable length fields is optional.**

Table D.3 – 2D Mandatory data elements

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	V6ANS
b.	DCB	Jurisdiction-specific restriction codes	Jurisdiction-specific codes that represent restrictions to driving privileges (such as airbrakes, automatic transmission, daylight only, etc.).	DL	V12ANS
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. (MMDDCCYY for U.S., CCYYMMDD for Canada)	Both	F8N

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
e.	DCS	Customer Family Name	Family name of the cardholder. (Family name is sometimes also called "last name" or "surname.") Collect full name for record, print as many characters as possible on portrait side of DL/ID.	Both	V40ANS
f.	DAC	Customer First Name	First name of the cardholder.	Both	V40ANS
g.	DAD	Customer Middle Name(s)	Middle name(s) of the cardholder. In the case of multiple middle names they shall be separated by a comma ",".	Both	V40ANS
h.	DBD	Document Issue Date	Date on which the document was issued. (MMDDCCYY for U.S., CCYYMMDD for Canada)	Both	F8N
i.	DBB	Date of Birth	Date on which the cardholder was born. (MMDDCCYY for U.S., CCYYMMDD for Canada)	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" = "073 in"
			Centimeters (cm): number of centimeters followed by " cm"
			  ex. 181 centimeters="181 cm"
				Both	F6AN

m.	DAG	Address – Street 1	Street portion of the cardholder address.	Both	V35ANS
n.	DAI	Address – City	City portion of the cardholder address.	Both	V20ANS
o.	DAJ	Address – Jurisdiction Code	State portion of the cardholder address.	Both	F2A

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
p.	DAK	Address – Postal Code	Postal code portion of the cardholder address in the U.S. and Canada. If the trailing portion of the postal code in the U.S. is not known, zeros will be used to fill the trailing set of numbers up to nine (9) digits.	Both	F11AN
q.	DAQ	Customer ID Number	The number assigned or calculated by the issuing authority.	Both	V25ANS
r.	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
s.	DCG	Country Identification	Country in which DL/ID is issued. U.S. = USA, Canada = CAN.	Both	F3A
t.	DDE	Family name truncation	A code that indicates whether a field has been truncated (T), has not been truncated (N), or – unknown whether truncated (U).	Both	F1A
u.	DDF	First name truncation	A code that indicates whether a field has been truncated (T), has not been truncated (N), or – unknown whether truncated (U).	Both	F1A
v.	DDG	Middle name truncation	A code that indicates whether a field has been truncated (T), has not been truncated (N), or – unknown whether truncated (U).	Both	F1A

D.12.5.2 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. Use of padding for variable length fields is optional.

Table D.4 – 2D Optional data elements

Data Ref.	Element 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	Bald, black, blonde, brown, gray, red/auburn, sandy, white, unknown. If the issuing jurisdiction wishes to abbreviate colors, the three-character codes provided in ANSI D20 must be used.	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. If audit information is not used on the card or the MRT, it must be included in the driver record.	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. (DHS recommended field)	Both	V25ANS
f.	DBN	Alias / AKA Family Name	Other family name by which cardholder is known.	Both	V10ANS
g.	DBG	Alias / AKA Given Name	Other given name by which cardholder is known	Both	V15ANS

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
h.	DBS	Alias / AKA Suffix Name	Other suffix by which cardholder is known	Both	V5ANS
i.	DCU	Name Suffix	Name Suffix (If jurisdiction participates in systems requiring name suffix (PDPS, CDLIS, etc.), the suffix must be collected and displayed on the DL/ID and in the MRT). Collect full name for record, print as many characters as possible on portrait side of DL/ID. • JR (Junior) • SR (Senior) • 1ST or I (First) • 2ND or II (Second) • 3RD or III (Third) • 4TH or IV (Fourth) • 5TH or V (Fifth) • 6TH or VI (Sixth) • 7TH or VII (Seventh) • 8TH or VIII (Eighth) • 9TH or IX (Ninth)	Both	V5ANS
j.	DCE	Physical Description – Weight Range	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.	Elem-ent ID	Data Element	Definition	Card type	Length / type
k.	DCL	Race / ethnicity	Codes for race or ethnicity of the cardholder, as defined in ANSI D20.	Both	F3A
l.	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
m.	DCN	Standard endorsement code	Standard endorsement code(s) for cardholder. See codes in D20. This data element is a placeholder for future efforts to standardize endorsement codes.	DL	F5AN
n.	DCO	Standard restriction code	Standard restriction code(s) for cardholder. See codes in D20. This data element is a placeholder for future efforts to standardize restriction codes.	DL	F12AN
o.	DCP	Jurisdiction-specific vehicle classification description	Text that explains the jurisdiction-specific code(s) for classifications of vehicles cardholder is authorized to drive.	DL	V50ANS
p.	DCQ	Jurisdiction-specific endorsement code description	Text that explains the jurisdiction-specific code(s) that indicates additional driving privileges granted to the cardholder beyond the vehicle class.	DL	V50ANS
q.	DCR	Jurisdiction-specific restriction code description	Text describing the jurisdiction-specific restriction code(s) that curtail driving privileges.	DL	V50ANS
r.	DDA	Compliance Type	DHS required field that indicates compliance: "M" = materially compliant; "F" = fully compliant; and, "N" = non-compliant.	Both	F1A
s.	DDB	Card Revision Date	DHS required field that indicates date of the most recent **version** change or modification to the visible format of the DL/ID (MMDDCCYY for U.S., CCYYMMDD for Canada)	Both	F8N

Data Ref.	Elem-ent ID	Data Element	Definition	Card type	Length / type
t.	DDC	HAZMAT Endorsement Expiration Date	Date on which the hazardous material endorsement granted by the document is no longer valid. (MMDDCCYY for U.S., CCYYMMDD for Canada)	DL	F8N
u.	DDD	Limited Duration Document Indicator	DHS required field that indicates that the cardholder has temporary lawful status = "1".	Both	F1N
v.	DAW	Weight (pounds)	Cardholder weight in pounds Ex. 185 lb = "185"	Both	F3N
w.	DAX	Weight (kilograms)	Cardholder weight in kilograms Ex. 84 kg = "084"	Both	F3N
x.	DDH	Under 18 Until	Date on which the cardholder turns 18 years old. (MMDDCCYY for U.S., CCYYMMDD for Canada)	Both	F8N
y.	DDI	Under 19 Until	Date on which the cardholder turns 19 years old. (MMDDCCYY for U.S., CCYYMMDD for Canada)	Both	F8N
z.	DDJ	Under 21 Until	Date on which the cardholder turns 21 years old. (MMDDCCYY for U.S., CCYYMMDD for Canada)	Both	F8N
a.a.	DDK	Organ Donor Indicator	Field that indicates that the cardholder is an organ donor = "1".	Both	F1N

D.12.5.3 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.

D.13   Example of raw PDF417 data

The following represents the data stream of a compliant PDF417 bar code. For this example Virginia was chosen and the IIN found in the header; the jurisdiction specific classification, restriction, endorsement codes; address jurisdiction; and jurisdiction specific field use data as though it was a Virginia document.

@$^{L}_{F}$ $^{R}_{S}$ $^{C}_{R}$

ANSI 636000060002DL00410278ZV03190008DLDAQT64235789$^{L}_{F}$

DCSSAMPLE^L_F

DDEN^L_F

DACMICHAEL^L_F

DDFN^L_F

DADJOHN^L_F

DDGN^L_F

DCUJR^L_F

DCAD^L_F

DCBK^L_F

DCDPH^L_F

DBD06062008^L_F

DBB06061986^L_F

DBA12102012^L_F

DBC1^L_F

DAU068 in^L_F

DAYBRO^L_F

DAG2300 WEST BROAD STREET^L_F

DAIRICHMOND^L_F

DAJVA^L_F

DAK232690000 ^L_F

DCF2424244747474786102204^L_F

DCGUSA^L_F

DCK123456789^L_F

DDAM^L_F

DDB06062008**^L_F**

DDC06062009**^L_F**

DDD1^C_R

ZVZVA01^C_R

Header Fields:
- Compliance Indicator: **@**
- Data Element Separator: Line Feed character (**^L_F**)
- Record Separator: Record Separator character (**^R_S**)
- Segment Terminator: Carriage Return character (**^C_R**)
- File Type: **'ANSI ' (Note: ANSI followed by a SPACE).**
- Issuer Identification Number (IIN): 6-digit IIN: **'636000'**
- AAMVA Version Number: **'06'**
- Jurisdiction Version Number: **'00'**
- Number of Entries: **'02'** (numeric value for # of sub-files in the barcode)

Sub-file Designator:
- Sub-file Type: **DL** – DL data
- Offset: **0041**
- Length: **0278**
- Sub-file Type: **ZV** – Jurisdiction Specific data
- Offset: **0319**
- Length: **0008**

Mandatory Fields:
- Customer Number - **DAQ**
- Family Name - **DCS**
- Family Name Truncation - **DDE**
- First Names – **DAC**
- First Names Truncation - **DDF**
- Middle Names **- DAD**
- Middle Names Truncation - **DDG**
- Virginia Specific Class - **DCA**
- Virginia Specific Restrictions - **DCB**
- Virginia Specific Endorsements - **DCD**
- Issue Date - **DBD**
- Date of Birth - **DBB**
- Expiration Date - **DBA**
- Sex - **DBC**
- Height - **DAU**
- Eyes - **DAY**
- Address - **DAG**
- City - **DAI**
- State - **DAJ**
- Zip – **DAK**
- Document Discriminator - **DCF**

- Country/territory of issuance - **DCG**

Optional Fields:
- Suffix - **DCU**
- Inventory Control Number – **DCK (Recommended for DHS compliant licenses)**
- Compliance Type (ex. "M" = materially compliant) – **DDA (Required for DHS compliant licenses)**
- Card Revision Date – **DDB (Required for DHS compliant licenses)**
- HazMat Endorsement Expiry Date – **DDC**
- Limited Duration Document Indicator – **DDD (Required for DHS compliant licenses)**

Jurisdiction Specific Fields:
- Court Restriction Code(s) – **ZVA**

Annex E
(informative)

Optional Card Test Methods

E.1 Introduction

Issuing authorities need an indication of a card's durability and resistance to compromise. A variety of tests are available to estimate these qualities. However, not all tests are applicable to all card types or to all card use environments.

