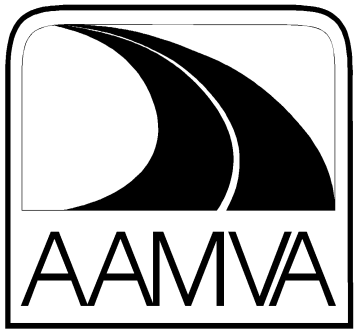
AAMVA

2000-06-30

AAMVA National Standard for the Driver License/Identification Card

AAMVA DL/ID-2000



American Association of Motor Vehicle Administrators

This document was produced by AAMVAnet, Inc. AAMVAnet is a division of the American Association of Motor Vehicle Administrators (AAMVA).

Contents

Foreword

(This foreword is not part of the AAMVA National Standard for the Driver License).

The purpose of the Driver License Card standard is to provide a uniform means to identify (a) issuers and (b) holders of Driver License cards within the United States.

The standard specifies minimum requirements for the presentation of identification information in human-readable form, and it specifies the format and data content of identification in the following technologies: magnetic stripe, bar code, integrated circuit cards, optical memory, and digital imaging.

It is important to note that inclusion of any technology is optional; however, when a technology is used, it must comply fully with the standard.

The scope of the standard is to specify *identification* information for Driver License applications. It does not standardize recording of driving related convictions or the withdrawal of driving privileges; however, in the high-capacity technologies, the standard employs international standard application coding such that additional applications may be possible on the same card.

This standard is a U.S. Driver License application of existing international identification card standards that relate to physical characteristics, layout, data access and storage techniques, physical security requirements, and to registration procedures for identification of card issuers.

Work on this standard began in 1997 and is a result of cooperation between ANSI NCITS B10, the American Association of Motor Vehicle Administrators (AAMVA) and their Industry Advisory Board. The development involved broad-based project teams including state driver license agencies, government, equipment and software suppliers, card vendors, and consultants.

This standard meets the following objectives:

— uniquely identifies the card issuer and cardholder;

— brings uniformity to the millions of Driver License cards now in circulation;

— encourages transition from existing practice to the new standard;

— assists administrative efficiency and accuracy through machine-readable identification within a foundation that encourages future applications;

— facilitates future development in technology and application.

Requests for interpretation, suggestions for improvement or addenda, or defect reports are welcome. Please send these to the Standards Program Director, AAMVAnet, 4301 Wilson Boulevard – Suite 400, Arlington, VA 22203 (www.aamva.org).

Driver License Cards - Identification Cards

1 Scope

This AAMVA National Standard specifies directly or by reference the requirements for cards used in driver license applications. It takes into consideration both human and machine aspects and states the minimum requirements for conformity. It contains physical characteristics, layout, data access techniques, data storage techniques, registration procedures, and security requirements. Security measures are defined as minimum requirements but card issuers are free to have more stringent security features.

2 Conformance

An identification card is in conformance with this standard if it meets all mandatory requirements specified directly or by reference herein.

3 Normative reference(s)

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this AAMVA National Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this AAMVA National 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 ANSI, ISO and IEC maintain registers of currently valid National and International Standards.

ANSI-D20: 1998, *Data Element Dictionary for Traffic Records Systems*

ANSI/ASQC Z1.4: *Military Standard, Sampling Procedures and Tables for Inspection by Attributes*

ANSI/NIST-CSL1-1993, *"Data Format for the Interchange of Fingerprint Information"*

ANSI X3.182 *Bar-Code Print Quality*

ASCII/ISO 8859-1: *"Information Processing - 8bit single byte coded graphic character sets - Part 1: Latin alphabet No. 1" 1998*

BioAPI Specification Version 1.00 : March 30, 2000 - *The BioAPI Consortium*

CJIS/FBI IAFIS-IC-0110 *Wavelet Scalar Quantization (WSQ)*

CJIS-RS-0010 *Appendix G "Interim IAFIS Image Quality Specifications for Scanners"*

ISO/IEC 646: 1991, *Information technology - ISO 7-bit coded character set for information interchange*

ISO/IEC 7810: 1995, *Identification cards - Physical characteristics*

ISO/IEC 7811-6: 1996, *Identification cards - Recording technique - Part 6: High coercivity magnetic stripe*

ISO 7816-1: 1987, *Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics*

ISO 7816-2: 1988, *Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of contacts*

ISO/IEC 7816-3: 1997, *Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols*

ISO/IEC 7816-4: 1995, *Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands*

ISO/IEC 7816-5: 1994, *Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers*

ISO/IEC 7816-6: 1996, *Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements*

ISO/IEC 10373: 1993, *Identification cards - Test methods*
Except for Clause 6.4 through 6.8, this standard has been superseded by:
ISO/IEC 10373-1: 1998, Identification Cards - Test Methods - Part 1: General characteristics tests
ISO/IEC 10373-1: 1998, Identification Cards - Test Methods - Part 2: Cards with mag stripes
ISO/IEC 10373-1: 1998, Identification Cards - Test Methods - Part 5: Optical memory cards

ISO/IEC 10536-1: 1992, *Identification cards - Contactless integrated circuit(s) cards - Part 1: Physical characteristics*

ISO/IEC 10536-2: 1995, *Identification cards - Contactless integrated circuit(s) cards - Part 2: Dimensions and locations of coupling areas*

ISO/IEC 10536-3: 1996, *Identification cards - Contactless integrated circuit(s) cards - Part 3: Electrical signals and mode switching*

ISO 10918-1: *Information Technology - Digital compression and coding of continuous-tone-still images: Requirements and Guidelines*

ISO/IEC 11693: 1994, *Identification cards - Optical memory cards - general characteristics*

ISO/IEC 11694-1: 1994, *Identification cards, Optical memory cards - Linear recording method Part 1: Physical characteristics*

ISO/IEC 11694-2: 1995, *Identification cards, Optical memory cards - Linear recording method Part 2: Dimensions and location of the accessible optical area*

ISO/IEC 11694-3: 1995, *Identification cards, Optical memory cards - Linear recording method Part 3: Optical properties and characteristics*

ISO/IEC 11694-4: 1996, *Identification cards, Optical memory cards - Linear recording method Part 4: Logical data structures*

ISO/IEC 14443-1: *Identification cards - Contactless integrated circuit cards - Proximity cards Part 1: Physical characteristics*

ISO/IEC 14443-2: *Identification cards - Contactless integrated circuit cards - Proximity cards Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3: *Identification cards - Contactless integrated circuit cards - Proximity cards Part 3: Initialization and anticollision*

ISO/IEC 14443-4: *Identification cards - Contactless integrated circuit cards - Proximity cards Part 4: Transmission protocols*

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

ISO/IEC 15693-1: *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 1: Physical characteristics*

ISO/IEC 15693-2: *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 2: Air interface and initialisation*

ISO/IEC 15693-3: *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 3: Protocols*

ISO/IEC 15693-4: *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 4: Registration of applications/issuers*

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

4 Term(s) and definition(s)

For the purposes of this AAMVA National Standard, the following terms and definitions apply:

4.1
driver license card
a card used to identify the card issuer and the card holder to facilitate Driver License transactions and to provide input data for such transactions

4.2
driver license card issuer
an organization that issues Driver License cards such as a Department of Motor Vehicles and the U.S. Department of State

4.3
driver license card holder
an individual to whom a Driver License card is issued

4.4
numeric (N)
digits 0 to 9

4.5
special characters (S)
! “ # $ % & ‘ ( ) * + , - . / : ; < = > ? [\ ] ^ _ @. A special character is removed from this category when it is used as a delimiter.

4.6
alphabetic (A)
alpha characters (UPPERCASE letters from A to Z)

4.7
alphanumeric (ANS)
alpha characters (UPPERCASE letters from A to Z), numeric characters, space, and special characters

4.8
front side of card
face of the card carrying visual information containing the card issuer and card holder identifiers

4.9
back side of card
the opposite face from the front

4.10
signature panel
area used for DL cardholder signature that is receptive to writing instruments

4.11
DF
dedicated files

4.12
EF
elementary files

4.13
MF
master files

4.14
CICCD
contactless integrated circuit card device

4.15
CICC
contactless integrated circuit card

4.16
ICC
integrated circuit card

4.17
DL
driver license

4.18
ID
identification card

4.19
AKA
also known as

4.20
IIN
issuer identification number

4.21
digital
any data that is composed of a discrete sample or collection of discrete samples that are represented as finite numbers

4.22
image
digital data that represents the visual likeness of its subject, such as a portrait, finger, or signature. Images may be collected, stored, and rendered for visual inspection using a variety for digital formats

5 Physical characteristics and card technologies

Various card technologies may be employed at the option of the card issuer subject to the restrictions described in 5.1 and 5.2. None of these card technologies are required on the card, however, if they are used they shall be implemented as defined in the appropriate annex.

5.1 Physical characteristics

Physical characteristics of cards that employ none of the optional card technologies are at the discretion of the card issuer provided that, after any folding, there is a front side and a back side as defined herein. Additional physical characteristics, if any, related to each card technology are specified in the annex for that card technology.

5.2 Card technologies

Available card technologies are shown in the following list. It is possible that certain types of card technologies may be incompatible in combination.

Annex	Technology	Use of technology on card
A	Magnetic stripe cards	Optional
B	Integrated circuit cards (ICC)	Optional
C	Finger imaging	Optional
D	Optical memory cards	Optional
E	Bar codes, 2 dimensional	Optional
F	Data compression for digital images	Optional

5.3 Durability of card structure

Durability of the card is not established in this standard. Each jurisdiction shall select which test methods to use, if any, and what minimum acceptable criteria to use, if any, based on a mutual agreement between the jurisdiction and their card supplier. If card durability testing is required then one or more of the test methods listed in Annex G shall be used. The jurisdiction shall communicate the mutually agreed to test method and criteria information to the card supplier prior to any card procurement request.

6 Data elements

Human-readable information is information that is printed or embossed on the surface of a Driver License card. This section also describes the information that can be electronically stored on the card. Annexes specify the mapping of this information to specific technologies. Data element definitions, length, and type shall follow ANSI D20.

6.1 Description of table headings

6.1.1 Reference Number

A number for each data element used in this standard.

6.1.2 Data element/label

Data element is the clear name of the data element. When used as a human readable element the **label** is the identifying “heading” before, after, over, or under the element as it appears on the DL/ID document. The label is shown in bold under the data element name (i.e., “date of birth” would be **“d.o.b.”)**.

6.1.3 Usage

The various uses for the data element. H = human readable, M = machine readable, B = both.

6.1.4 Definition

A statement of meaning and the attributes of the data element. In the case of a different definition or format between the data element for the purposes of being **(Human)** or **(Machine)** readable, the distinction has been provided.

6.1.5 Field length and type

The valid field length for each data element. The following refer to the valid characters used (A=alpha A-Z, N=numeric, S=special) in the related application. See ANSI D20. Magnetic Stripe data element length when different has been noted.

6.1.6 Address requirement

The “mailing” related address fields were selected as the default to provide driver address information versus the “residence” optional fields. The “residence” fields may be substituted for the “mailing” fields but shall adhere to the length and type specified herein.