This annex provides guidance specifically on test selection as well as on the broader card durability and integrity assessment process.

Note that durability tests in general do not provide a guarantee that a particular card will last for a specific amount of time. Test results only provide a means of ranking or comparing one card structure to another.

E.2 Scope

This annex covers the following:

- The purpose and applicability of a range of standardized card durability tests.

- Guidelines for conducting a card durability assessment.

- Notes on assessing card integrity.

E.3 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.4 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 INCITS 322-2008, *Card durability test methods*

ISO/IEC 10373-1:2006, *Identification cards - Test methods - General characteristics*

E.5 Terms and definitions

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

E.5.1 Card service life

period of time between card issuance and expiration date

E.6 Durability testing

E.6.1 Card evaluation process

The card evaluation process consists of the following steps:

1. Define the environment within which cards will be used, and the related durability requirements. Also document the card properties known at this point. (See E.6.2.)

2. Identify card tests that are appropriate, given the use environment, durability requirements and known card properties. (See E.6.3, E.6.4 and E.6.5.)

3. Determine the relative importance of each test. (See E.6.6.)

4. Conduct card tests and rank results. (See E.6.7.)

E.6.2 Card use environment and durability requirements

Each issuing authority's needs in respect of card durability are unique. The following general requirements can be adapted to an issuing authority's needs:

> The materials and manufacturing process used for the production of DL/ID cards shall be of such a quality that a DL/ID card shall stay intact and shall not delaminate, deform, chip, tear, disintegrate or become illegible or otherwise dysfunctional under conditions of normal wear and tear from the point where it is produced until the expiry of the validity period of the DL/ID card. In particular, all details, including the photograph/image, signature images, machine-readable data and security features, shall not fade, and shall remain clearly legible/readable/distinguishable for the validity period of the DL/ID card.

As with the general requirements, conditions of normal wear and tear will be differ between issuing authorities. The list below can be used as basis to compile issuing-authority specific conditions:

1. Carrying a DL/ID card in a wallet, or loose in a pocket (along with keys or coins), in all weather conditions, for 12 hours at a time, on a daily basis, including in dusty, dirty and gritty environments.

2. Leaving a DL/ID card in a motor vehicle on the dashboard, during which time it could daily be subject to direct sunlight and high temperatures (up to 90°C) for a continuous period of up to one month.

3. Leaving a DL/ID card in a motor vehicle at night in cold conditions, during which time it could be subject to temperatures as low as -5°C, followed by an increase in temperature up to 20°C (when the vehicle is in use again), associated with manual handling of the DL/ID card (at any temperature).

4. Leaving a DL/ID card in a piece of clothing during which time it will be subject to water with high temperatures, washing and abrasion (e.g. in a washing machine or dryer) and/or dry cleaning chemicals.

5. Occasional exposure to the following:

    a. Water, rain, hail and snow.

    b. Matter such as mud, oil, grease and fuel.

    c. Magnetic fields.

    d. X-Rays.

E.6.3 Standardized tests

Table E.1 discusses various tests that can be used to get an indication of a card's durability properties. For each test, the following is provided:

- A reference to the standards document (and clause within such document) that specifies the test. "ANSI 322" refers to ANSI INCITS 322-2002, *Card durability test methods*, and "ISO" refers to ISO/IEC 10373-1:2006, *Identification cards - Test methods - General characteristics*.

- The name of the test

- The "answer" (output) provided by the test.

- Notes providing additional information on the test and its use.

- An indication of whether the test is recommended for testing DL/ID cards and the machine-readable features of the card.

- The suggested method by which the outcome of the tests of different cards can be compared (this is used within the context of E.6.7).

Table E.1 — Standardized card tests

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ANSI 322 5.1	Delamination – 180°	Force required to separate layers.	In general does not apply to cards with only heat transfer film layers. The force required in the 180° test typically is twice the	Yes	Rank cards according to force required to separate layers.
ANSI 322 5.2	Delamination – 90°	Force required to separate layers.	force required in the 90° test. Recent experience by card testers indicated that for driver license cards the material almost always tears before the bonding layer. In practice, these tests are mostly applicable to credit cards. Also noteworthy is that the adhesive used to secure a card to the test rig for the 90° test sometimes gives way before either the card material or bonding does. In the 180° test, clamps can be used in addition to the adhesive. In light of the above, it is recommended that the 180° test be performed first, and that the 90° test be performed only if in the 180° test the bonding (and not the material) failed.	Conditional (see notes)	Rank cards according to force required to separate layers.

---

[10] Each card is awarded a score out of a maximum of 10 points (10 being best and 0 being worst). Scores should reflect not only the order of preference, but also how much better (or worse) one card is than another.

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ANSI 322 5.3	Delamination – cross hatch tape test	Rating from 0 (more than 65% removal of film) to 5 (no removal of film).	Specifically intended for heat transfer film layers. The test may however also have applicability where a patch (such as the AAMVA security device) is applied to a polycarbonate card. Note that film layers/patches thicker than 1mil typically tend to be difficult to prepare for the test due to corner tearing.	Yes	Rank cards according to rating.
ANSI 322 5.4	ID-1 Card flexure	Number of flex cycles (up to 100,000) until fracture.	Driving licenses typically go to 100,000 cycles without fracture; some polycarbonate cards may fracture before then.	Yes	Rank cards according to number of flex cycles
ANSI 322 5.5	ID-1 Card static stress	Number of cards tested and number of cards fractured.		Yes	Rank cards according to number of cards fractured
ANSI 322 5.6	ID-1 Card stress and plasticizer exposure	Time until a fracture of 13mm has occurred.	Plasticizer dioctylphthalate (DOP) used. This substance poses a health hazard.	Yes	Rank cards according to time until 13mm fracture
ANSI 322 5.7	Impact resistance	Energy required to start a crack.	Primarily intended to determine embossing properties of a card.	No	

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ANSI 322 5.8	Elevated temperature and humidity exposure	Standard output: Description of any deterioration observed. Additional output: Dimensional and card warpage.	This is the first part of the "card structure integrity test sequence" (ANSI 322 6), except that the temperature is higher (71°C instead of 60°C) in the card structure integrity test sequence. This test can also be used as an alternative to ISO/IEC 10373-1 5.5 (card dimensional stability and warpage with temperature and humidity), which implies that dimensional and card warpage information (observed at the end of the test) should form part of the test output.	Yes	Rank cards according to observed deterioration, and dimensional and card warpage
ANSI 322 5.9	Surface abrasion	Number of cycles until wear-through of card feature is observed, or 5,000 cycles, whichever comes first.	Proposed use is on the portrait side of the cards being tested.	Yes	Rank cards according to number of cycles, and then according to observed degradation.

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ANSI 322 5.10	Bar code abrasion (1D)	Number of cycles until ANSI grade F is reached, or ANSI grade (A, B, C, or D) after 5,000 cycles.	Test is currently limited to cards with one-dimensional bar codes. It is recommended that the test be amended to measure the barcode in accordance with ISO/IEC 15415. Card vendors should be required to include a PDF417 barcode on the card that contains realistic information, and of which the position is standardized (i.e. the barcode position does not have to be standardized in the test description). (It is recognized that the eventual position and size of the barcode on the card may change prior to production. Consequently, it will be necessary to re-perform this test at the commencement of production (on sample cards) to establish a new baseline.	Only if the card has a bar code	Rank cards according to ISO overall symbol grade
ANSI 322 5.11	Magnetic stripe abrasion		Limited to cards with magnetic stripes.	Only if the card has a magnetic stripe	
ANSI 322 5.12	Image abrasion	Standard output: Number of Taber cycles (up to 5,000) until reflection density drops below 50% of its original value for each of the colors (C, M, Y, K, CB). Alternative output: Number of Taber cycles (up to 5,000) until "breakthrough"	Requires color dots with specific colors in specific locations (along the path of the Taber abrader wheel). This test essentially measures firstly the impact on readability (as soon as the abrader starts to scratch the surface of the card), and secondly the resistance of the layers above any printing to abrasion (up to the point where the printing is scratched off). It is postulated that the image abrasion test (as specified) has some drawbacks in the driver license environment. If a personalized (color) portrait image is	Yes	Rank cards according to number of cycles, and then according to observed degradation.

Reference	Test name	Output	Notes	Recommended	Assessment[10]
		occurs (see Notes).	overlaid by a separate security layer, the DL/ID card becomes compromised as soon as the security feature becomes compromised, which may be long before the portrait image itself becomes unreadable. Measuring the reflection density of an image (or of standard dots) thus would not be a true reflection of a DL/ID card's resistance to abrasion. It is suggested that the test be changed to become an integrity abrasion test. A DL/ID card's integrity becomes compromised as soon as any security layer, security feature or personalization shows "breakthrough" (i.e. becomes scratched off to the extent that the material beneath the feature becomes visible without impediment). The number of Taber cycles until "breakthrough" is measured. Cards are positioned on the abrader to that the security feature/personalization that extends the least into the depth of the card lies under the path of the abrader wheels. This position is based in information provided by the Vendor. (It is important to always keep in mind that this test should not be used in isolation, and that the intrinsic security value of security features should be weighed against any associated durability weaknesses.)		
ANSI 322 5.13	Temperature and humidity induced dye migration	Percentage increase in reflectivity for each of the colors (C, M, Y, K).	Requires a preprinted test pattern (i.e. a regular DL/ID sample card will not suffice), and is intended specifically for dye diffusion printed information (such as is rendered by a dye sublimation printer).	Yes	Rank cards according to percentage increase in reflectivity

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ANSI 322 5.14	Plasticizer induced dye migration	Time until edge contrast of test pattern falls to 75% of its original value.	Requires a preprinted test pattern (i.e. a regular DL/ID sample card will not suffice), and is intended specifically for dye diffusion printed information (such as is rendered by a dye sublimation printer).	Yes	Rank cards according to time
ANSI 322 5.15	Ultraviolet light exposure	A description of deterioration and discoloration observed.		Yes	Rank cards according to observed deterioration and discoloration
ANSI 322 5.16	Daylight exposure image stability – Xenon arc	Percentage change in color density as well as other test parameters. Alternative output: A description of deterioration and discoloration observed (see Notes).	Requires a preprinted test pattern (i.e. a regular DL/ID sample card will not suffice). It is suggested to conduct this test without the preprinted test pattern, and to use as output a description of deterioration and discoloration observed (similar to the output of ANSI 322 5.15).	Yes	Rank cards according to observed deterioration and discoloration
ANSI 322 5.17	Laundry test	Description of any observed defects.		Yes	Rank cards according to observed defects
ANSI 322 5.18	Embossed character retention – pressure		In general not applicable to driver licenses. Tactile features on DL/ID cards can be assessed primarily via ANSI 322 5.12 (wet abrasion and impact test), as well as via the amended version of ANSI 322 5.12 (image abrasion test).	No	

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ANSI 322 5.19	Embossed character retention – heat		In general not applicable to driver licenses. Tactile features on DL/ID cards can be assessed primarily via ANSI 322 5.12 (wet abrasion and impact test), as well as via the amended version of ANSI 322 5.12 (image abrasion test).	No	
ANSI 322 5.20	Corner impact test	Description of any delamination or fracture that occurred.		Yes	Rank cards according to number of fractured/delaminated cards.
ANSI 322 5.21	Wet abrasion and impact	Description of the extent to which any delamination occurred.	For sequential testing, it is recommended that the test be amended by adding a specified number of coins (spread evenly across the denominations) to the paint shaker, in order to better reflect actual conditions.	Yes	Rank cards according to observed delamination.
ANSI 322 5.22	IC Card with contacts micromodule adhesion	Peak force achieved.	Limited to integrated circuit cards with contacts.	Only if the card contains an integrated circuit with contacts.	Rank cards according to peak force achieved.
ISO/IEC 10373-1 5.9	Dynamic torsional stress	Testable functional (i.e. machine-readable technology intact) or not.	Primarily aimed at cards with integrated circuits.	Only if the card contains an integrated circuit.	Rank cards according to number of cards testably functional.
ISO/IEC 10373-1 5.1	Card warpage	Warpage value.		Yes	Not used in evaluation. Used to identify serious defects and as reference for future testing.

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ISO/IEC 10373-1 5.2	Dimensions of cards	Standard output: Card dimensions. Additional output: Height profile of any tactile features.		Yes	Not used in evaluation. Used to identify serious defects and as reference for future testing.
ISO/IEC 10373-1 5.3	Peel strength	Peel strength.	This test is similar to the Delamination – 90° test specified in ANSI NCITS 5.2.	No	
ISO/IEC 10373-1 5.4	Resistance to chemicals.	Description of effects.	According to experts involved in the drafting process, this test was included to preclude the use of any card other than a plastic card (e.g. cardboard or metal) for use in the banking industry. The tests prescribed nevertheless include common chemicals that could be encountered in day-to-day use, and hence this test should be performed.	Yes	Rank cards according to observed effects
ISO/IEC 10373-1 5.5	Card dimensional stability and warpage with temperature and humidity	Card dimensions and card warpage.	ANSI 322 5.8 (being a much harsher test), with the addition of dimensional measurements as output, should be used instead.	No	
ISO/IEC 10373-1 5.6	Adhesion or blocking	Description of any visible signs of deterioration.	Used primarily by equipment manufacturers to establish suitability of cards for production processes.	No	

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ISO/IEC 10373-1 5.7	Bending stiffness	Deflection distance.	The primary purpose of this test is to allow cards to bend sufficiently to allow magnetic stripes to be affixed during the production process. This test was introduced to the ISO specification after it was decided to remove any (stated) requirement that card material should be "plastic".	No	
ISO/IEC 10373-1 5.8	Dynamic bending stress	Testable functional (i.e. machine-readable technology intact) or not.	This test is similar to the ID-1 Card flexure test specified in ANSI NCITS 5.4, although performed with a different frequency.	No	
ISO/IEC 10373-1 5.10	Opacity		Not applicable to the DL/ID environment.	No	
ISO/IEC 10373-1 5.11	Ultraviolet light	Testable functional (i.e. machine-readable technology intact) or not.	This test is intended primarily for integrated circuit cards (the lamp used is similar to lamps used in the earlier days of personal computers when EPROMS could be erased using an ultraviolet light).	No	
ISO/IEC 10373-1 5.12	X-rays	Testable functional (i.e. machine-readable technology intact) or not.	This test is intended primarily for integrated circuit cards.	Only if the card contains an integrated circuit.	Rank cards according to number of cards testably functional.
ISO/IEC 10373-1 5.13	Static magnetic fields	Testable functional (i.e. machine-readable technology intact) or not.	This test is intended primarily for integrated circuit cards.	Only if the card contains an integrated circuit.	Rank cards according to number of cards testably functional.

Reference	Test name	Output	Notes	Recommended	Assessment[10]
ISO/IEC 10373-1 5.14	Embossing relief height of characters	Value of overall relief height	This test is intended primarily for bank cards.	No	
ISO/IEC 10373-1 5.15	Resistance to heat	Maximum deflection and a description of any discoloration or delamination.	Similar to the elevated temperature and humidity exposure test specified in ANSI NCITS 5.8, except that the cards are subjected to forced deflection during exposure, and that the exposure period is shorter.	No	
ISO/IEC 10373-1 5.16	Surface distortions and raised areas		Not applicable to the DL/ID environment.	No	

In addition to the above standardized tests, the following two tests can be useful:

- Dry-cleaning test. The probability of cards being subjected to accidental dry-cleaning is real, and the chemicals used in the process may have a detrimental effect on a card. The test is conducted by putting cards in a laundry bag (made of woven fabric, i.e. not plastic or other similar impervious material), each card in a separate pocket (i.e. such that cards will not directly touch each other during the cleaning process), and sending the bag to an approved commercial dry cleaner with the instruction to dry clean. Cards are ranked according to observed defects. Each card is awarded a score out of a maximum of 10 points (10 being best and 0 being worst). Scores should reflect not only the order of preference, but also how much better (or worse) one card is than another. Note that this test is non-repeatable, and that the results should be used only to compare cards that were part of the same batch.

- Cold test. DL/ID cards are often exposed to cold conditions (e.g. overnight in a vehicle, or when used as an ice scraper), hence the applicability of this test. Cards are placed under mechanical stress (as per ANSI 322 5.5) inside a temperature controlled chamber set at -5°C for 24 hours. Upon opening the chamber, the opening is draped (to keep the cold inside) while trying to snap the cards with an impactor (in accordance with ANSI 322 5.5). Cards are ranked according to the number of cards fractured.

E.6.4 Matching tests to requirements

In order to assist in determining the relative importance of tests found to be applicable, the tests and requirements are matched up to each other in a table such as Table D.2. The table matches the conditions listed in E.6.2 to the tests that may be applicable to all cards. An issuing authority will draft its own version of this table.

Table D.2 — Matching to standardized card tests

Conditions	ANSI														ISO/IEC	Dry-cleaning test	Cold test
	5.1	5.3	5.4	5.5	5.6	5.8	5.9	5.10	5.12	5.15	5.16	5.17	5.20	5.21	5.4		
A person carrying a DL/ID card in a wallet, or loose in a pocket (along with keys or coins), in all weather conditions, for 12 hours at a time, on a daily basis, including in dusty, dirty and gritty environments.		x	x	x	x	x	x	x	x				x	x			
Leaving a DL/ID card in a motor vehicle on the dashboard, during which time it could be subject to direct sunlight and high temperatures (up to 90°C) for a continuous period of up to one month.						x				x	x						
Leaving a DL/ID card in a motor vehicle at night in cold conditions, during which time it could be subject to temperatures as low as -5°C, followed by an increase in temperature up to 20°C (when the vehicle is in use again), associated with manual handling of the DL/ID card (at any temperature).																	x
Leaving a DL/ID card in a piece of clothing during which time it will be subject to water with high temperatures, washing and abrasion (e.g. in a washing machine or dryer) and/or dry cleaning chemicals.												x				x	
Occasional exposure to water, rain, hail and snow.																	x
Occasional exposure to matter such as mud, oil, grease and fuel.							x	x	x				x	x			
Occasional exposure to magnetic fields.																	
Occasional exposure to X-Rays.																	
Integrity attack	x																

The table below matches the various tests to the requirements, for those tests applicable to only some cards.

Table D.3 — Matching to a limited set of standardized card tests

Conditions	ANSI				ISO/IEC		
	5.2	5.13	5.14	5.22	5.9	5.12	5.13
A person carrying a DL/ID card in a wallet, or loose in a pocket (along with keys or coins), in all weather conditions, for 12 hours at a time, on a daily basis, including in dusty, dirty and gritty environments.					x		
Leaving a DL/ID card in a motor vehicle on the dashboard, during which time it could be subject to direct sunlight and high temperatures (up to 90°C) for a continuous period of up to one month.		x					
Leaving a DL/ID card in a motor vehicle at night in cold conditions, during which time it could be subject to temperatures as low as -5°C, followed by an increase in temperature up to 20°C (when the vehicle is in use again), associated with manual handling of the DL/ID card (at any temperature).							
Leaving a DL/ID card in a piece of clothing during which time it will be subject to water with high temperatures, washing and abrasion (e.g. in a washing machine or dryer) and/or dry cleaning chemicals.							
Occasional exposure to water, rain, hail and snow.							
Occasional exposure to matter such as mud, oil, grease and fuel.			x				
Occasional exposure to magnetic fields.							x
Occasional exposure to X-Rays.						x	
Integrity attack	x			x			

E.6.5 Combinations of tests

ANSI 322 also allows for some of the tests to be performed in sequence on the same set of cards. Although it is clearly infeasible to test all combinations, some test sequences that imitate real world conditions do make sense. The following tests can be considered as "conditioning" tests, i.e. tests that can be performed to "condition" cards for further testing:

- ANSI 5.8 (elevated temperature and humidity exposure)

- ANSI 5.15 (ultraviolet light exposure)

- ANSI 5.16 (daylight exposure image stability – Xenon arc)

- ANSI 5.17 (laundry test)

- ISO 5.14 (resistance to chemicals)

- Commercial dry-cleaning test

Issuing authorities can select test combinations that reflect their unique needs. For example, for purposes of testing card performance under general use (as opposed to intentional attack), preconditioned cards can be submitted to the following tests:

- ANSI 5.4 (card flexure)

- ANSI 5.21 (wet impact and abrasion)

The sequenced tests are conducted in addition to individual tests. For example, three sets of a particular vendor's sample cards are submitted to the elevated temperature and humidity exposure test, and one of the sets is then submitted to the card flexure test, and another set to the surface abrasion test.