6.2 Required data elements

Table 1 — Required data elements

Ref. #	Data element/label	Usage	Definition	Field length & type
1	Driver License Name	B	NAME of the individual holding the Driver License or ID as defined in ANSI D20 Data Dictionary. (Lastname@Firstname@MI@ suffix if any) **(Machine**, Mag Stripe uses '**$**' and Bar Code uses '**,**' in place of '@'**)** Firstname, Middle Initial, Lastname **(Human)**	Variable 35/AS
2	Driver Mailing Street Address 1	B	The place where the registered driver of a vehicle (individual or corporation) may be contacted such as a house number, street address etc.	Variable 35/ANS Variable 29/ANS (Mag Stripe only)
3	Driver Mailing City	B	NAME OF CITY for mailing address.	Variable 20/ANS Variable max 13/ANS (Mag Stripe only)
4	Driver Mailing Jurisdiction Code	B	JURISDICTION CODE for mailing address. Conforms to Canadian, Mexican and US Jurisdictions as appropriate. Codes for provinces (Canada) and states (US and Mexico).	Fixed 2/AN
5	Driver Mailing Postal Code	B	POSTAL CODE used for mailing. (As used by Canadian, Mexican and US jurisdictions.)	Fixed 11/ANS
6	Driver License/ID Number **DL#**	B	NUMBER assigned or calculated by the jurisdiction which identifies the Driver or ID Holder.	Variable 25/AN Variable max 13/N (Mag Stripe only)
7	ID/DL # *	M (Mag Stripe only)	Overflow for numbers longer than 13 characters.	Fixed 5/N (Mag Stripe only)
8	Driver License Classification Code	B	A=Class A; B=Class B; C=Class C (Class A, B and C are defined by Federal Highway regulations); M=Class M motorcycle as defined by AAMVA; others are defined by DL Classification Code Standards.	Fixed 4/AN Fixed 2/AN (Mag Stripe only)
9	Driver License Restriction Code	B	A restriction applicable to a driver license.	Fixed 10/AN

Ref. #	Data element/label	Usage	Definition	Field length & type
10	Driver License Endorsement Code	B	Any endorsements on a driver license which authorize the operation of specified types of vehicles or the operation of vehicles carrying specified loads. Endorsements shall be specific to classification of a driver license.	Fixed 5/AN
11	Driver License Expiration Date **exp.**	B	YYMM, CCYYMMDD Year, Month, Day **(Machine)** Month, Day, Year **(Human)**	Fixed 8/N Fixed 4/N (Mag Stripe only)
12	Date of Birth **d.o.b.**	B	CCYYMMDD **(Machine)** Month, Day, Year **(Human)**	Fixed 8/N
13	Driver Sex **sex**	B	DRIVER SEX as defined by the ANSI D20 standard. **(Machine)** M for Male, F for Female **(Human)**	1/N
14	Driver License or ID Document Issue Date **iss.**	B	CCYYMMDD **(Machine)** Month, Day, Year **(Human)**	8/N
15	ISO Issuer Identifier Number (IIN)	M	This is the assigned identification number from ISO. This number shall always begin with a “6”.	Fixed 6/N
16	Driver License or Identification Card Identifier	B	Indicates that the document is a driver license or identification card, whichever is applicable.	
17	Color Photograph or Image	B	The card holder’s photograph or image.	
18	Signature **holder’s signature**	B	The card holder’s signature.	
19	Security Features	B	To deter alteration and counterfeiting.	

6.3 Optional data elements

Table 2 — Optional data elements

Ref. #	Data element/label	Usage	Definition	Field length & type
20	Height (FT/IN) **hgt**	B	FEET (1); Inches (2). Ex. 509 = 5 ft., 9 in.	3/N
21	Weight (LBS) **wgt**	B	WEIGHT in LBS.	3/N
22	Eye Color **eyes**	B	EYE COLOR as defined by the ANSI D20 standard.	3/AN
23	Hair Color **hair**	B	HAIR COLOR as defined by the ANSI D20 standard.	3/AN

Ref. #	Data element/label	Usage	Definition	Field length & type
24	Social Security Number	B	The number assigned to an individual by the Social Security Administration.	9/N
25	Driver Permit Classification Code	B	Identifies the type of permit as defined by ANSI D20.	2/A
26	Driver Permit Expiration Date	B	CCYYMMDD; Date permit expires **(Machine)** Month, Day, Year **(Human)**	8/N
27	Permit Identifier	B	Type of permit.	25/AN
28	Driver Permit Issue Date	B	CCYYMMDD; Date permit was issued. **(Machine)** Month, Day, Year **(Human)**	8/N
29	Driver Permit Restriction Code	B	PERMIT RESTRICTIONS as defined by ANSI D20.	10/AN
30	Driver Permit Endorsement Code	B	PERMIT ENDORSEMENTS as defined by ANSI D20.	6/AN
31	Driver Last Name	B (except Mag Stripe)	LAST NAME or SURNAME of the individual holding the Driver License or ID. Hyphenated names acceptable, but no other use of special symbols.	35/AN
32	Driver First Name	B (except Mag Stripe)	FIRST NAME or GIVEN NAME of the individual holding the Driver License or ID. Hyphenated names acceptable, but no other use of special symbols.	35/AN
33	Driver Middle Name or Initial	B (except Mag Stripe)	MIDDLE NAME(s) or INITIALS of the individual holding the Driver License or ID. Hyphenated names acceptable, spaces between names acceptable, but no other use of special symbols.	35/AN
34	Driver Name Suffix	B (except Mag Stripe)	An affix occurring at the end of a word, e.g.; Sr., Jr., II, III, IV, etc.	3/AN
35	Driver Name Prefix	B (except Mag Stripe)	PREFIX to Driver Name. Not defined in ANSI D20. Freeform as defined by issuing jurisdiction.	5/AN
36	Driver Mailing Street Address 2	B (except Mag Stripe)	STREET ADDRESS LINE 2. (MAILING)	35/AN
37	Driver Residence Street Address 1	B (except Mag Stripe)	STREET ADDRESS LINE 1. (MAILING)	35/AN

Ref. #	Data element/label	Usage	Definition	Field length & type
38	Driver Residence Street Address 2	B (except Mag Stripe)	STREET ADDRESS LINE 2. (MAILING)	35/AN
39	Driver Residence City	B (except Mag Stripe)	NAME OF CITY for mailing address.	20/AN
40	Driver Residence Jurisdiction Code	B (except Mag Stripe)	JURISDICTION CODE for mailing address. Conforms to Canadian, Mexican and US Jurisdictions as appropriate. Codes for provinces (Canada) and states (US and Mexico).	2/AN
41	Driver Residence Postal Code	B (except Mag Stripe)	POSTAL CODE of Residence	11/AN
42	Height (CM)	B (except Mag Stripe)	HEIGHT in CENTIMETERS	3/N
43	Weight (KG)	B (except Mag Stripe)	WEIGHT in KILOGRAMS	3/N
44	Issue Timestamp	M (except Mag Stripe)	A string used by some jurisdictions to validate the document against their data base.	26/N
45	Number of Duplicates	B (except Mag Stripe)	Number of duplicate cards issued for a license or ID if any.	2/N
46	Medical Indicator/Codes	B (except Mag Stripe)	STATE SPECIFIC. Freeform; Standard "TBD"	20/AN
47	Organ Donor	B (except Mag Stripe)	STATE SPECIFIC. Freeform; Standard "TBD"	10/AN
48	Non-Resident Indicator	B (except Mag Stripe)	"Y"; Used by some jurisdictions to indicate holder of the document is a non-resident.	1/A
49	Unique Customer Identifier	B (except Mag Stripe)	A number or alphanumeric string used by some jurisdictions to identify a "customer" across multiple data bases.	25/AN
50	Driver "AKA" Date Of Birth	B (except Mag Stripe)	ALTERNATIVE DATES(S) given as date of birth.	8/N
51	Driver "AKA" Social Security Number	B (except Mag Stripe)	FORMAT SAME AS DRIVER SOC SEC NUM. ALTERNATIVE NUMBERS(S) used as SS NUM.	9/N

Ref. #	Data element/label	Usage	Definition	Field length & type
52	Driver "AKA" Name	B (except Mag Stripe)	ALTERNATIVE NAME(S) of the individual holding the Driver License or ID. FORMAT same as defined in ANSI D20 Data Dictionary. (Lastname@Firstname@MI@ suffix if any.)	35/AN
53	Driver "AKA" Last Name	B (except Mag Stripe)	ALTERNATIVE LAST NAME or SURNAME of the individual holding the Driver License or ID. Hyphenated names acceptable, but no other use of special symbols.	35/AN
54	Driver "AKA" First Name	B (except Mag Stripe)	ALTERNATIVE FIRST NAME or GIVEN NAME of the individual holding the Driver License or ID. Hyphenated names acceptable, but no other use of special symbols.	35/AN
55	Driver "AKA" Middle Name	B (except Mag Stripe)	ALTERNATIVE MIDDLE NAME(s) or INITIALS of the individual holding the Driver License or ID. Hyphenated names acceptable, spaces between names acceptable, but no other use of special symbols.	35/AN
56	Driver "AKA" Suffix	B (except Mag Stripe)	ALTERNATIVE SUFFIX as defined in ANSI D20.	3/AN
57	Driver "AKA" Prefix	B (except Mag Stripe)	ALTERNATIVE PREFIX to Driver Name. Not defined in ANSI D20. Freeform as defined by issuing jurisdiction.	5/AN

6.4 Format conventions

6.4.1 Character set

Unless otherwise specified, the information elements are alphanumeric as defined in clause 4.

6.4.2 Format of dates

Human-readable dates shall be shown as 6 characters, "mm/dd/yy", where mm = 2-digit month, dd = 2-digit day, and yy = 2 last digits of year; or if the day is not required, as 4 characters, "mm/yy"; or if century is required, as 8 or 6 characters, "mm/dd/ccyy" or "mm/ccyy", where cc = century.

7 Physical security

7.1 Definitions

The industry definitions of overt, covert, first line inspection, second line inspection, and third line inspection are as follows and apply to this standard for the purposes of identifying and grouping the following security features.

7.1.1 Covert

Security features that are hidden in the document and are not intended to be made public. Used by Motor Vehicle Administrators and law enforcement for document authentication and forensic purposes. (**C**=Covert)

7.1.2 Overt

A security feature that is visible or apparent without requiring special instruments. May require some instruction on how to observe it. The feature may be particularly visible on the genuine document (a passive visible feature) or may only show after a copy has been made. (**O**=Overt)

7.1.3 First line inspection

Cursory examination without tools or aids involves easily identifiable visual or tactile features for rapid inspection at point of usage. (**1**=First Line Inspection)

7.1.4 Second line inspection

Examination by trained inspectors with simple equipment (magnifying glass, UV light, machine reading equipment, etc.). (**2**=Second Line Inspection)

7.1.5 Third line inspection

Inspection by forensic specialists conducting detailed examination allows for more in-depth evaluation and may require special equipment to provide true certification. (**3**=Third Line Inspection)

7.2 Physical security requirement

Jurisdictions issuing driver licenses and identification documents shall incorporate one or more overt security features (e.g., optically variable devices) designed to limit tampering, counterfeiting, photocopying, or otherwise duplicating the license or document for fraudulent purposes and to limit use of the license or document from impostors. Jurisdictions should also include one or more covert security features (e.g., machine-readable technologies) to further safeguard the license or document. Acceptable security features include, but are not limited to, the list found in Annex H of this document.

8 Encryption

This standard will not address which data should be encrypted and how. Rather, there are certain elements that must not be encrypted and conformance can be achieved only by leaving them accessible (not encrypted and readable) in one of the technology formats specified herein. Under no circumstances may any Header as defined in Section E.4.2 or the Subfile designators as defined in E.4.3 be encrypted.

Users at a minimum **shall not encrypt** the Data Elements outlined in Table 3:

Table 3 — Minimum Non-encrypted data elements

Ref. #	Data Element
1	Driver License Name
6	Driver License/ID Number
11	Driver License Expiration Date
12	Date of Birth
15	ISO Issuer Identification Number (IIN) Example: 636000 (Virginia)

NOTE It is strongly recommended that all fields be left unencrypted in order to gain the maximum benefit from the use of a Machine Readable technology. The Machine Readable information shall also be visible (human readable) on the DL/ID card as a secondary verification method. The Machine Readable information shall not be encrypted unless privacy protection acts or specific legislation mandates it by law. The Machine Readable information must give enough information on the license holder so that it is usable by the various communities as a Machine Readable verification or audit methodology.

Annex A
(normative)

Mapping of driver license/identification card information to magnetic stripe cards

Introduction

This annex defines mapping of the DL/ID card machine-readable data elements, as defined in clause 6, onto a magnetic stripe card.

A.1 Conformance

Conformance with all parts of ISO/IEC 7811-6 is required with the exception of data content and coded character sets as defined in Table A.1 and A.2.