E.6.6 Occurrence frequency of environmental conditions

In addition to the tables in E.6.4, the frequency with which a particular environment is encountered should be considered. An example of how this can be performed is shown below. An issuing authority will draft its own version of this table.

Table D.4 — Environment Frequency for standardized card tests

Condition	Frequency encountered
A person carrying a DL/ID card in a wallet, or loose in a pocket (along with keys or coins), in all weather conditions, for 12 hours at a time, on a daily basis, including in dusty, dirty and gritty environments.	8.5 out of 10 card holders, on a daily basis
Leaving a DL/ID card in a motor vehicle on the dashboard, during which time it could be subject to direct sunlight and high temperatures (up to 90°C) for a continuous period of up to one month.	In sunlight: 1 out of every 500 drivers daily. In car: 1 out of 80 drivers daily
Leaving a DL/ID card in a motor vehicle at night in cold conditions, during which time it could be subject to temperatures as low as -5°C, followed by an increase in temperature up to 20°C (when the vehicle is in use again), associated with manual handling of the DL/ID card (at any temperature).	1 out of 55 drivers, twice a year
Leaving a DL/ID card in a piece of clothing during which time it will be subject to water with high temperatures, washing and abrasion (e.g. in a washing machine or dryer) and/or dry cleaning chemicals.	Every card holder 5 times a year
Occasional exposure to water, rain, hail and snow.	19 out of every 25 drivers once a year
Occasional exposure to matter such as mud, oil, grease and fuel.	3.5 out of 100 card holders daily
Occasional exposure to magnetic fields.	Every card holder 50 times a year
Occasional exposure to X-Rays.	Every card holder 15 times a year

E.6.7 Assessment

The ideal output of a durability test would be an estimate of the annual number of cards that will have to be replaced (given the issuing volumes and card validity period). Unfortunately, none of the published card tests currently provide such information.

As an alternative, the frequency with which cards are subjected to a particular condition (as described in Clause E.6.4) should be considered. The argument is that conditions to which cards are subjected more often (and consequently the tests that cover these conditions) should have a relatively bigger influence on card failures than conditions to which cards are subjected less often. However, in using this alternative, cognizance should be taken of the fact that the frequency with which a particular condition occurs is not necessarily proportionally equal to the portion of failures caused by a particular condition. That is, a condition that occurs less frequently may eventually cause most of the card failures.

Another complicating factor is that not all tests simulate the identified conditions equally well. A commercial dry-cleaning test is a very good simulation of actual conditions, whereas the corner impact test is an example of a test that, whilst it can give valuable information on a card's properties, is less representative of the condition it simulates.

Given the above, the following assessment procedure is appropriate:

1. Commence the evaluation by considering the outcome of tests that should give a reasonable estimate of the number of annual failures that can be expected. An example is the commercial dry cleaning test, or if contact with one of the chemicals in the resistance to chemicals test causes a card to fail. Note that a particular test may cause failures only for some cards.

2. Try to use stochastic domination to rank cards. As part of the evaluation, the maximum number of failures under other conditions in order for cards to be equivalent can be calculated, and the probability of that happening can be assessed.

3. Assign a score for each card, by considering the following:

    a. Outcome of the tests covering each condition (as shown in Section E.6.4).

    b. Frequency with which each condition occurs (as shown in Section E.6.6).

    c. Outcome of steps 1 and 2 above.

Each card is awarded a score out of a maximum of 10 points (10 being best and 0 being worst). Scores should reflect not only the order of preference, but also how much better (or worse) one card is than another.

E.7 Integrity testing

E.7.1 Threats

The specific threats that a card should protect against need to be assessed. The list of threats need not be limited to e.g. those listed at 37 CFR Part 6, but can go beyond that to suit a particular environment. The following represents a typical list of threats:

- Simulation or imitation of a DL/ID card with the intent to pass as genuine in circumstances of ordinary use, including the use of amongst others:

    o Similar security features, and/or

    o Reproduction of a genuine DL/ID card or part thereof by means of a reproductive device.

- Substituting the customer's portrait image.

- Substituting the customer's signature.

- Deletion/alteration of the dynamic data.

- The construction of a fraudulent DL/ID card, using materials from a legitimate DL/ID card for parts thereof.

- Theft of genuine generic cards or DL/ID card components.

Additional requirements can include the following:

- Any attempt to tamper with the DL/ID card shall result in the irreversible destruction of the security features and/or damage to the card, which shall be visible (i.e. Level 1) in circumstances of ordinary use[11].

- As a minimum, the DL/ID card shall incorporate the mandatory "security elements" identified in Clause C.6 of ISO/IEC 18013-1 [i.e. UV-dull card body, tamper evident properties, security background pattern (using at least 2 colors, and including micro-lettering), UV-fluorescent ink, optically variable element].

- The combination of security features used shall protect the DL/ID card against all the threats identified above. Although the combination of security features shall allow second and third line verification of a DL/ID card, the combination of security features shall be designed especially to facilitate first line inspection (in respect of all the threats), and to immediately highlight any circumvention attempts upon such inspection.

E.7.2 Integrity tests

It is recommended that integrity testing be performed by security consultants, with the aim to report on the integrity of a card under professional attack.

Vendors are typically asked to specify a card's security characteristics in their bids. The card and list of characteristics are then submitted to an integrity-testing laboratory for verification. In addition, the laboratory is instructed to attack the card, and to attempt to make counterfeit cards.

Instructions to the laboratory for attacking a card can read as follow:

> Make an attempt to change the data and/or photograph/image on a card using any appropriate techniques, such that the changes may be able to evade detection under cursory inspection. Report on the methods, time, cost and effort required for each alternation. Also report on the card's resistance to the various forms of attack employed, including the card's resistance to peeling and/or removing the security feature(s) / laminate(s) using means such as sharp instruments, chemicals, cold and/or heat, in order to gain access to the data and/or photograph/image. Make and report on attempts to remove the security feature(s) / laminate(s) in its entirety and place it on another card, with the purpose of transferring the security feature(s) / laminate(s) from one card to another, and report the findings.

Instructions to the laboratory for attempting to produce counterfeit cards can read as follow:

> Make an attempt to counterfeit cards that would pass a cursory inspection. The counterfeits can be made using color copies and/or photograph/images of the license, readily available "credit card" core stock, graphic arts supplies, and security feature(s) / laminate(s) removed from the genuine cards. Attempt

---

[11] To resolve any doubt, a procedure such as the following can be used: Five law enforcement officers will each be shown a number of cards that have been tampered with amongst a similar number of original cards and requested to identify the tampered cards. If 85% of the answers are correct, the integrity features shall be deemed to be of acceptable quality.

counterfeits at two levels: One where the inspecting person physically handles the card (e.g. when renting a motor vehicle), and another where the cardholder just shows portrait side of the card (whilst possibly still in a transparent billfold flip-out) to the inspecting person. Report on the effort, cost and mechanisms used for each counterfeit.

The output of integrity testing is the following:

- A report describing the extent to which a card complies with the claimed security characteristics.

- A report describing the extent to which security features in a card provided resistance to attack. The report should include all samples used, and provide photographs or images documenting the results as necessary.

- Cards that have been altered in some form or fashion by the laboratory.

- Counterfeit cards manufactured by the laboratory.

E.8 Test reports

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

- Test identification (test specification name, clause number, specification date)

- Test title

- Sample size

- Test date

- Identifying name or number to describe the type/color/style of card tested

- Result for each card tested (numeric and/or qualitative)

Annex F
(informative)

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 A – *Mapping of driver license/identification card information to magnetic stripe 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 standard, AAMVA had adopted the magnetic stripe annex from the AAMVA DL/ID-2000 standard (Annex A). The minimum mandatory data elements of the new standard (see paragraph 4.2 of this standard) 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. The 2010 standard introduced a change in Track 3 with an updated approach to representing both the version of the standard being followed and a field to accommodate incremental/iteration changes made by the issuer.

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 F.1 and F.2.

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

ASCII	Hex	Binary					ASCII	Hex	Binary				
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
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	P	2^5	2^4	2^3	2^2	2^1	2^0	ASCII	Hex	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

ASCII	Hex	Binary							ASCII	Hex	Binary						
?	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 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, address.	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

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
4	35	V-max	R	Name	Priority is as follows, spaces allowed; familyname$givenname$suffix 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
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, IIN Number.	see Table A.1

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
1	1	F	R	Start sentinel	This character shall be encoded at the beginning of the track.	;
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 AAMVA Standards Assistant.	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	CDS Version #	This is a decimal value between 0 and 9 that specifies the version level of the mag stripe format. All mag stripes compliant with this current AAMVA standard shall be designated "0". Should a need arise requiring major revision to the format, this field provides the means to accommodate additional revision.	0-9
3	1	F	R	Jurisdiction Version #	This is a decimal value between 0 and 9 that specifies the jurisdiction version level of the mag stripe format. Notwithstanding iterations of this standard, jurisdictions may implement incremental changes to their mag stripes.	0-9

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
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	1 for male, 2 for female.	1,2
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
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
(informative) **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 standard, 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.

Annex H (informative)
Optional Enhanced Driver
License (EDL)

H.1 Introduction

Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, requires the Secretary of Homeland Security, in consultation with the Secretary of State, to develop and implement a plan by to require U.S. citizens (and non-U.S. Citizens) who were previously exempt from document requirements to present a passport or other authorized travel document that denotes identity and citizenship when entering the United States. The WHTI final regulation for land and sea requires that all travelers have specific acceptable documentation when entering the United States at land and sea ports by June 1, 2009.