A.2 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.

A.3 Coded character set

Tables A.1 and A.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 A.1 — Coded character set for 5 bit numeric

ASCII	Hex	Binary					ASCII	Hex	Binary				
		P	2^3	2^2	2^1	2^0			P	2^3	2^2	2^1	2^0
0	30	1	0	0	0	0	8	38	0	1	0	0	0
1	31	0	0	0	0	1	9	39	1	1	0	0	1
2	32	0	0	0	1	0	**:**	3A	1	1	0	1	0
3	33	1	0	0	1	1	**;**	3B	0	1	0	1	1
4	34	0	0	1	0	0	**<**	3C	1	1	1	0	0
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 A.2 — Coded character set for 7 bit alphanumeric

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

A. 4 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.

A.4.1 Track 1

Table A.3 — Track 1 information content and format

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

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
iv	For Fields 1 through 6 only the following characters from Table A.2 are allowed: A-Z 0-9 $ % ( ) - . / ^ ? space					

A.4.2 Track 2

Table A.4 — Track 2 information content and format

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
-	40	V-max	O	Track 2	Numeric data in 5 bit binary code for DL number, expiration date, birthdate.	see Table A.1
1	1	F	R	Start sentinel	This character shall be encoded at the beginning of the track.	;
2	6	F	R	ISO IIN	This is the assigned identification number from ISO. This number shall always begin with a "6". This number shall be obtained from the AAMVAnet Standards Program Director.	0-9
3	13	V-max	R	DL/ID#	This field is used to represent the DL/ID number assigned by each jurisdiction. Overflow for DL/ID numbers longer than 13 characters is accommodated in field number 7.	0-9
4	1	F	R	Field Separator	A field separator must be used after the DL/ID number regardless of length.	=

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
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 at the end of the 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.	?
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).						

A.4.3 Track 3

Table A.5 — Track 3 information content and format

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
-	82	V-max	O	Track 3	A/N data in 7 bit binary code for postal code, class, restrictions.	see Table A.2 and ii
1	1	F	R	Start sentinel	This character shall be encoded at the beginning of the track.	%
2	1	F	R	Version #	This field used to store the mag stripe version used.	02
3	1	F	R	Security v.#	This field used to store the	0-9

Field # in order	Length (char.)	Length fixed or variable	Req'd or optional	Name	Information	Allowable characters
					security version being used (00-63), 00 means no security being used.	
4	11	F	R	Postal code	For an 11 digit postal or zip code. (left justify fill with spaces, no hyphen)	A-Z, 0-9, space
5	2	F	R	Class	Represents the type of DL (ANSI codes modified for CDLIS).See i	A-Z, 0-9, space
6	10	F	R	Restrictions	See i, iii	A-Z, 0-9, space
7	4	F	R	Endorsements	See i, iii	A-Z, 0-9, space
8	1	F	R	Sex	M for male, F for female.	M,F
9	3	F	R	Height	See i, iii	0-9, space
10	3	F	R	Weight	See i, iii	0-9, space
11	3	F	R	Hair Color	See i, iii	A-Z, space
12	3	F	R	Eye Color	See i, iii	A-Z, space
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.					

A.5 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.

A.6 Error detection

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

Annex B
(normative)

Mapping of driver license/identification card information to integrated circuit(s) cards (ICC)

Introduction

This annex defines the mapping of the driver license/identification card data elements onto an integrated circuit card (ICC). The ICC may be either a contactless ICC or an ICC with contacts.

This annex defines:

- physical characteristics of an ICC, in addition to those characteristics specified in ISO/IEC 7810.
- location and dimensions of the contact or coupling areas,
- electrical signals to support communications between the ICC and the Interface Device (IFD);
- transmission protocols and answer to reset;
- command set;
- the file structure for the driver license/identification card application; and
- the data element mappings to the files.

All these requirements are aligned with the ISO/IEC standards for integrated circuit cards. There is one form of ICC with contacts and there are three forms of contactless ICCs. All are defined the respective groups of standards:

ISO/IEC 7816 Identification cards - Integrated circuit(s) cards with contacts
ISO/IEC 10536 Identification cards - Contactless integrated circuit(s) cards - Closely coupled cards
ISO/IEC 14443 Identification cards - Contactless integrated circuit(s) cards - Proximity cards
ISO/IEC 15693 Identification cards - Contactless integrated circuit(s) cards - Vicinity cards

This annex defines the card structure and commands to be used when the ICC card is in operation (used by the cardholder) but does not address the means used to manufacture or issue such a card. The issuance phases (initialization, personalization, distribution) are beyond the scope of this standard.

Note The choice of technologies may affect interoperablity of the ICC, especially with POS systems that have already been installed. The use the technologies defined in ISO/IEC 10536 and ISO/IEC 15693 may not be appropriate for that environment.

B.2 Physical characteristics

The physical characteristics of the ICC shall adhere to the physical characteristics specified in the standard for the respective type of card.

B.3 Location and dimensions of coupling areas

The location and dimension of the contact or coupling areas of the ICC shall adhere to the location and dimension specified in the standard for the respective type of card.

B.4 Electronic signals

The electronic signals and reset procedures are given in the standard for the respective type of card.

B.5 Transmission protocols and answer to reset

B.5.1. Transmission protocols

The driver license/identification card may support a variety of protocols in accordance with the standard for the respective type of card. Both the IFD and the ICC shall support at least the protocol T = 0 (see ISO/IEC 7816-3). Other protocols that may be used are defined in the respective standards.

B.5.2. Answer to reset

The answer to reset shall adhere to the answer to reset specified in the standard for the respective type of card. A contact ICC shall not specify a separate programming voltage. The use of historical bytes in the answer to reset is a vendor option, but shall be in compliance with the respective standard.

B.6 Application selection

ICCs may support more than one application. The driver license application shall be the default application if none is selected. There may be only one active driver license application in the ICC.

The driver license application shall be selected by use of the Application Identification (AID) as a reserved DF name. The AID shall consist of the Registered Application Identifier (RID) assigned by ISO according to ISO/IEC 7816-5. The AID shall not contain a Proprietary Application Identifier Extension (PIX). The RID is ‘A0 00 xx xx xx’.

B.7 File structure

Information on an ICC is stored in a file system defined in ISO/IEC 7816-4. The card file system is organized hierarchically into dedicated files (DFs) and elementary files (EFs). Dedicated files (DFs) contain elementary files or other dedicated files. A master file (MF) is the root of the file system.

One DF as defined by this specification contains driver license information about the cardholder. The DF has the name ‘A0 00 xx xx xx’ for the application (the registered AID) and is selected by this name. It can be placed anywhere in the DF tree attached to the MF of the card, including the MF itself.

The EFs defined by this specification store the driver license/identification information elements in a record structure. The records contain specific data elements as described in B.9. The Issuer file contains the control data elements for the issuing authority. The License data file contains the data elements for the driver license. The Photo file contains the digitized photo image if present. The issuer may use additional files for other information as desired. Additional security controls may be placed these additional files as desired.

B.8 Command set

The commands to be supported by the driver license/identification card are as follows:

- SELECT FILE by DF name (full name) to select the application

- READ RECORD by short EF identifier with a specified record number

These commands, formats, and their return codes are defined in ISO/IEC 7816-4. When a READ RECORD command is issued to the card on a file that does not exist (e.g., optional files) or that is not accessible (see clause B.10 on security), the card will return an error code according to ISO/IEC 7816-4.

Example of application selection

The application shall be selected by use of the following parameters for the APDU.

CLA	'00'
INS	'A4'
P1	'04' – (select by DF name – the AID)
P2	'00'
L_c	'05' – (length of AID)
Data field	'A0 00 xx xx xx' – (the AID)
L_e	'00' – return the application label if present

The response data field contains the application label. The label shall be 'Driver License'.

Example of reading a record from a file

The READ command shall be used to access a specific record number. This example reads record number one from the issuer file that is known by the short file identifier ’01.’ The APDU parameters for this action are shown below.

CLA	‘00’
INS	‘B2’
P1	‘01’ - specifies record number one
P2	‘0C’ - read by record number from SFI ‘01’
L_c	Empty
Data field	Empty
L_e	0 - specifies to read the entire record

The response data field contains the record.

B.9 File contents

This clause defines the mapping of the machine-readable information elements defined in clause 6. The files contain the data elements as data objects within specific records. The structure and coding of data objects are defined in ISO/IEC 7816-4 and 7816-6. Each data object has an identification tag that is specified in hexadecimal coding (for example, ‘5A’). Standard tags are used wherever possible. The tags defined in this standard use the proprietary coding option with tag values from ‘C0’ to ‘DF20’. Each data object has a unique tag, a length and a value. The data objects that may be present in a file are identified as mandatory (M) or optional (O). The definitions contain the specific reference to the data element number defined in clause 6.

This definition provides for two additional data elements that are not available with magnetic stripe or bar code technologies. These elements provide for the storage of a digitized photographic image (tag ‘5F40C’) and a digitized handwritten signature image (tag ‘5F43’) as defined in ISO/IEC 7816-6. These data elements are stored in a separate file since they may require the reading of multiple records to obtain the data.

B.9.1. EF_{ISSUER} (Issuer Information) SFI ‘01’

This EF contains the identity of the issuer of the driver license/identification card and any information related to the issuing of the driver license. The identity of the issuer in the United States is defined by the ISO IIN assigned to each state and is in data object ’42.’ In anticipation of use by other countries, the record may contain the country code of the issuer in data object ‘41’ instead. (See ISO/IEC 7816-6 for additional information.) The data objects defined below will be read as the first record in the file. Additional records with other data objects may be present in the file at the issuer’s discretion. These records are beyond the scope of this standard.

The maximum size of this record is 127 bytes.

Short EF Identifier: '01'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
'42'	Issuer Identification Number	M	Fixed - 6	N	15
'44'	Application Version Number	M	Fixed - 2	N	n/a
'DF00'	Security Version Number	M	Fixed - 2	N	n/a
'5A'	Driver License/ID Number	M	Var - 25	N or AN	6 (and 7)
'5F25'	Issue Date	M	Fixed – 8	AN	14
'DF0C'	Issue Timestamp	O	Var - 26	N	45
'DF0D'	Number of Duplicates	O	Fixed - 2	N	46
'DF08'	Unique Customer Identifier	O	Var - 25	AN	50

B.9.2. EF_{DL} (Driver License data) SFI '02'

This EF contains the required and optional data elements for the cardholder as data objects in fixed content records. The mapping of data objects to records is specified below. The contents and maximum sizes of these records are:

Record number	Contents	Maximum size
1	Mandatory data elements	201
2	Personal characteristics	192
3	Permit data elements, Residence address and mailing address	186
4	'AKA' data elements	189

The file is variable length and may contain additional records. The file must contain at least one record, the mandatory data elements.

B.9.2.1 Record 1 – mandatory data elements

Short EF Identifier: '02'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
‘42’	Issuer Identification Number	M	Fixed - 6	N	15
‘5A’	Driver License/ID Number	M	Var - 25	AN	6 (and 7)
’5F20’	Driver License Name	M	Var - 35	AS	1
’5F42’	Driver Address	M	Var - 29	ANS	2
’D7’	Driver Mailing City	M	Var - 15	AS or AN	3
‘D8’	Driver Mailing Jurisdiction Code	M	Fixed - 2	AN	4
‘D9’	Driver Mailing Postal Code	M	Fixed - 11	ANS	5
‘C0’	Driver License Classification Code	M	Fixed - 4	AN	8
‘C1’	Driver License Restriction Code	M	Fixed - 10	AN	9
‘C2’	Driver License Endorsement Code	M	Fixed - 5	AN	10
‘5F24’	Driver License Expiration Date	M	Fixed - 8	N	11
‘5F2B’	Date of Birth	M	Fixed - 8	N	12
‘5F35’	Driver Sex	M	Fixed - 1	N	13
‘5F26’	Driver License or ID Document Issue Date	M	Fixed - 8	N	14

B.9.2.2 Record 2 – personal characteristics

Short EF Identifier: '02'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
'CA' or 'DF0A'	Height (FT/IN) or Height (CM)	O	Fixed - 3	N	20 43
'CB' or 'DF0B'	Weight (LBS) or Weight (KG)	O	Fixed - 3	N	21 44
'CC'	Eye Color	O	Fixed - 3	N	22
'CD'	Hair Color	O	Fixed - 3	N	23
'D0'	Driver Last Name	O	Var – 35	AN	31
'D1'	Driver First Name	O	Var – 35	AN	32
'D2'	Driver Middle Name or Initial	O	Var – 35	AN	33
'D3'	Driver Name Suffix	O	Fixed – 3	AN	34
'D4'	Driver Name Prefix	O	Fixed – 5	AN	35
'C9'	Social Security Number	O	Fixed – 9	N	24
'DF06'	Medical Indicator/Codes	O	Var – 20	AN	47
'DF07'	Organ Donor	O	Fixed – 10	AN	48

B.9.2.3 Record 3 – permit data elements, residence address and mailing address

Short EF Identifier: '02'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
'C3'	Driver Permit Classification Code	O	Fixed - 2	A	25
'C4'	Driver Permit Expiration Date	O	Fixed - 8	N	26
'C5'	Permit Identifier	O	Fixed - 25	AN	27
'C6'	Driver Permit Issue Date	O	Fixed - 8	N	28
'C7'	Driver License Restriction Code	O	Fixed - 10	AN	29
'C8'	Driver License Endorsement Code	O	Fixed - 6	AN	30
'D5'	Driver Mailing Street Address 1	O	Var – 20	AN	36
'D6'	Driver Mailing Street Address 2	O	Var – 20	AN	37
'DA'	Driver Residence Street Address 1	O	Var – 20	AN	38
'DB'	Driver Residence Street Address 2	O	Var – 20	AN	39
'DC'	Driver Residence City	O	Var – 15	AN	40
'DD'	Driver Residence Jurisdiction Code	O	Fixed - 2	AN	41
'DE'	Driver Residence Postal Code	O	Fixed - 11	AN	42
'CE'	Non-Resident Indicator	O	Fixed - 1	A	49

B.9.2.4 Record 4 – “AKA” data elements

Short EF Identifier: '02'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
‘DF2B’	Driver "AKA" Date of Birth	O	Fixed - 8	N	51
‘DF09’	Driver "AKA" Social Security Number	O	Fixed - 9	N	52
‘DF20’	Driver "AKA" Name	O	Var – 35	AN	53
‘DF01’	Driver "AKA" Last Name	O	Var – 35	AN	54
‘DF02’	Driver "AKA" First Name	O	Var – 35	AN	55
‘DF03’	Driver "AKA" Middle Name or Initial	O	Var – 35	AN	56
‘DF04’	Driver "AKA" Name Suffix	O	Fixed - 3	AN	57
‘DF05’	Driver "AKA" Name Prefix	O	Fixed - 5	AN	58

B.9.3 EF_{MAG} (Magnetic Stripe Information) SFI ‘03’

This EF contains the image of the data contained in the magnetic stripe(s) All driver license information contained in a magnetic stripe shall be stored in this file. Any combination of the three tracks on the magnetic stripe may be present. The data shall be written in ASCII character coding structure. The data objects exclude the special characters used for start sentinel, end sentinel and LRC.

The maximum size of this record is 201 bytes.

Note The use of this data format should be maintained until the use of the magnetic stripe has been completely phased out and all interface devices (terminals) have been revised to use only the data in EF_{DL} or EF_{ISSUER}. This format may be needed during the lengthy transition process and migration to the use of the ICC in place of the magnetic stripe.

Short EF Identifier: '03'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
'56'	Track 1 in ASCII	O	Var – 79	ANS	Track 1
'57'	Track 2 in ASCII	O	Var – 37	N	Track 2
'58'	Track 3 in ASCII	O	Var - 79	AN	Track 3

B.9.4 EF_{POR} (Digitized Portrait Image) SFI '04'

This EF contains the digitized image of the cardholder's portrait image. This data element is contained in a cardholder image template '6C.' Use of the template code is optional. See ISO/IEC 7816-6 for a more detailed description of additional data elements that may be in the template. Since the data element may be large, multiple READ RECORD commands may have to be issued to obtain the full record. See ISO/IEC 7816-4 for more information.

Short EF Identifier: '04'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
'6C'	Template for digitized image information	O	Var	B	N/a
'5F40'	Portrait image (See ISO/IEC 10918-1)	O	Var	B	N/a

B.9.5 EF_{SIG} (Digitized Handwritten Signature Image) SFI '05'

This EF contains the digitized image of the cardholder's handwritten signature. This data element is contained in a cardholder image template '6C.' Use of the template code is optional. See ISO/IEC 7816-6 for a more detailed description of additional data elements that may be in the template. Since the data element may be large, multiple READ RECORD commands may have to be issued to obtain the full record. See ISO/IEC 7816-4 for more information.

Short EF Identifier: '05'H	Structure: Record	Mandatory EF

Tag	Description	M/O	Length	Char Set	Data Element
'6C'	Template for digitized image information	O	Var	B	N/a
'5F43'	Handwritten signature image (see ISO/IEC 11544)	O	Var	B	N/a

B.10 Security

ICCs can be used to secure and protect the information they contain. For example, because of privacy issues, an issuer may decide to restrict the access of some information stored in the card to the cardholder and may require a PIN for authentication. This standard does not impose any security structure. This standard does acknowledge the fact that security restrictions imposed by a given issuer may induce the IC card to reject a command when used in an incorrect security context (e.g., UPDATE RECORD of a file protected against modification such as the Issuer Number EF). A security scheme version number may be specified in the data file with the issuer information, EF_{ISSUER}.

Some of the optional data elements may require more security. These data elements may be placed in other files, with separate security constraints for each file. The recommended technique is to use the record structures defined above in another EF with the next available short file identifier: '06'H, '07'H, etc.

The magnetic stripe data in EF_{MAG} should not be encrypted and it should be available to be read by any interface device. The data in EF_{MAG} should be updated only by the issuer.

The portrait and handwritten signatures images should not be encrypted and should be available to be read by any interface device. The data in EF_{POR} and EF_{SIG} should be written once by the issuer. The security risks coincident with the ability to update these images should be carefully considered by the issuer. It is recommended that the card be reissued if this data must be changed.

B.11 Data element tags

Ref. #	Data element/label	Tag	SFI	Record
1	Driver License Name	‘5F20’	‘02’	1
2	Driver Address	‘5F42’	‘02’	1
3	Driver Mailing City	‘D7’	‘02’	1
4	Driver Mailing Jurisdiction Code	‘D8’	‘02’	1
5	Driver Mailing Postal Code	‘D9’	‘02’	1
6	Driver License/ID Number	‘5A’	‘01’ ‘02’	1 1
7	ID/DL # *	-	-	-
8	Driver License Classification Code	‘C0’	‘02’	1
9	Driver License Restriction Code	‘C1’	‘02’	1
10	Driver License Endorsement Code	‘C2’	‘02’	1
11	Driver License Expiration Date	‘5F24’	‘02’	1
12	Date of Birth	‘5F2B’	‘02’	1
13	Driver Sex	‘5F35’	‘02’	1
14	Driver License or ID Document Issue Date	‘5F26’	‘02’	1
15	ISO Issuer Identifier Number (IIN)	‘42’	‘01’ ‘02’	1 1
16	Driver License or Identification Card Identifier	‘4F’	DF name	
17	Color Photograph or Image	‘5F40’ template ‘6C’	‘04’	Multiple
18	Signature	‘5F43’ template ‘6C’	‘05’	multiple
19	Security Features **	-	-	-

Ref. #	Data element/label	Tag	SFI	Record
20	Height (FT/IN)	‘CA’	‘02’	2
21	Weight (LBS)	‘CB’	‘02’	2
22	Eye Color	‘CC’	‘02’	2
23	Hair Color	‘CD’	‘02’	2
24	Social Security Number	‘C9’	‘02’	2
25	Driver Permit Classification Code	‘C3’	‘02’	3
26	Driver Permit Expiration Date	‘C4’	‘02’	3
27	Permit Identifier	‘C5’	‘02’	3
28	Driver Permit Issue Date	‘C6’	‘02’	3
29	Driver Permit Restriction Code	‘C7’	‘02’	3
30	Driver Permit Endorsement Code	‘C8’	‘02’	3
31	Driver Last Name	‘D0’	‘02’	2
32	Driver First Name	‘D1’	‘02’	2
33	Driver Middle Name or Initial	‘D2’	‘02’	2
34	Driver Name Suffix	‘D3’	‘02’	2
35	Driver Name Prefix	‘D4’	‘02’	2
36	Driver Mailing Street Address 1	‘D5’	‘02’	3
37	Driver Mailing Street Address 2	‘D6’	‘02’	3
38	Driver Residence Street Address 1	‘DA’	‘02’	3
39	Driver Residence Street Address 2	‘DB’	‘02’	3
40	Driver Residence City	‘DC’	‘02’	3
41	Driver Residence Jurisdiction Code	‘DD’	‘02’	3
42	Driver Residence Postal Code	‘DE’	‘02’	3
43	Height (CM)	‘DF0A’	‘02’	2
44	Weight (KG)	‘DF0B’	‘02’	2
45	Issue Timestamp	‘DF0C’	‘01’	1

Ref. #	Data element/label	Tag	SFI	Record
46	Number of Duplicates	‘DF0D’	‘01’	1
47	Medical Indicator/Codes	‘DF06’	‘02’	2
48	Organ Donor	‘DF07’	‘02’	2
49	Non-Resident Indicator	‘CE’	‘02’	3
50	Unique Customer Identifier	‘DF08’	‘01’	1
51	Driver "AKA" Date Of Birth	‘DF2B’	‘02’	4
52	Driver "AKA" Social Security Number	‘DF09’	‘02’	4
53	Driver "AKA" Name	‘DF20’	‘02’	4
54	Driver "AKA" Last Name	‘DF01’	‘02’	4
55	Driver "AKA" First Name	‘DF02’	‘02’	4
56	Driver "AKA" Middle Name	‘DF03’	‘02’	4
57	Driver "AKA" Suffix	‘DF04’	‘02’	4
58	Driver "AKA" Prefix	‘DF05’	‘02’	4
	Magnetic Stripe Track 1	‘56’	‘03’	1
	Magnetic Stripe Track 3	‘57’	‘03’	1
	Magnetic Stripe Track 3	‘58’	‘03’	1
	Application version number	‘44’	‘01’	1
	Security version number	‘DF00’	‘01’	1

* The driver license number extension is included in element 6.

** The smart card provides its own security features.

Annex C
(normative)

Finger imaging

Introduction

This annex defines standards to ensure interoperability in the collection and use of finger imaging with driver license and identification cards.

C.1 Conformance

The use of finger imaging and finger image data with driver license and identification cards shall comply with the following: ANSI/NIST-CSL1-1993, CJIS/FBI IAFIS-IC-0110, and CJIS-RS-0010, BioAPI Specification Version 1.00, The BioAPI Consortium, March 30, 2000.

C.2 Application Definitions

C.2.1 Verification

A one-to-one comparison of the currently collected finger image with a previously collected finger image associated with the claimed identity being verified. The previously collected finger image may be either retrieved from a database or placed in machine readable form on the card.

C.2.2 Search

A one-to-many comparison on a database to determine the unknown identity of the individual being processed or to determine uniqueness of the individual being enrolled to ensure one identity per person. This process reduces the possibility of one person having multiple identities in the database.

C.2.3 Core

The approximate center of the fingerprint pattern as defined for the various pattern types.