The Enhanced Driver's License or Enhanced Identification Card (collectively termed 'EDL') Program has been developed between the Department of Homeland Security and individual states to provide a lower cost, convenient alternative travel document for U.S. citizen residents of states that choose to issue such a document.

The EDL has been developed consistent with the standards of the REAL ID regulation. The EDL is a dual-purpose document; it is a permit to drive as well as a limited-use travel document. The EDL can be used for identification purposes to board a domestic airline, but cannot be used as a travel document for international flights. A state can issue an EDL only to a U.S. citizen who is a resident of that state.

An EDL advances the security of travel documents and facilitates passenger processing at the United States' land and sea ports of entry in a manner that also protects the privacy of cardholders. The unique number on the EDL's RFID tag is read automatically at the border and acts as a pointer to a secure U.S. Customs and Border Protection (CBP) database displaying biographic information, a photograph/image, and the results of terrorist/criminal checks for the CBP Officer as the traveler's car pulls up to the booth. The CBP officer can quickly review the results and focus on the individuals in the vehicle—a practice that promotes officer safety and faster processing.

The biographic information that is shared with CBP for border crossing purposes under the EDL program is limited to: family and given names; date of birth; gender; digital image (portrait); travel document type (e.g., EDL); *issuing jurisdiction* (mandatory), date of expiry; *citizenship*; *optical character read (OCR) identifier located in the Machine Readable Zone; and RFID tag numbers.* States interested in developing an EDL program will have to consider technical questions including whether to maintain a database of biographic EDL information that will be accessed by CBP when a card holder crosses the border or whether to provide CBP with a copy of this biographical information to be maintained by CBP. CBP's use, retention and sharing of EDL information under both models is explained in the Privacy Impact Assessments and System of Records Notices prepared by CBP as part of WHTI implementation, including the Western Hemisphere Travel Initiative Land and Sea Final Rule, Use of Radio Frequency Identification Technology for Border Crossings and the Procedures for Processing Travel Documents at the Border Privacy Impact Assessments. These documents are available through the DHS Privacy Office and online at Privacy Office section of the DHS website, www.dhs.gov.

CBP has also worked with Canada Border Services Agency (CBSA) to develop a mechanism by which Canadian provinces and territories could also develop EDLs; they can be issued only to a Canadian citizen who is a resident of the issuing province or territory.

It is important to note that the state and province employees processing applications do not adjudicate citizenship for the EDL holder; they only verify citizenship. based on specific documents reviewed. If there is any question about the documents presented, the applicant is encouraged to obtain another type of travel document.

H.2 Scope

This annex defines the design elements and mapping of the EDL/ID card machine-readable data elements into the machine-readable zone and the direction for use of radio frequency identification.

H.3 Conformance

An EDL is expected to be generally in conformance with this annex if it meets all the mandatory requirements specified directly or by reference herein for the physical design of the EDL. However, before engaging in the development of an EDL program, an interested state or province/territory is required to enter into a memorandum of agreement (MOA) with CBP or the Canada Border Services Agency, respectively. Upon signing the MOA, a state or province/territory would work with its federal partner to develop a business plan and establish a technical working group to address specific issues related to the exchange of information. Only after successful testing of the data exchange and EDL document would CBP designate the card as WHTI-compliant through the publication of a Notice in the Federal Register.

H.4 Normative references

The following normative documents contain provisions which, though referenced in this text, constitute provisions of this annex. The latest addition of the references applies. DHS/CBP/OIT/PSPO documents are available from request from DHS/CBP.

DHS/CPB/OIT/PSPO 2600-006-MRZ-RFID: *Western Hemisphere Travel Initiative Recommended Enhanced Driver's License Format: Radio Frequency Identification Technical and Machine Readable Zone Requirements* (For a copy of this document, please contact CBP through AAMVA)

DHS/CPB/OIT/PSPO 2600-006-RFID Tag Format Choice: *WHTI RFID Tag Format Choice; Use of the EPCglobal Standard "Global Document Type Identifier" (GDTI-96) Tag Data Format for International Travel Documents* (For a copy of this document, please contact CBP through AAMVA)

DHS/CPB/OIT/PSPO 2600-006-RFID Tag TID: *WHTI The RFID Tag TID Preventing Cloning* (For a copy of this document, please contact CBP through AAMVA)

ICAO 9303 Part 3 - Machine Readable Official Travel Documents, Volume 1 – MRTDs with Machine Readable Data Stored in Optical Character Recognition Format, Third edition – 2008 (Available from www.icao.org)

EPCglobal Tag Data Standards Version 1.4 (Available from www.epcglobalinc.org)

ISO 18000-6:2004/Amd.1:2006(E): *Information Technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860MHz to 960 MHz, AMENDMENT 1: Extension with Type C and update of Types A and B)*

ISO 1831: *Printing Specifications for Optical Character Recognition*

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

ISO 1073-2:1976: *Alphanumeric character sets for optical recognition -- Part 2: Character set OCR-B -- Shapes and dimensions of the printed image*

ISO 8601:2004: *Data elements and interchange formats -- Information interchange -- Representation of dates and times*

H.5 EDL Technical Requirements

The technical requirements for the Enhanced Drivers Licenses, as mentioned above, include sharing the following Data with CBP: family and given names; date of birth; sex; digital image (portrait); travel document type (e.g., DL); *issuing jurisdiction* (mandatory), date of expiry; *citizenship*; *optical character read (OCR) identifier located in the Machine Readable Zone; and RFID tag numbers.* This information is shared with or retrieved by CBP only when a traveler presents his or her EDL when applying for admission to the United States at a land or sea port of entry.

H.5.1 Issuance

After the MOA is signed and approved, EDLs are expected to meet minimum specifications in several areas: card issuance, use of facilitative technology, determination of citizenship, document security elements, employee requirements and technical requirements.

H.5.2 Data Transmission

States interested in developing an EDL program will have to consider technical questions including whether to maintain a database of biographic EDL information that will be accessed by CBP when a card holder crosses the border or whether to provide CBP with a copy of this biographical information to be maintained by CBP. Canadian provinces/territories interested in participating in the EDL program should contact CBSA for more information.

Interfaces developed jointly by CBP and participating states support a transfer of new or updated EDL data information between the states and CBP. This information can be transferred in a "Push" or "Pull" model. CBP recommends both models use NLETS as the data transfer method.

When an EDL holder crosses the border, the Radio Frequency Identification (RFID) or Machine Readable Zone (MRZ) data will be used to trigger access to the state EDL database. When a document is read at the border, name, date of birth, gender, citizenship and photo/image, along with the results of law enforcement queries, will be presented to the CBP Officer in the inspection booth for review.

In the "Push" model, issuing states will push EDL data at time of issuance to CBP, which will insert and store the EDL data into a secure database for access as mentioned above.

In the "Pull" model, issuing states store their data in their own database, and CBP retrieves the data at time of presentation at a border crossing via NLETS. CBP pings a state's database at the port of entry via NLETS when an EDL is presented at the border.

CBP's use, retention and sharing of EDL information under both models is explained in the Privacy Impact Assessments and System of Records Notices prepared by CBP as part of WHTI implementation, including the Western Hemisphere Travel Initiative Land and Sea Final Rule, Use of Radio Frequency Identification Technology for Border Crossings and the Procedures for Processing Travel Documents at the Border Privacy Impact Assessments. These documents are available through the DHS Privacy Office and online at Privacy Office section of the DHS website, www.dhs.gov.

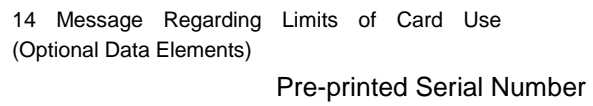## H.6 EDL Physical Requirements

The EDL contains both eye readable (human-readable) and machine readable information. In addition to the AAMVA requirements for human-readable information, the EDL must include the word "Enhanced" and an image of the U.S. flag (for U.S. state-issued EDLs) on the portrait side of the EDL. For machine reading and interoperability, information corresponding to the human-readable data is printed in the Machine Readable Zone on the non-portrait side of the document.

The card also includes a vicinity RFID chip that will contain the unique identifier for the issued card.

H.6.1 Machine Readable Zone (MRZ)

The MRZ is standard to all travel documents and is a mandatory requirement for EDLs. It is located in Zone VII (by ICAO standards) on the non-portrait side of the EDL. The ICAO standards with EDL recommendations for the non-portrait side of an ID/DL-sized document are below. A minimum white space of 23mm must be made available in Zone VII for the MRZ. Figures H.1 and H.2 show the recommended non-portrait side layout for an EDL and a sample non-personalized EDL. Figure H.3 provides a sample of data in an EDL MRZ. For more detailed information, please reference *ICAO 9303 Part 3 Volume 1* and *WHTI Recommended EDL Format, RFID and MRZ Requirements.*

Figure H.1 – EDL Card back

Figure H.2 – Sample EDL Card back

Figure H.3 – MRZ Example

Enhanced Drivers License MRZ

Document Type Code "ID" = Enhanced Driver's License / Identity Card

Issuing country – USA or CAN

Document number up to 9 alphanumeric characters

Check digit on the document number

Filler characters to end of line

IDUSASNUZ5A3J03<<<<<<<<<<<<<<<<

Check digit on date of birth

Date of birth in format YYMMDD

Date of document expiry in format YYMMDD

Nationality of holder – USA or CAN

Reserved for future use if necessary

Composite check digit for upper and middle machine readable lines

8505246F1305241USA<<<<<<<<VT<4

Gender of holder

Check digit on date of expiry

Positions 27-28 reserved for State code

DOE<<MARY<JANE<<<<<<<<<<<<<<<<

Primary Identifier; if more than one component, each is separated by a single filler character