C.3 Finger Selection

A Driver License or Identification Card shall include biometric data collected from a minimum of two fingers. Selection of fingers collected shall be in the following order:

1) Left Fore (Index)

2) Right Fore (Index)

3) Left Thumb

4) Right Thumb

5) Left Middle

6) Right Middle

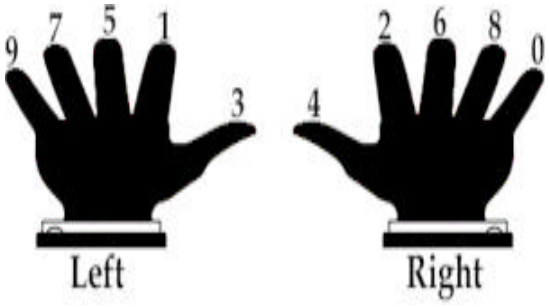
7) Left Ring

8) Right Ring

9) Left Little

0) Right Little

Figure C.1 — Finger Selection



If an individual is missing the selected finger, the next finger in this order shall be used. Where usable finger images are not available, this shall be noted in the record describing the hand configuration.

C.4 Image Quality

There are two factors in collecting quality finger images: the collection device performance and the actual quality of each image collection in terms of repeatability and consistency needed for successful matching processes.

C.4.1 Finger Image Collection Device

Finger live-scan collection devices shall conform to CJIS-RS-0010 Appendix G. This specification sets performance standards on finger image scanners for resolution, geometric image accuracy, modulation transfer function, signal-to-noise ratio, grayscale range, grayscale linearity, and grayscale uniformity.

C.4.2 Finger Image Collection Result

The imaging of the finger pattern shall result in an image in which the core of the pattern is positioned within 25% of the image center. The ridge pattern shall be clearly visible (smudge-free) with differentiable ridges and valleys for the entire area around the core.

C.5 Compression

If compression is used it shall be Criminal Justice Information Services CJIS/FBI IAFIS-IC-0110 Wavelet Scalar Quantization (WSQ). The average compression ratio applied using WSQ shall not be greater than 15:1.

C.6 Data Format

Finger image data shall be interchanged between jurisdictions using the data format specified in ANSI/NIST-CSL1-1993 "Data Format for the Interchange of Fingerprint Information". The configuration of the data shall include Record type1 Transaction information, record type 2 User-Defined Text, and record type 4 Fingerprint image data (high-resolution grayscale).

NOTE Because different AFIS use minutiae and potentially use other features extracted from the finger image to improve speed and performance, interchange between jurisdictions shall be accomplished using finger images, not minutiae data, so that the best possible matching performance can be achieved.

C.7 Minutiae Extraction Introduction

This section of the Annex provides interoperability between different finger matchers for the purposes of one-to-one verification of an individual's identity against a previously collected and stored finger record. The interoperability is based on defining the finger minutiae extraction rules and record format that are common to most all finger matchers for acceptable matching accuracy, while allowing for proprietary data to be attached so that the highest accuracy can be maintained for matching accomplished with the same matcher type.

C.8 External Standards Referenced

BioAPI Specification Version 1.00, The BioAPI Consortium, March 30, 2000

C.9 Definitions

C.9.1
Filtering
partitioning a database through the use of exogenous information about the user not discernible from the biometric patterns, such as sex, age or race

C.9.2
Friction Ridge
The ridges present on the skin of the fingers and toes, the palms and soles of the feet, which makes contact with an incident surface under normal touch. On the fingers, the unique patterns formed by the friction ridges make up *fingerprints.*

C.9.3
Live-Scan Print
a fingerprint image that is produced by scanning or imaging a live finger to generate an image of the friction ridges

C.9.4
Minutia (single)
Minutiae (pl)
Friction ridge characteristics that are used to individualize a fingerprint. *Minutiae* occur at points where a single *friction ridge* deviates from an uninterrupted flow. Deviation may take the form of ending, division, or immediate origination and termination.

C.9.5
Resolution
the number of pixels (picture elements) per unit distance in the image of the fingerprint

C.9.6
Ridge Ending
The point at which a *friction ridge* terminates or, alternatively, begins. A *ridge ending* is surrounded on three sides by valley.

C.9.7
Ridge Bifurcation
the point at which a *friction ridge* splits into two ridges or, alternatively, where two separate *friction ridges* combine into one

C.9.8
Valley
the area surrounding a *friction ridge*, which does not make contact with an incident surface under normal touch

C.10 Minutiae Description

C.10.1 Principle

Establishment of a common feature-based representation must rest on agreement on the fundamental notion for representing a fingerprint. A significant number of technology providers follow a traditional approach of encoding a fingerprint through location of “minutia” points. These minutiae are points located at the places in the fingerprint image where friction ridges end or split into two ridges. Describing a fingerprint in terms of the location and direction of these ridge endings and splits provides sufficient information to reliably determine whether two fingerprint records are from the same finger.

Fingerprint images can be represented with “light ridges” or “dark ridges”. The minutia points shall be located in such a way that the points and their directions do not change when the light and dark polarity of the image is inverted. This decision not only provides for consistent data extraction regardless of image polarity, but also ensures equal behavior of ending and bifurcation points with respect to image degradations such as noise and contrast variance. The specifications of minutia location and minutia direction described below accomplish this. See Figure C.2 for an illustration of the definitions below.

C.10.2 Minutia Type

Each minutia point has a “type” associated with it. There are two major types of minutia: a “ridge ending” and a “ridge bifurcation” or split point. There are other types of “points of interest” in the friction ridges that occur much less frequently and are more difficult to define precisely. This standard defines a category of “other” minutia for points that are not clearly a ridge ending nor a bifurcation.

C.10.3 Minutia Location

C.10.3.1 Coordinate System

The coordinate system used to express the minutia points of a fingerprint shall be a Cartesian coordinate system. Points shall be represented by their X and Y coordinates where X is increasing to the right and Y is increasing upward. Note that this is in agreement with typical mathematical graphing practice, but the direction of the Y-axis is the opposite of most imaging and image processing use. The X and Y coordinates of the minutia points shall be in pixel units, with the spatial resolution of a pixel given in the “X Resolution” and “Y Resolution” fields of the format. X and Y resolutions are stated separately.

C.10.3.2 Minutia Placement on a Ridge Ending

The minutia point for a ridge ending shall be defined as the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the valley area were thinned down to a single-pixel-wide skeleton, the point

where the three legs intersect is the location of the minutia. In simpler terms, the point where the valley “Y”’s, or (equivalently) where the three legs of the thinned valley area intersect.

C.10.3.3 Minutia Placement on a Ridge Bifurcation

In corresponding fashion, the minutia point for a ridge bifurcation shall be defined as the point of forking of the medial skeleton of the ridge. If the ridge were thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia. In simpler terms, the point where the ridge “Y”’s, or (equivalently) where the three legs of the thinned ridge intersect.

C.10.3.4 Minutia Placement on Other Minutiae Types

For minutiae other than a bifurcation or ridge ending the placement and angle of direction shall be vendor defined.

C.10.4 Minutia Direction

C.10.4.1 Angle Conventions

Angles are expressed in standard mathematical format, with zero degrees to the right and angles increasing in the counterclockwise direction.

C.10.4.2 Angle of a Ridge Ending

The angle of a ridge ending is defined as the angle of a line segment originating at the minutia point location, and extending to the end of the medial skeleton of the ridge itself. In other words, the angle of a line from the minutia point to the point at the end of the thinned ridge.

C.10.4.3 Angle of a Ridge Bifurcation

The angle of a ridge bifurcation is defined as the angle of a line segment originating at the minutia point location, and extending to the end of the medial skeleton of the area between the two ridge branches. In other words, the angle of a line from the minutia point to the endpoint of the enclosed valley.

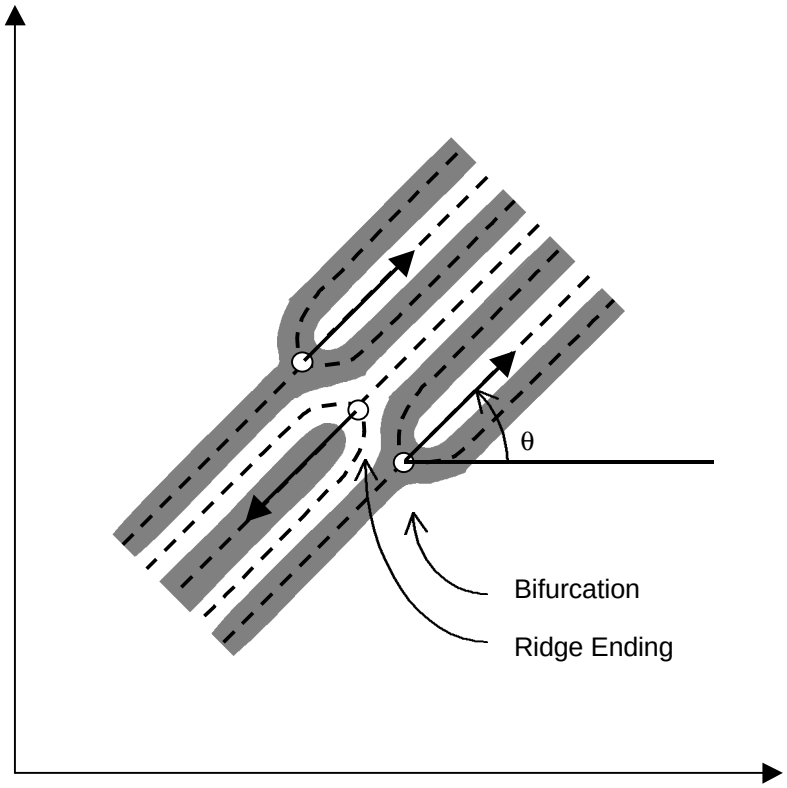


Figure C.2 - Minutia Location

C.11 Finger Minutiae Record Format

The minutiae record format shall be used to achieve interoperability between finger matchers providing a one-to-one verification. The minutia data shall be represented in a common format, containing both public and private (proprietary) data. With the exception of the Format Identifier and the Version number for the standard, which are null-terminated ASCII character strings, all data is represented in binary format. There are no record separators or field tags; fields are parsed by byte count.

All multibyte quantities are represented in Big-Endian format; that is, the more significant bytes of any multibyte quantity are stored at lower addresses in memory than (and are transmitted before) less significant bytes. All numeric values are fixed-length integer quantities, and are unsigned quantities.

The organization of the record is as follows:

- A fixed-length (26-byte) record header containing information about the overall record, including the number of fingers represented and the overall record length in bytes;
- A Single Finger record for each finger, consisting of:
    - A fixed-length (4-byte) header containing information about the data for a single finger, including the number of minutiae;
    - A series of fixed-length(6-byte) minutia point descriptions, including the position, type, angle and quality of the minutia point;
- One private data areas for each finger, containing vendor-specific information.

C.11.1 Record Header

There shall be one and only one record header for minutiae record to hold information describing the identity and characteristics of device that generated the minutiae data.

C.11.1.1 Format Identifier

The Finger Minutiae Record shall begin with the three ASCII characters “FMR” to identify the record as following this standard, followed by a zero byte as a NULL string terminator.

C.11.1.2 Version Number

The version number for the version of this standard used in constructing the minutiae record shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major revision number and the third character will represent the minor revision number.

Upon approval of this specification, the version number shall be “ 10” (an ASCII space followed by an ASCII ‘1’ and an ASCII ‘0’).

C.11.1.3 Length of Record

The length of the entire record shall be recorded in two bytes.

C.11.1.4 System Vendor ID

These two bytes shall uniquely identify the vendor or “owner” of the encoding equipment. This “owner code” shall use values defined and maintained by the International Biometric Industry Association (www.ibia.org). A value of zero will not be allowed.

C.11.1.5 Feature Extraction Software ID

The feature extraction version shall be recorded in two bytes. A value of all zeros will be acceptable and will indicate that the SW ID is unreported. The value of this field is determined by the vendor. Applications developers may obtain the values for these codes from the vendor.

C.11.1.6 Scanner ID

The scanner ID shall be recorded in two bytes. A value of all zeros will be acceptable and will indicate that the scanner ID is unreported. The value of this field is determined by the vendor. Applications developers may obtain the values for these codes from the vendor.

C.11.1.7 Size of Scanned Image in X direction

The size of the original image in pixels in the X direction shall be contained in two bytes.