Two filler characters indicate end of Primary Identifier

Secondary Identifier; each component separated by a single filler character

Filler to end of line indicate no other name components
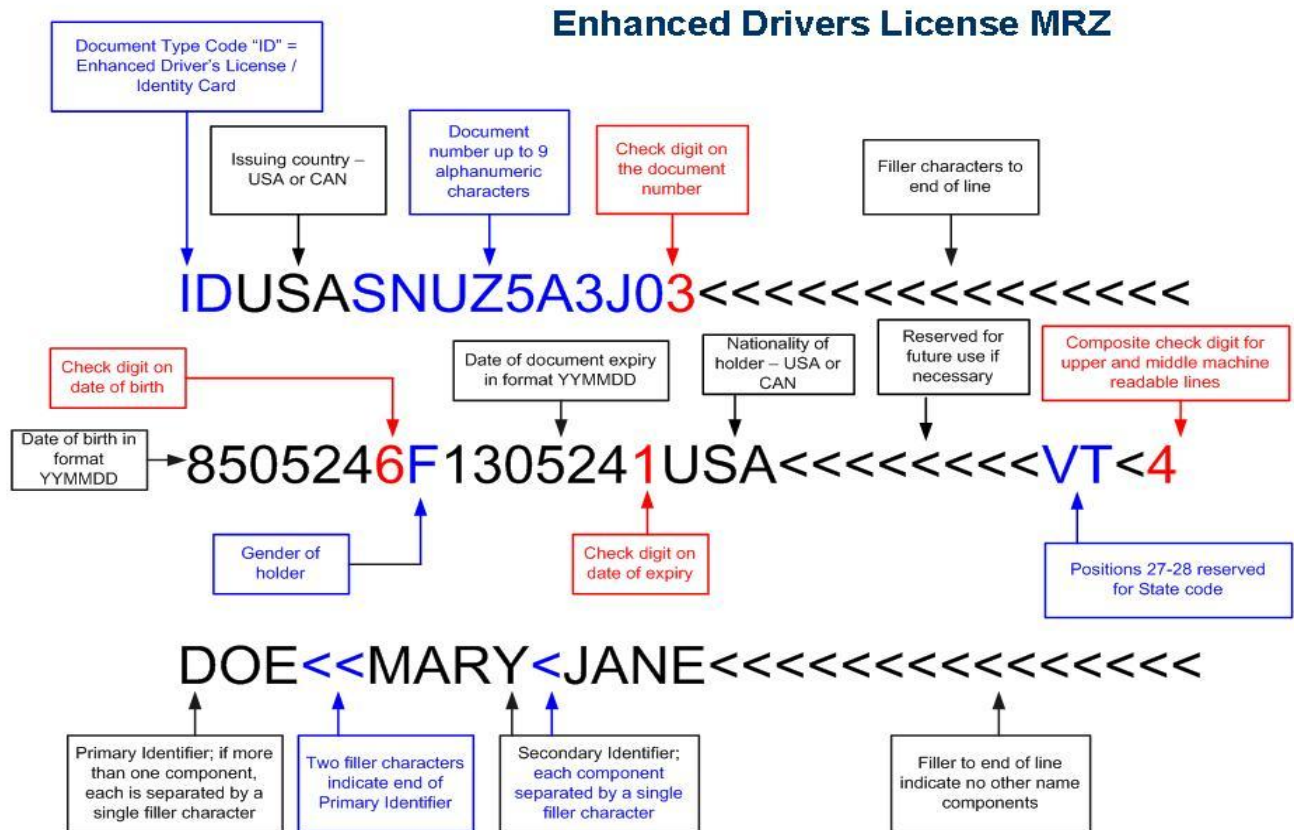
H.6.2 Use of Radio Frequency Identification Technology in the EDL

Radio Frequency Identification (RFID) is a wireless technology that stores and retrieves data remotely on devices. An RFID system typically includes an RFID tag with a microchip and antenna embedded in a card or other item, an RFID reader with an antenna, and a database. The EDL is embedded with a passive RFID tag, which means it does not have a power source. CBP selected vicinity RFID technology because it facilitates cross border travel by allowing documents to be read automatically, with minimal action by travelers as they drive toward the inspection booth at a land port. Vicinity RFID allows CBP officers to quickly read the advanced information on all travelers presenting RFID-enabled cards, and allows for automated watch list queries. In addition, multiple cards can be read simultaneously with vicinity RFID, allowing an entire car of people to be processed at once.

The RFID tag embedded in an EDL does not contain any personally identifiable information (PII), just a unique reference number that means something only to the secure CBP system. Tampering with, or deactivating the RFID tag will invalidate the EDL for purposes of border crossing.

An RFID reader at the border crossing sends a signal to the tag in the EDL and collects the reference number so it can be matched to CBP's records to verify the information printed on the portrait side of the EDL. Data

encryption, secure networks, and firewalls protect the information while it is being retrieved from the database. Vicinity RFID tags can be read up to 30 feet from a reader; however, CBP reader antennas are tuned to read at a distance of 10 – 15 feet. For added security, an RF-attenuation security sleeve should be provided to protect the RFID tag from being read when the cardholder is not using it for border crossing**.**

Generally, if the RFID document is in a sleeve, held close to the body, or is blocked by anything composed of metal or water, it cannot be read. While such a risk of the RFID tag being read without the owner's knowledge is minimal, education and the use of a security sleeve helps protect the traveling public from unauthorized reads.

H.6.2.1   EDL Integrated Circuit Chip (ICC) Data Schema

Among participating government entities, there is consensus to use EPCglobal standards in determining the information stored on the RFID chip. EPCglobal is a not-for-profit organization that develops and promotes standards used in the RFID community. Adherence to EPCglobal standards makes it easier to work with a wide choice of vendors, and helps promote interoperability between vendors.

The unique identifier of each card to be electronically written should comply with *EPCglobal Tag Data Standards*. The key to be used is the Global Document Type Identifier (GDTI-96), a simple tool to identify a document by type. The following represents a high-level overview of the GDTI-96 data schema. For more detail, please reference *EPCglobal Tag Data Standards Version 1.4*.

The data schema primarily consists of (see Table H.1):

- EPCglobal **Header** specifying the tag data is encoded as a GDTI-96 96-bit tag construct.

- EPCglobal **Filter Value** of 001 identifying a tag as a 'travel document'. All WHTI-compliant RFID-enabled travel documents will contain '001' for the Filter Value Field. CBP lane equipment is designed to filter all other Gen 2 RFID numbers for operational needs.

- **Company Prefix:** Every new state, agency, or organization that plans to use GDTI-96 for RFID-enabled travel documents must request a Company Prefix from the GS1/EPCglobal organization. The Company Prefix is a 6 to 12 digit number that uniquely identifies an organization throughout the world. The Company Prefix block of the GDTI-96 tag will contain this number. The number is assigned only once; the issuing authority will use the same company prefix for all RFID-enabled travel documents.

- **Document Type:** A field managed by the issuing authority that can be used to differentiate between different types of travel documents. While use of this field is not required, AAMVA recommends that all participating agencies follow the AAMVA "STATE DOCUMENT TYPE" repository code for filtering capabilities. Values in this field are always numeric, but will map back to real world values that define the type of document in use: "1" = Driver License; "2" = Driver Permit; "3" = State Identification Card.

- **Serial Number:** 41 bits offers 2^{41} = 2,199,023,255,552 (2.1+ trillion) unique numbers that are managed by the issuing organization. Serial numbers are unique per organization, so any organization can issue a serial number in the range [1 - 2,199,023,255,552].   Each managing organization is responsible to ensure unique serial numbers are encoded across a set of issued travel documents. CBP recommends that serial numbers be assigned using a random number generator. Once a number is assigned, and to prevent subsequent rewriting of data on the chip, the issuing authority is required to use the permalock feature of the chip.

Table H.1 — Integrated Circuit Chip Data Schema

	Header	Filter Value	Partition	Company Prefix	Document Type	Serial Number
Bit Size:	8 bits	3 bits	3 bits	20-40 bits	21-1 bits	41 bits
Value Range	0010 1100 (*Static, Binary Value*)	001	*Indicates lengths in Company Prefix and Document Type fields[12].*	999,999 – 999,999,999,999 (Max. decimal range[8])	999,999-0 (Max. decimal range[1])	2.1+ trillion
Assigned By:	EPCglobal	EPCglobal	EPCglobal	EPCglobal	Tag Owner	Tag Owner

H.6.3 Preventing Cloning with the TID

The *EPC Generation 2 Air Interface Specification* defines a Tag Identifier (TID). The TID is a section of memory within a Generation 2 RFID tag that provides manufacturer identification data and is allowed to provide a unique number for each tag. When the TID is implemented with a unique number and is used in conjunction with the GDTI-96 value, it provides a very powerful tool to negate the threat of cloning or duplicating a WHTI GDTI-96 encoded RFID card. In order to enhance anti-counterfeiting measures and defeat cloning, participating entities must ensure that all cards used for WHTI-compliant travel documents include a TID memory bank initialized with a unique serial number that conforms to the EPC RFID Air Interface specification. This TID number must be factory encoded and permanently locked and must be accessible from or pointed to by the TID memory bank of the RFID card Integrated Circuit. For further information, please review the appropriate references.

---

[12] The Company Prefix and Document Type fields are both variable length. The Partition field indicates which lengths can be found in each of the fields.

Annex I (informative)
Optional Compact
Encoding

I.1 Scope

This Annex provides a compact encoding scheme as an alternative to the scheme in D.12. The compact encoding scheme allows issuing authorities the option of compiling a 2D bar code that is compliant with ISO/IEC 18013-2.

For compact encoding, a typical minimum capacity of 300 usable bytes is required. Typical media on which compact encoding is implemented are:

- 2D bar codes

- High coercivity high density magnetic stripes

NOTE   When high coercivity high density magnetic stripe media is used, all six tracks shall be read.

The limited storage capacity means that the number of data groups is restricted, as is the data size of each. For the data groups defined in ISO/IEC 18013-2, the compact encoding scheme accordingly provides for Data Group 1, and optionally for any combination of data groups 2, 3, 4, 7 and 11 subject to storage capacity availability.

The Annex also provides means of validating and authenticating the stored data.