C.11.1.8 Size of Scanned Image in Y direction

The size of the original image in pixels in the Y direction shall be contained in two bytes.

C.11.1.9 Scan Rate in X direction

The resolution of the finger scanner shall be recorded in two bytes having the units of pixels per centimeter. The value of the sensor X resolution shall not be zero.

C.11.1.10 Scan Rate in Y direction

The resolution of the finger scanner shall be recorded in two bytes having the units of pixels per centimeter. The value of the sensor Y resolution shall not be zero.

C.11.1.11 Number Of Fingers

The number of fingers contained in the minutiae record shall be recorded in one byte.

C.11.1.12 Reserved Byte

A single byte is reserved for future revision of this specification. For Version 1.0 of this standard, this byte must be set to 0.

C.11.2 Single Finger Record Format

C.11.2.1 Finger Header

A finger header shall start each section of finger data providing information for that finger. There shall be one finger header for each finger contained in the finger minutiae record. The finger header will occupy a total of four bytes as described below. Note that it is permissible for more than one finger record to represent the same finger, with (presumably) different data, perhaps in the private area.

C.11.2.1.1 Finger Position

The finger position shall be recorded in one byte. The codes for this byte shall be as defined in Table 5 of ANSI/NIST-CSL 1-1993, “Data Format for the Interchange of Fingerprint Information”. This table is reproduced here for convenience. Only codes 0 through 10 shall be used; the “plain” codes are not relevant for this standard.

Table C.1 - Finger Position codes

Finger position	Code
Unknown finger	0
Right thumb	1
Right index finger	2
Right middle finger	3
Right ring finger	4
Right little finger	5
Left thumb	6
Left index finger	7
Left middle finger	8
Left ring finger	9
Left little finger	10
Plain right thumb	*11*
Plain left thumb	*12*
Plain right four fingers	*13*
Plain left four fingers	*14*

C.11.2.1.2 Impression Type

The impression type of the finger images that the minutiae data was derived from shall be recorded in one byte. The codes for this byte shall be as defined in Table 4 of ANSI/NIST-CSL 1-1993, “Data Format for the Interchange of Fingerprint Information”. This table is reproduced here for convenience. Only codes 0 through 3 shall be used; the “latent” codes are not relevant for this standard.

Table C.2 - Impression Type codes

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3
Latent impression	*4*
Latent tracing	*5*
Latent photo	*6*
Latent lift	*7*

C.11.2.1.3 Finger Quality

The quality of the overall finger minutiae data shall be between 0 and 100 and recorded in one byte. This quality number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutia record. A value of 0 shall represent the lowest possible quality and the value 100 shall represent the higher possible quality. The numeric values in this field will be set in accordance with the general guidelines contained in Section 2.1.42 of the “BioAPI H-Level Specification Version 1.00”. This value may be used by the matcher to determine its certainty of verification.

C.11.2.1.4 Number of Minutiae

The number of minutiae recorded for the finger shall be recorded in one byte.

C.11.2.2 Finger Minutiae Data

The finger minutiae data for a single finger shall be recorded in blocks of six bytes per minutia point. The order of the minutiae is not specified.

C.11.2.2.1 Minutiae Type

The type of minutiae will be recorded in the first two bits of the upper byte of the X coordinate. There will be two bits reserved at the beginning of the upper byte of the Y coordinate for future use. The bits “00” will represent a minutia of “other” type, “01” will represent a ridge ending and “10” will represent a bifurcation.

C.11.2.2.2 Minutiae Position

The X coordinate of the minutia shall be recorded in the rest of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header. Note that position information shall be present for each minutia point, regardless of type, although position for minutiae of type “other” is vendor defined.

C.11.2.2.3 Minutiae Angle

The angle of the minutia shall be recorded in one byte in units of 2 degrees. The value shall be a non-negative value between 0 and 179, inclusive. For example, an angle value of 5 represents 10 degrees. Note that angle information shall be present for each minutia point, regardless of type, although angle for minutiae of type “other” is vendor defined.

C.11.2.2.4 Minutiae Quality

The quality of each minutia shall be recorded in one byte. The quality figure shall range from 100 as a maximum to 1 as a minimum. Any equipment that does not supply quality information for individual minutia points shall set all quality values to 0.

C.11.3 Proprietary Data

The optional section of the finger minutiae record is open to placing proprietary data required by the matcher to maintain its highest performance level. The size of this section should be kept as small as possible, augmenting the data stored in the standard minutiae section. The proprietary data for each finger shall immediately follow the standard minutiae data.

C.11.3.1 Type Identification Code

The type identification code shall be recorded in two bytes, and shall distinguish the format of the private area (as defined by the Vendor specified in field C.11.1.4). A value of zero shall indicate that there is no following proprietary data. This code shall be maintained by the vendor.

C.11.3.2 Length of Data

The length of the proprietary data section, including the vendor identification and length of data fields, shall be recorded in two bytes. This value is used to skip to the next finger minutiae data if the matcher cannot decode and use this data. If the type identification (field C.11.3.1) for the private area is zero, indicating no private data, this field shall not be present.

C.11.3.3 Private Data

The data field of the proprietary data is specifically defined by the equipment that is generating the finger minutiae record. If the type identification (field C.11.3.1) for the private area is zero, indicating no private data, this field shall not be present.

Minutiae Record Format Summary

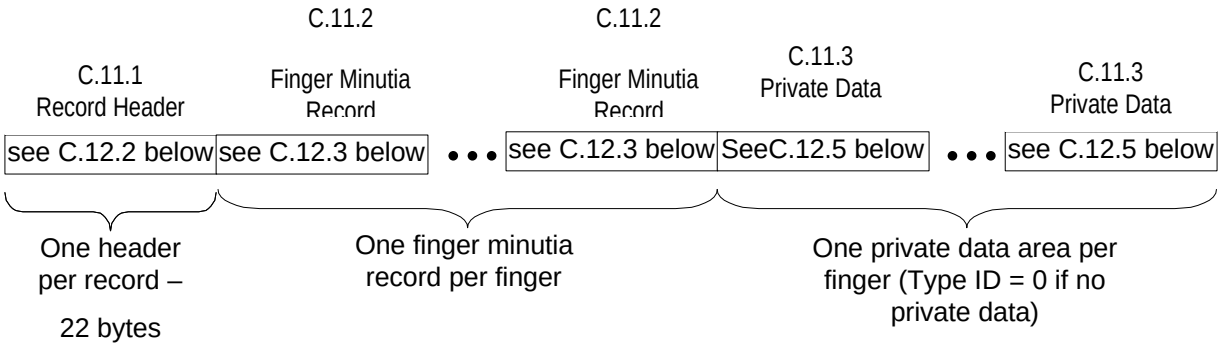
The following table is a reference for the fields present in the Finger Minutia Record format. For more specific information, please refer to the text and to the Record Format Diagrams in the next section.

Table C.3 - Minutia Record Format Summary

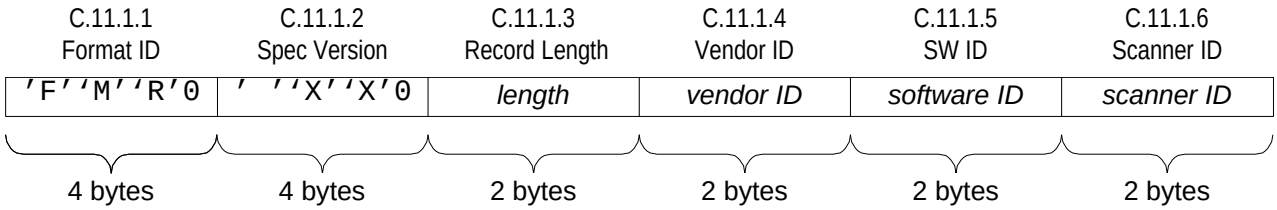
	Field	Size	Valid Values	Notes
record	Format Identifier	4 bytes	'F' 'M' 'R' 0x0	"FMR " – finger minutiae record
	Version of this standard	4 bytes	n n n 0x0	" XX"
	Length of total record	2 bytes	>= 26	In bytes
	Scan System			
	Vendor / Format owner ID	2 bytes		Registration authority controlled
	Feature Extraction SW Ver.	2 bytes		Vendor specified
	Scanner ID	2 bytes		Vendor specified
	Image Size in X	2 bytes		in pixels
	Image Size in Y	2 bytes		in pixels
	Sensor X Resolution	2 bytes		in pixels per cm
	Sensor Y Resolution	2 bytes		in pixels per cm
	Number of Fingers	1 byte		
	Reserved	1 byte	0x00	Always 0x00 currently
finger	Finger Position	1 byte	0 to 11	Refer to ANSI/NIST standard
	Impression Type	1 byte	0 to 3	Refer to ANSI/NIST standard
	Finger Quality	1 byte	0 to 100	0 to 100
	Number of Minutiae	1 byte		
minutia	X (minutia type in upper 2 bits)	2 byte		Expressed in image pixels
	Y (upper 2 bits reserved)	2 byte		Expressed in image pixels
	θ	1 byte	0 to 180	Resolution is 2 degrees
	Quality	1 byte	0 to 100	1 to 100 (0 indicates "quality not reported")
finger	Type Code for Private Area	2 bytes		0x0000 = no private area
	Length of private feature area	2 bytes		only present if Type Code non-zero
	Private feature area	Specified in previous field		only present if Type Code non-zero

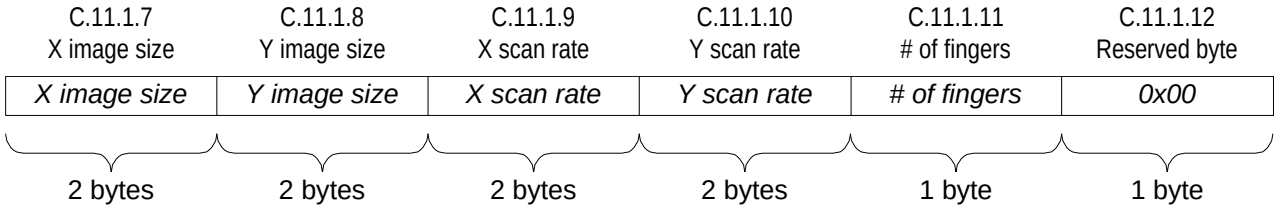
C.12 Record Format Diagrams

C.12.1 Overall Record Format

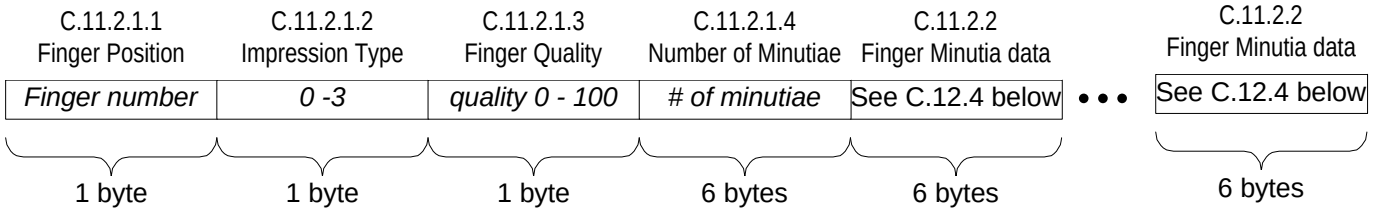


C.12.2 Record Header

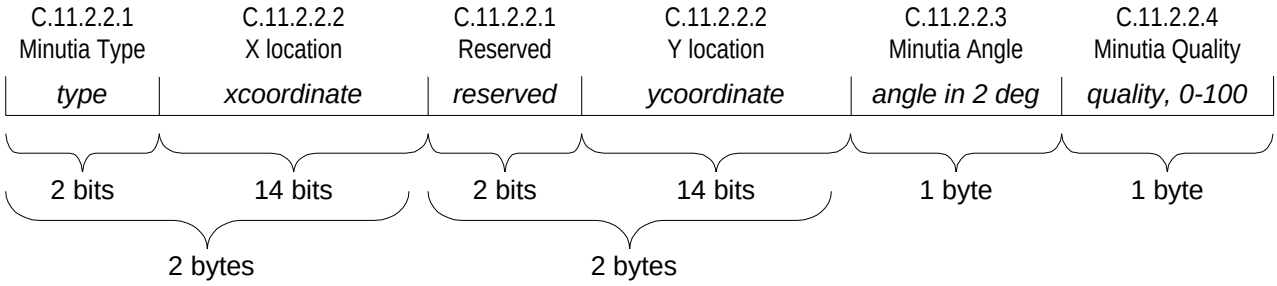




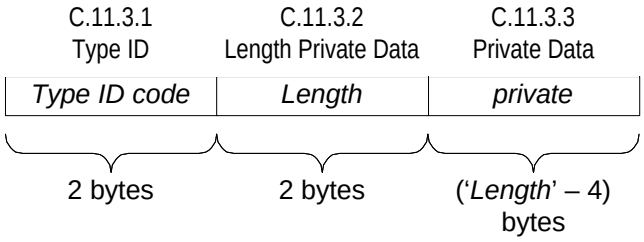
C.12.3 Single Finger Minutia Record



C.12.4 Finger Minutiae Data



C.12.5 Private (Proprietary) Data



C.13 Interoperable Matcher Performance (Informative)

The concept of operation for 1 to 1 verification matching is as follows. All compliant equipment will provide a minutia records consisting of at least the public areas defined above. Based on the data contained in these fields, and the common definitions of minutia points and their locations and angles, all compliant vendors will be able to achieve some reasonably high level of performance in verifying a live sample against the public record. This is represented by “Algorithm B” matching in the diagram below. Note that “Algorithm A” produces the record, and “Algorithm B” reads only the public area.