I.2   Normative References

The following referenced documents are indispensable for the application of this Annex. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7811-7:2004, *Identification cards — Recording technique — Part 7: Magnetic stripe — High coercivity, high density*

ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 18013-2:2008, *Personal Identification – ISO Compliant Driving License – Part 2: Machine Readable Technologies*

ISO/IEC 19794-3:2006, *Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data*

I.3   Overview

The compact encoding method generates one data string containing all data groups. This data string is written to (and read from) storage media in the format provided for by each technology.

The compact encoding method differentiates between the following two types of data groups:

- Type 1 data group: Data groups that contain only data of which the allowable characters are specified in this International Standard (i.e. data groups 1, 2 and 3).

- Type 2 data group: Data groups that include data of which the allowable characters are specified by another standard (i.e. data groups 4 and 7), and which thus may include delimiters as part of the field content.

Data Group 11 can be either a Type 1 or a Type 2 data group, depending on the information stored in this Data Group.

The encoding of data in a Type 1 data group is based on a fixed sequence of possible data elements in the data file. Each data field and data group (including optional and/or empty data fields and data groups) is terminated by an "end of field" or "end of data group" indicator. Data fields read sequentially from the data file thus can be assigned the appropriate data field name. This encoding method does not require each field to be identified individually with a tag in the data file, nor does it require the length of any field to be included in the data file.

The parsing rules for a Type 2 data group do not depend on delimiters to identify the data fields. Sufficient information is supplied in the data to calculate the position of the first and last bytes of each data field in the data stream.

I.4   Character set encoding

Unless otherwise specified, data objects are encoded as indicated in Table I.1.

Table I.1 — Encoding rules

Object	Encoding
Data fields of which the abstract values are defined as consisting of only N characters	BCD
Data fields of which the abstract values are defined as containing (although not necessarily exclusively) any A or S characters	As per ISO/IEC 8859-1
Delimiters	As per ISO/IEC 8859-1
Data object length	ASN.1
NOTE A field that is defined in this International Standard as containing (amongst others) A and/or S characters will always be encoded using ISO/IEC 8859-1, even if an issuing authority's implementation of the same field is limited to N characters.	

I.5   Structure

I.5.1   Data file

The structure of a data file created using compact encoding can be represented as follows:

> [header] × [Data Group 1] × [Data Group 2] × [Data Group 3] × [Data Group 4] × [Data Group 7] × [Data Group 11] ¶

The header and Data Group 1 are mandatory; all other elements of the data file are optional. Data groups are delimited using the data group delimiter (×). The number of data group delimiters is fixed regardless of the number of optional data groups actually present. Data Group 11 is followed by the end of file delimiter (¶).

NOTE   The data group delimiter (×) is a multiplication sign and not a lower case X. Spaces (periods) have been inserted before and after the data group delimiter and before the end of file delimiter above for ease of reading only.

I.5.2   Header

The header consists of the following components:

> [AID] [version] [length]

where

AID   =   Application identifier, 7 bytes. Consists of a 5 byte Registered Application Identifier (RID), 'A0 00 00 02 48', and a 2 byte Proprietary Application Identifier Extension (PIX) '01 00'.

Version   =   2 byte number. The value of the first byte shall be '01' for this version of this Standard. The second byte is assigned by the issuing authority for each new version of their specification controlling the coding of domestic data (Data Group 11).

Length   =   Length of the data file (in bytes), encoded using ASN.1. The length equals the total number of bytes from (and including) the data group delimiter between the header and Data Group 1, up to and including the last character of the Logical Data Structure (LDS) (i.e. the end of file delimiter).

> NOTE   Although it is strictly speaking not necessary to know the length of the data file, it is included to assist in read verification.

EXAMPLE

Suppose that:

RID	=	A0 00 00 02 48
PIX	=	01 00
Version level	=	1
Domestic version level	=	not specified (defaults to 0)
Total length	=	1598 bytes ('82 06 3E' in ASN.1 hexadecimal representation)

Then, the header would be encoded as follows (spaces are included for clarity only and are not encoded; apostrophes are used to indicate hexadecimal characters and are not encoded):

'A0 00 00 02 48 01 00 01 00 82 06 3E'

I.5.3 Type 1 Data Group

A Type 1 data group consists of data elements delimited by the field delimiter (÷) as follows:

…× [element_1] ÷…÷ [element_n] ÷…÷ [element_last] ×…

All data elements are delimited (including optional elements), regardless of whether or not an element contains data. The only exception is if the data group contains no data, in which case no field delimiters are used. To facilitate forward compatibility, parsers shall be able to accommodate additional elements appended to a data group. The sequence of fields are specified in the respective data group definitions.

A data element can be sub-divided into data sub-fields. In a Type 1 data group, sub-fields are delimited by a sub-field delimiter ((;) sub-delimiter for short) as follows:

…[element_2] ÷ [field_3.1] ; [field_3.2] ; [field_3.3] ÷ [element_4]…

If a data sub-field is the last data element in a data group, it is terminated with the data group delimiter.

For data elements containing a fixed number of data sub-fields (e.g. the address field), the number of sub-delimiters is constant, regardless of the number of optional sub-fields present. The only exception is if none of the sub-fields contain data, in which case no sub-field delimiters are present.

The set of sub-fields in a data field may be repeated. If a set of sub-fields is not terminated with a field delimiter or a data group delimiter, it means that the next field will be the first sub-field of another set of sub-fields.

EXAMPLE   A license category field consists of 6 sub-fields, of which the first sub-field is mandatory. A license category field containing 3 license categories can then be coded as follows:

…÷ [category_1—field_1] ; [category_1—field_2] ; [category_1—field_3] ; ; ; ; [category_2—field_1] ; ; ; [category_2—field_4] ; ; ; [category_3—field_1] ; ; ; [category_3—field_4] ; [category_3—field_5] ; [category_3—field_6] ÷…

NOTE   Spaces (periods) have been inserted before and after the data group, field and sub-field delimiters above for ease of reading only.

I.5.4   Type 2 Data Group

The contents of a Type 2 data group can generally be represented as follows:

× [fixed_length_field_1] [fixed_length_field_2] … [fixed_length_field_n] [variable_length_field_ length] [variable_length_field] ×

where × is the data group delimiter. The length of a variable_length_field is specified using ASN.1 rules (see Appendix A to Annex C). The number of fixed length fields and the number of variable length fields is not restricted. The number and sequence of fields are specified in the data group definition.

I.6   Implementation

I.6.1   Data Element Mapping

Table I.2 provides a mapping between the data elements defined in ISO/IEC 18013-2 and the AAMVA data elements defined in this Standard.

Table I.2 — Data element mapping

ISO/IEC 18013-2 data element	AAMVA data element	Data Group	Optional (O) / Mandatory (M)
Family name	Family name	DG1	M
Given[a] names	Given names	DG1	M
Date of birth	Date of birth	DG1	M
Date of issue	Date of Issue	DG1	M
Date of expiry	Date of expiry	DG1	M
Issuing country		DG1	M
Issuing authority	Issuing jurisdiction	DG1	M
License number	Customer identifier	DG1	M
Categories of vehicles/restrictions/ conditions (refer to Annex A of ISO/IEC 18013-2 for field assembly rules)		DG1	M

ISO/IEC 18013-2 data element	AAMVA data element	Data Group	Optional (O) / Mandatory (M)
Gender	Cardholder sex	DG2	M
Height	Height	DG2	M
Weight	Weight	DG2	O
Eye colour	Eye color	DG2	M
Hair colour	Hair color	DG2	O
Place of birth	Place of birth	DG2	O
Normal place of residence	Cardholder address	DG2	M
Administrative number	Audit information	DG3	O
Document discriminator	Document discriminator	DG3	M
Data discriminator		DG3	O
ISO issuer ID number	Issuer Identification Number	DG3	O
Portrait image timestamp		DG4	O
Type of image		DG4	O
Portrait image	Portrait	DG4	O
BDB format owner		DG7	O
BDB format type		DG7	O
Biometric data block length		DG7	O
Biometric data block		DG7	O
	Family name truncation	DG11	M
	Given names truncation	DG11	M
	Name suffix	DG11	O
	Alias / AKA Family Name	DG11	O
	Alias / AKA Given Name	DG11	O
	Alias / AKA Suffix Name	DG11	O
	Race / ethnicity	DG11	O
	Jurisdiction-specific vehicle classification description	DG11	O
	Jurisdiction-specific endorsement code description	DG11	O

ISO/IEC 18013-2 data element	AAMVA data element	Data Group	Optional (O) / Mandatory (M)
	Jurisdiction-specific restriction code description	DG11	O
	Date of first issue per category	DG11	O
	Separate expiry dates for vehicle classifications	DG11	O
	Inventory control number	DG11	O
	Compliance Type	DG11	O
	Card Revision Date	DG11	O
	HAZMAT Endorsement Expiration Date	DG11	O
	Limited Duration Document Indicator	DG11	O

See ISO/IEC 18013-2 for field definitions of ISO/IEC 18013-2 data elements. Field values must be rendered in the format prescribed in ISO/IEC 18013-2. Fields that are not defined in ISO/IEC 18013-2 must be rendered as specified in Annex D.

I.6.2 Data Group 1: Mandatory Data

Data Group 1 is a Type 1 data group.

A sub-field delimiter is used between different instances of the category of vehicle/restriction/condition data object.

EXAMPLE 1

Assume the following:

Family name	=	Smithe-Williams
Given name	=	Alexander George Thomas
Date of birth	=	1 March 1970
Date of issue	=	15 September 2002
Date of expiry	=	30 September 2007
Issuing country	=	USA
Issuing authority	=	North Carolina DMV

License number   =   A290654395164273X

Categories of vehicles, restrictions:

Category B vehicles, issued 1 September 1991, expires 1 March 2035

The above data group will be coded as follows:

[header]✕Smithe-Williams÷Alexander George Thomas÷'19 70 03 01'÷'20 02 09 15'÷'20 07 09 30'÷USA÷NORTH CAROLINA DMV÷A290654395164273X÷B;19910901;20350301;;;✕[next data group]

Where

Smi…ams	=	Family name
Ale…mas	=	Given names
'19 70 03 01'	=	BCD encoding of birthday, 1 March 1970
'20 02 09 15'	=	BCD encoding of IDL issue date, 15 September 2002
'20 07 09 30'	=	BCD encoding of IDL expiry date, 30 September 2007
USA	=	Issuing country
NOR…DMV	=	Issuing authority
A29….73X	=	License number
B	=	Category B vehicles
'19 91 09 01'	=	BCD encoding of issue date of category B, 1 September 1991
'20 35 03 01'	=	BCD encoding of expiry date of category B, 1 March 2035

I.6.3   Data Group 2: Optional License Holder Information

Data Group 2 is a Type 1 data group.