However, the optimum in performance (defined as minimal False Accept Rate and False Reject Rate) may be achieved by using proprietary methods and features. To allow vendors to support this enhanced level of performance, the proprietary or “private” data area allows additional data to be present. If the reading and matching equipment can interpret and make use of this additional data (either because the same vendor supplies it, or because of cross-licensing of technology or other collaboration), then higher levels of performance may be achieved. This situation is represented by “Algorithm A” matching below.

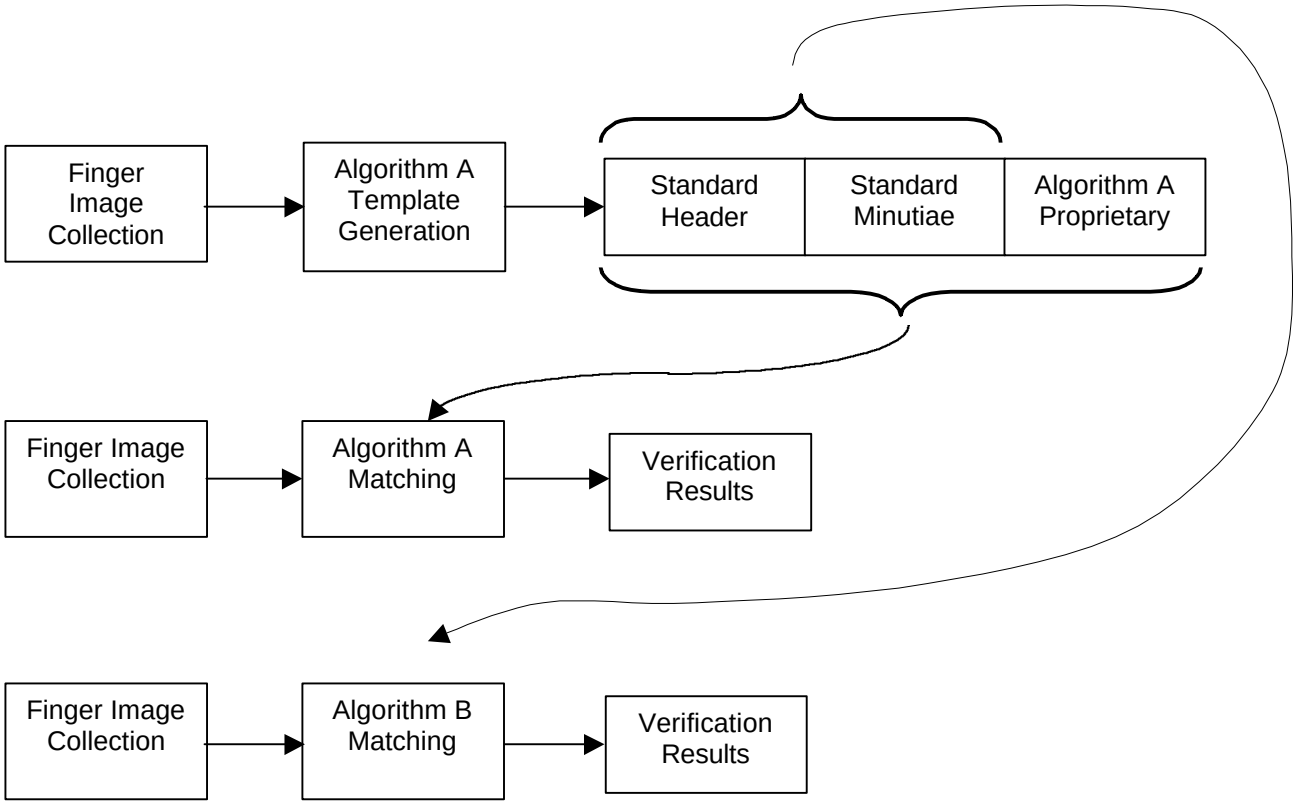


Figure C.3 - Interoperability Concept

C.14 Compliance (Informative)

Interoperability of one-to-one matching relies on each matcher to adhere within a tolerance to the determination of the minutiae. Compliance with this specification is important in two areas: format compliance and minutiae extraction accuracy.

Testing for compliance is not described in this standard; refer to applicable Best Practices documents for further description.

C.14.1 Record format compliance

Equipment and algorithms that are compliant with this standard must observe the format and syntax described herein. This includes: order and size of fields, presence of all required fields, adherence to range limits on values, and internal consistency (the number of single finger records must match the number of fingers, for example).

C.14.2 Finger Minutiae Extraction

Finger images of sufficiently good quality should generate minutiae records that are “sufficiently similar” for all compliant equipment and algorithms. This is essential to the underlying goal of interoperability. Testing for this requirement may consist of encoding and formatting of data from a test set of sample images, with a known set of minutiae features. The equipment under test may be evaluated based on the number of minutiae points that differ from the known standard by a significant degree, and on the number of minutiae points detected by one system and not the other. Standards for these metrics (degree of difference, allowable numbers of differences) are dependent on the specific application.

C.15 Example MInutiae Record (Informative)

This example minutiae record demonstrates the format for a given set of data.

C.15.1 Data

Scan System: Vendor ID = 0x42, Feature Extraction SW Version code 0x11, Scanner ID = 0x00B5
(these values are determined by the IBIA (for the Vendor ID) and by the vendor)

Sensor Resolution: 500 dpi in both X and Y axes; 196.85 pixels per cm, Image was 512 by 512 pixels

Plain live-scan prints of the left and right index fingers

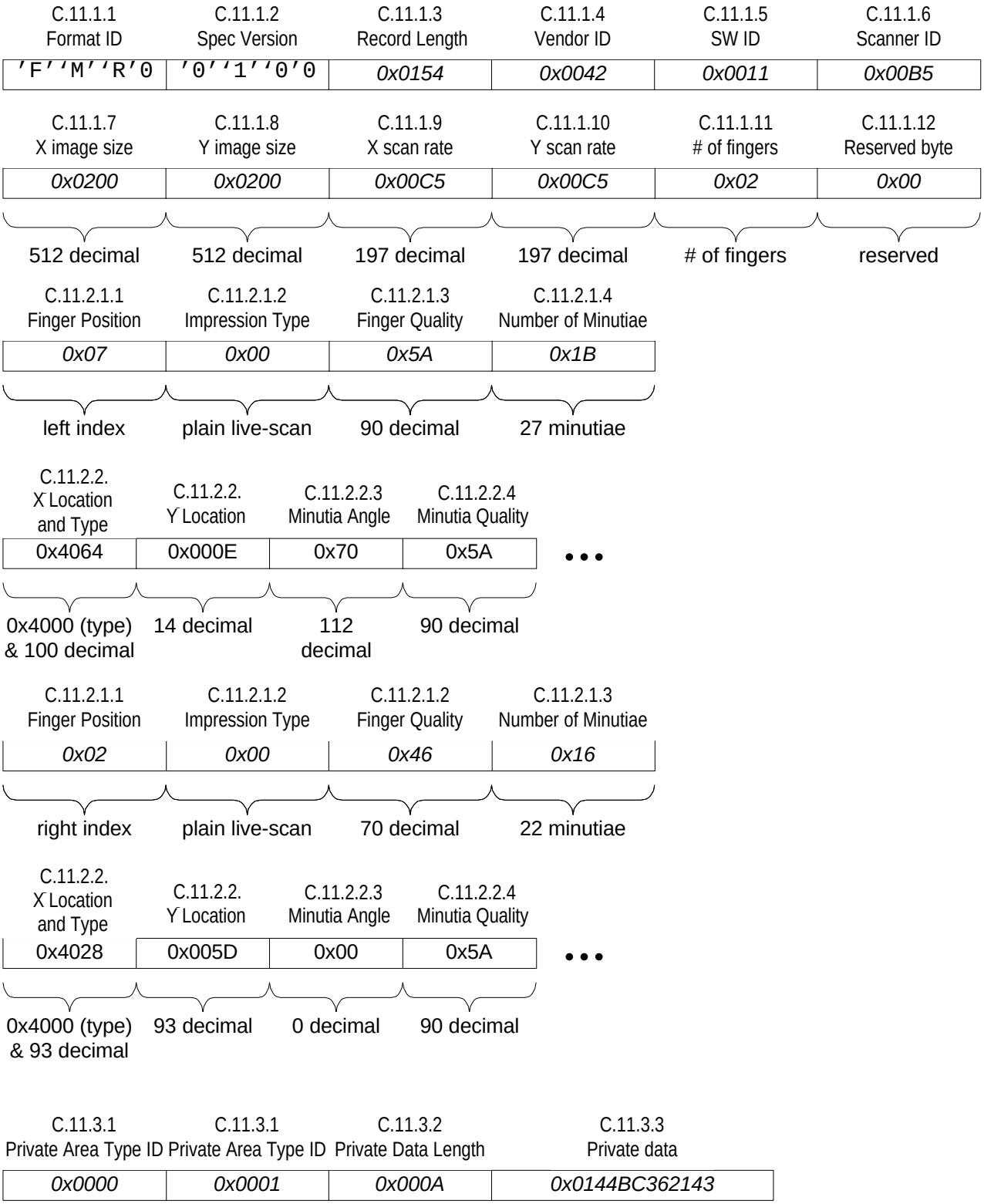
Left Index: Finger quality is 90% of the maximum possible
27 minutia, listed in table below.
No private feature data

Right Index: Finger quality is 70% of the maximum possible
22 minutia, listed in table below.
Private feature data area (Type 01) consisting of six bytes: 0x01, 0x44, 0xBC, 0x36, 0x21, 0x43

Record length = 340 = 26 (record header) + 2 * 4 (finger headers) + 27 * 6 (minutia for 1st finger) + 22 * 6 (minutia for 2nd finger) + 2 (null private area for 1st finger) + 10 (private area for 2nd finger)