EXAMPLE

Assume the following:

Gender	=	Male
Height	=	172 cm
Weight	=	82 kg

Eye color   = Blue

Hair color   = Bald

Normal place of residence   =   471 Monica Road, 201 Delta Building, Lynnwood, Georgia, 01234, USA

The above data group will be coded as follows:

[previous data group] ✕ 1 ÷ '01 72' ÷ '00 82' ÷ BLU ÷ BLD ÷ ÷ 471 Monica Road;201 Delta Building;Lynnwood;Georgia;01234;USA ✕ [next data group]

Where

1   = male (per ISO/IEC 5218)

'01 72'   = BCD encoding of height, 172 cm

'00 82'   = BCD encoding of weight, 82 kg

BLU   = Blue eyes (per ANSI D20)

BLD   = Bald (per ANSI D20)

471 Mo…USA = Residence information

NOTE   No place of birth included.

I.6.4 Data Group 3: Optional Issuing Authority Information

Data Group 3 is a Type 1 data group.

The document discriminator field as well as the data discriminator field shall be each encoded as a 1 byte binary number. The ISO issuer ID number field shall be encoded as a 4 byte binary number.

EXAMPLE

Assume the following:

Administrative number   =   123456789B

Document discriminator   =   01

ISO issuer ID number   =   636000

The above data group will be coded as follows:

[previous data group] ✕ 123456789B ÷ '01' ÷ ÷ '00 09 B4 60' ✕ [next data group]

Where

    123456789B   =   Administrative number

    '01'   =   Document discriminator

    '63 60 00'   =   BCD encoding of ISO issuer ID number

NOTE   No data discriminator included.

I.6.5 Data Group 4: Optional Portrait Images

For compact encoding, Data Group 4 supports one portrait image only. Consequently, not all of the fields defined in 8.4 of ISO/IEC 18013-2 are provided for. The coding of the portrait image is specified outside of this International Standard, and thus Data Group 4 is a Type 2 data group. Data Group 4 is coded as follows (spaces are included to enhance legibility only, and are not encoded):

    [previous data group] ✕ [type of image] [image length] [image] ✕ [next data group]

Where

    [type of image] is a fixed length field

    [image length] is the length of the [image] field, expressed using ASN.1 rules

    [image] is a variable length field

    the [image] field is encoded as a binary object.

EXAMPLE

Assume that the data group consists of one JPEG portrait image with a total length of 2075 bytes ($81B_{16}$ bytes). This will be encoded as follows:

    [previous data group] ✕ '03' '82 08 1B' [2075_{10} byte image field] ✕ [next data group]

Where

    '03'   =   image type 3 (JPEG)
    '82 08 1B'   =   ASN.1 encoding of the image length of 2075 bytes
    ..image….. =   Image field including definition details and binary data

I.6.6 Data Group 5: Optional Signature/Mark Image

Data Group 5 is not supported in compact encoding.

I.6.7 Data Group 6: Optional Facial Biometric Template

Data Group 6 is not supported in compact encoding.

I.6.8 Data Group 7: Optional Finger Template

Data Group 7 is a Type 2 data group. Due to limited storage space, only finger minutiae data and finger pattern spectral data are supported in Data Group 7. This limitation precludes the use of optional data elements listed in Table 6 of ISO/IEC 18013-2.

Data Group 7 thus is coded as follows (spaces are included to enhance legibility only, and are not encoded):

[previous data group] × [BDB format owner] [BDB format type] [biometric data block length] [biometric data block] × [next data group]

Where

[BDB format owner] is a fixed length field

[BDB format type] is a fixed length field

[biometric data block length] is the length of the [biometric data block] field, expressed using ASN.1 rules

[biometric data block] is a variable length field, encoded in accordance with Table I.1, with the understanding that delimiters may be included in data fields as data (i.e. without fulfilling a delimiting function).

The content of the biometric data block complies with ISO/IEC 19794-2 or ISO/IEC 19794-3. Consequently, the following BDB format owner and BDB format type combinations are valid:

Table I.3 — BDB format owner and type combinations

BDB format owner	BDB format type
'01 01'	'00 01' (finger-minutia-record-n)
'01 01'	'00 02' (finger-minutia-record-x)
'01 01'	'00 03' (finger-minutia-card-normal-v))
'01 01'	'00 04' (finger-minutia-card-normal-n)
'01 01'	'00 05' (finger-minutia-card-compact-v)
'01 01'	'00 06' (finger-minutia-card-compact-n)
'01 01'	'00 0A' (finger-pattern-spectral)

EXAMPLE

Assume that the data group consists of a finger pattern spectral biometric data block with a total length of 234 bytes ('EA'$_{16}$ bytes). This will be encoded as follows:

[previous data group]× '01 01' '00 0A' '81 EA' [234$_{10}$ byte biometric data block]×[next data group]

Where

'01 01'	=	BDB format owner (ISO/IEC JTC1 SC37 - Biometrics)
'00 0A'	=	BDB format type (finger pattern spectral data format as specified in ISO/IEC 19794-3)
'81 EA'	=	ASN.1 encoding of the biometric data block length of 234 bytes
..image…..	=	Image data block including definition details and binary data

I.6.9 Data Group 8: Optional Iris Biometric Template

Data Group 8 is not supported in compact encoding.

I.6.10 Data Group 9: Optional Other Biometric Template

Data Group 9 is not supported in compact encoding.

I.6.11 Data Group 10: Reserved for Future Use

Data Group 10 is not currently supported in compact encoding.

I.6.12 Data Group 11: Optional Domestic Use

Data Group 11 is a Type 1 data group.

The content and sequence of data elements in Data Group 11 is specified in Table I.2.

Annex J (informative)
Optional Integrated Circuit
for Standard Encoding

J.1 Introduction

Standard encoding is designed for random access and is suitable for use on documents employing ICCs with contacts and PICCs based on ISO/IEC 7816 and ISO/IEC 14443 respectively. Rewriting, updating, and appending functions may be supported to the extent allowed by the technology (or technologies) used. If implemented, such functions shall comply with the principles set out herein. Security options are established to support authenticity and integrity of machine-readable data.

A driving license containing an optional integrated circuit is compliant with this annex if it complies with ISO/IEC 18013-2, as amended and expanded in clause J.2.

The remainder of clause J.1 reflects background information, and includes text borrowed from ISO/IEC 18013-2.

Design considerations

The file structure and encoding rules have been defined with the following considerations and assumptions:

- A wide variety of implementations must be supported to satisfy specific needs of different issuing authorities. More specifically the data structure must efficiently support:

  o Mandatory and optional sets of data elements.

  o Multiple occurrences of specific data elements that may exist within a data group.

  o A range of possible access conditions in respect of optional data elements as required by different issuing authorities (due to significant variance in business requirements driven by privacy and other statutory requirements).

  o The unconditional availability of mandatory data.

  o An optional mechanism to verify one or more digital signatures.

  o Discovery of the interoperability and security requirements in respect of the optional data elements from the card.

- The structure supports at least two (2) application data sets:

  o The IDL application, which has the following properties:

- Contains data elements with the following properties:

    - Includes information that would enable a reading authority to identify the access control, authentication and integrity validation mechanisms present on the card.

    - Write protected.

    - Modifiable by the issuing authority (or trusted agent of the issuing authority), subject to the requirements in 5.1 (for example the machine-readable data may not differ from the human-readable data).

  - Optionally protected with one or more digital signatures (defined in ISO/IEC 18013-3).

  o DDL application(s)

- Contact between the driver license and passport environments is considered more likely than contact between the driver license environment and non-passport environments (that are compliant with ISO/IEC 7816s). Consequently, tag assignments are aligned with ISO/IEC 7501-1 (ICAO Doc 9303-1).

Interoperability considerations

To provide global interoperability this Annex defines:

- Physical characteristics

- Location and dimensions of the contacts or coupling areas

- Electrical signals to support communication between the IC and the interface device

- Transmission protocols

- Application selection and discovery of optional data elements and security requirements

- Encoding rules

- The file structure and tag assignments for the IDL Logical Data Structure

- Command set

- Data element mappings to the files

Security requirements

Issuing authorities may need to confirm data validity and authenticity. ISO/IEC 18013-3 specifies mechanisms and means by which to achieve this.

J.2 AAMVA-specific Data Requirements

The following represent those data elements that are required for compliance with this standard.

J.2.1 EF.DG2 Data Group 2 License holder information, Tag = '6B', short EF identifier = '02'

All of Data Group 2.

J.2.2 EF.DG11, Data Group 11 Mandatory and Optional domestic data, Tag to be assigned by issuing authority, short EF identifier = '0B'

Table J.1

Tag	Length	Value	Value format	Mandatory/Optional	Example
'5C'	X	Tag list	binary		List of all data elements present
'5F68'	'01'	Family Name Truncation	F1A	Mandatory	"N" – not truncated
'5F69'	'01'	First Name Truncation	F1A	Mandatory	"N" – not truncated
'5F6A'	'01'	Middle Name Truncation	F1A	Mandatory	"N" – not truncated
'5F6B'	'01'	Compliance Type	F1A	Optional	"M" – materially compliant
'5F6C'	'01'	Card Revision Date	F8N	Optional	"09302010" – MMDDCCYY
'5F6D'	'01'	Limited Duration Document Indicator[a]	F1N	Optional	"1"
a = The Limited Duration Document Indicator will only be present if applicable.					
NOTE For compliance with DHS programs the following fields are required: Compliance Type; Card Revision Date; and Limited Duration Document Indicator					