Minutia #	Left Index Finger					Right Index Finger				
	Type	X	Y	Angle	quality	Type	X	Y	Angle	quality
0	Ending	100	14	112	90	ending	40	93	0	90
1	Ending	164	17	85	80	bifurcation	116	100	0	80
2	Bifurcation	55	18	22	90	ending	82	95	12	70
3	Bifurcation	74	22	76	60	bifurcation	140	113	15	70
4	Ending	112	22	90	80	ending	122	135	18	80
5	Bifurcation	42	31	44	90	bifurcation	55	72	21	50
6	Bifurcation	147	35	51	90	ending	94	74	24	60
7	Ending	88	38	165	40	ending	155	62	42	80
8	Bifurcation	43	42	4	80	bifurcation	42	64	55	70
9	Ending	56	48	33	70	ending	155	85	59	80
10	Ending	132	49	72	90	bifurcation	96	192	62	80
11	Bifurcation	71	50	66	80	ending	114	86	85	80
12	Other	95	51	81	90	bifurcation	142	90	90	70
13	Ending	112	53	132	50	ending	57	137	90	90
14	Bifurcation	135	58	32	80	ending	131	75	90	80
15	Other	41	60	59	70	ending	45	113	98	80
16	Bifurcation	67	62	145	90	bifurcation	111	171	114	50
17	Ending	91	63	132	80	ending	95	62	156	60
18	Ending	112	65	33	60	bifurcation	61	114	165	80
19	Ending	53	71	45	90	bifurcation	143	72	171	80
20	Bifurcation	104	74	12	80	ending	63	104	172	70
21	Ending	75	79	21	90	bifurcation	125	73	173	40
22	Bifurcation	48	80	92	90					
23	Ending	130	89	45	80					
24	Bifurcation	63	95	126	80					
25	Ending	47	108	164	90					
26	Bifurcation	126	115	172	30					

C.15.2 Example Data Format Diagrams



C.15.3 Raw Data for the Resulting Minutiae Record

Record Header:

0x464D5200303130000154004200110 0B50200020000C500C50200

1st Finger Header:

0x07005A1B

1st Finger Minutiae data:

0x4064000E705A	0x40A400115550	0x80370012165A
0x804A00164C3C	0x407000165A50	0x802A001F2C5A
0x80930023335A	0x40580026A528	0x802B002A0450
0x403800302146	0x40840031485A	0x804700324250
0x005F0033515A	0x407000358432	0x8087003A2050
0x0029003C3B46	0x8043003E915A	0x405B003F8450
0x40700041213C	0x403500472D5A	0x8068004A0C50
0x404B004F155A	0x803000505C5A	0x408200592D50
0x803F005F7E50	0x402F006CA45A	0x807E0073AC1E

2nd Finger Header:

0x02004616

2nd Finger Minutiae data:

0x4028005D005A	0x807400640050	0x4052005F0C46
0x808C00710F46	0x407A00871250	0x803700481532
0x405E004A183C	0x409B003E2A50	0x802A00403746
0x409B00553B50	0x806000C03E50	0x407200565550
0x808E005A5A46	0x403900895A5A	0x4083004B5A50
0x402D00716250	0x806F00AB7232	0x405F003E9C3C
0x803D0072A550	0x808F0048AB50	0x403F0068AC46
0x807D0049AD28		

1st Private Data Area:

0x0000

2nd Private Data Area:

0x0001000A0144BC362143

Annex D
(normative)

Mapping of driver license/identification card information to optical memory cards

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.

D.1 Conformance

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

D.2 File location

The Information content of the magnetic stripe, defined in annex A 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 A.4. Unused sectors in the first and last user data tracks shall be reserved for future use.

D.3 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 E
(normative)

Mapping of driver license/identification card information to 2 dimensional bar codes

Introduction

This annex defines mapping of the driver license/identification card machine-readable information elements, as defined in clause 6, onto a 2 Dimensional bar code.

E.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.

E.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 application.

For the Drivers License Application, 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

E.3 Card Characteristics

E.3.1 Symbology Characteristics

The symbology characteristics shall conform to ISO/IEC 15438.

E.3.2 Dimensions and Print Quality

E.3.2.1 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.

E.3.2.2 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.

E.3.2.3 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.

E.3.2.4 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.

For the drivers license application the minimum symbol grade shall be 3.5/10/660, where:

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

Measurement Aperture = .250mm (0.010 inch)

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

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

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

E.3.2.5 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.

E.3.2.6 Symbol Durability

If Bar Code Symbol durability is required then the test method in Annex G, G.5, should be used.

E.3.3 Bar code area

The bar code area shall be located on the back side of the drivers license card. 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”).

E.3.4 Orientation and Placement

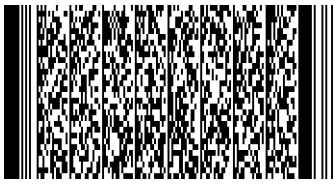
E.3.4.1 PDF417 Orientation

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

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

E.3.4.2 Designing the Card Layout

Figure E.1 — Orientation of PDF417 symbol on bottom



Plan for the maximum amount of data:

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

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

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

E.4 Information contents and formats

E.4.1 Data Structure

All compliant 2D symbols shall employ a HEADER which shall allow interested parties to interpret the encoded data. SUBFILES shall be employed to carry the specific information. The combination of a HEADER and one or more SUBFILE DESIGNATORS shall make up a compliant 2D symbol.

Each 2-Dimensional bar code shall begin with a file header that will identify the bar code as complying with the standard. The header shall be followed by a Subfile Designator “DL” to identify the Drivers License data type stored in the file. Each data element contained in a Subfile shall be prefaced by a Field Identifier as defined in E.4.4.1 and E.4.4.2. The use of a field separator character shall serve to both terminate a field and indicate the presence of a following field identifier.

E.4.2 Header

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

Table E.1 — 2D symbols header format

Field	Bytes	Contents
1	1	**Compliance Indicator:** A 2D symbol encoded according to the rules of this standard shall include a Compliance Indicator. The Compliance Indicator as defined by this standard is the Commercial At Sign (“@”) (ASCII/ISO 646 Decimal “64”) (ASCII/ISO 646 Hex “40”). The Compliance Indicator is the first character of the symbol.

Field	Bytes	Contents
2	1	**Data Element Separator:** The Data Element Separator is used in this standard to indicate that a new data element is to follow, *and* that the current field is terminated. Whenever a Data Element Separator is encountered (within a Subfile type which uses Data Element Separators), the next character(s) shall either be a Segment Terminator or shall define the contents of the next field according to the template of the specific Subfile. The Data Element Separator as defined by this standard is the Line Feed character ("$^{L}_{F}$" ASCII/ISO 646 Decimal "10") (ASCII/ISO 646 Hex "0A"). The Data Element Separator is the second character of the symbol.
3	1	**Record Separator:** The Record Separator as defined by this standard is the Record Separator character ("$^{R}_{S}$" ASCII/ISO 646 Decimal "30") (ASCII/ISO 646 Hex "1E"). As this report is presented for ratification, there is no special case defined for when this field will be used. It is embodied within the recommendation for future growth. The Record Separator is the third character of the symbol and shall always be reflected within the header in a compliant symbol.
4	1	**Segment Terminator:** As used in this standard the Segment Terminator is used to end Subfiles where Field Identifiers are employed. The Segment Terminator as defined by this standard is the Carriage Return character ("$^{C}_{R}$" ASCII/ISO 646 Decimal "13") (ASCII/ISO 646 Hex "0D"). The Segment Terminator is the fourth character of the symbol.
5	5	**File Type:** This is the designator that identifies the file as an AAMVA compliant format. The designator is defined as the 5 byte upper character string "ANSI ", with a blank space after the fourth character .
6	6	**Issuer Identification Number (IIN):** This number uniquely identifies the issuing jurisdiction and can be obtained by contacting the ISO Issuing Authority (AAMVA).
7	2	**Version Number:** This is a decimal value between "0 and 63", that specifies the version level of the Hi-Density bar code format. Version "0" is reserved for bar codes printed to the specification of the American Association of Motor Vehicle Administrators (AAMVA) prior to the adoption of this AAMVA National Standard. All bar codes compliant with this standard shall be designated Version "1" and are likely to remain Version "1", but should a need arise requiring major revision to the format, this field provides the means to accommodate revision.
8	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* which 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.

E.4.3 Subfile Designator

All compliant 2D bar code symbols must contain the "DL" subfile structure as defined below immediately after the Header as defined in E.4.2.

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 Drivers License Subfile type containing Required and Optional data elements as defined in Sections 6.2, E.4.4.1 and E.4.4.2. Any jurisdiction has the right to define a Subfile Type to contain jurisdiction specific information provided that the Subfile type is a 2 character uppercase character field whose first character is "Z".
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.

E.4.4 Elements

Tables E.4.4.1 and E.4.4.2 define required and optional data elements which may be included in the "DL" subfile type. Jurisdiction specific data elements may also be encoded provided that the Bar Code ID is a 3 character uppercase character field beginning with "Z" Jurisdiction specific data elements shall be stored in a "Z" subfile type.

E.4.4.1 Required

Data Element	Ref. #	Bar Code ID
Driver License Name	1	DAA
Driver Mailing Street Address 1	2	DAG
Driver Mailing City	3	DAI
Driver Mailing Jurisdiction Code	4	DAJ
Driver Mailing Postal Code	5	DAK
Driver License/ID Number	6	DAQ
Driver License Classification Code	8	DAR
Driver License Restriction Code	9	DAS
Driver License Endorsements Code	10	DAT
Driver License Expiration Date	11	DBA
Date of Birth	12	DBB
Driver Sex	13	DBC
Driver License or ID Document Issue Date	14	DBD

E.4.4.2 Optional

Data Element	Ref. #	Bar Code ID
Height (FT/IN)	20	DAU
Weight (LBS)	21	DAW

Data Element	Ref. #	Bar Code ID
Eye Color	22	DAY
Hair Color	23	DAZ
Social Security Number	24	DBK
Driver Permit Classification Code	25	PAA
Driver Permit Expiration Date	26	PAB
Permit Identifier	27	PAC
Driver Permit Issue Date	28	PAD
Driver Permit Restriction Code	29	PAE
Driver Permit Endorsement Code	30	PAF
Driver Last Name	31	DAB
Driver First Name	32	DAC
Driver Middle Name or Initial	33	DAD
Driver Name Suffix	34	DAE
Driver Name Prefix	35	DAF
Driver Mailing Street Address 2	36	DAH
Driver Residence Street Address 1	37	DAL
Driver Residence Street Address 2	38	DAM
Driver Residence City	39	DAN
Driver Residence Jurisdiction Code	40	DAO
Driver Residence Postal Code	41	DAP
Height (CM)	42	DAV
Weight (KG)	43	DAX
Issue Timestamp	44	DBE
Number of Duplicates	45	DBF
Medical Indicator/Codes	46	DBG
Organ Donor	47	DBH
Non-Resident Indicator	48	DBI
Unique Customer Identifier	49	DBJ
Driver "AKA" Date Of Birth	50	DBL
Driver "AKA" Social Security Number	51	DBM
Driver "AKA" Name	52	DBN
Driver "AKA" Last Name	53	DBO
Driver "AKA" First Name	54	DBP
Driver "AKA" Middle Name	55	DBQ
Driver "AKA" Suffix	56	DBR
Driver "AKA" Prefix	57	DBS

E.4.5 Example of 2D Symbol

Following is an example of a 2D symbol printed in accordance with this standard and containing the following information:

Drivers License Number:	0123456789ABC
Driver License Name:	John Q Public
Driver Street Address:	123 Main Street
Driver Mailing City:	Anytown
Driver Mailing Jurisdiction Code:	VA
Driver Mailing Postal Code:	123459999
Driver Class Code(s):	DM
DL Restriction Codes:	(none)

Driver License Endorsements:	(none)
Height:	509
Weight:	175
Eye Color:	BL
Hair Color:	BR
DL Expiration Date:	20011201
Date of Birth:	19761123
Driver Sex:	M
Driver License Document Issue Date:	19961201
Jurisdiction Defined Code:	JURISDICTIONDEFINEDELEMENT

when decoded would result in a data stream as follows (Note: β = Blank):

@$^{L}_{F}$ $^{R}_{S}$ $^{C}_{R}$ANSIβ6360000102**DL**00390187**ZV**02260031**DL*DAQ***0123456789ABC$^{L}_{F}$

DAAPUBLIC,JOHN,Q$^{L}_{F}$***DAG***123βMAINβSTREET$^{L}_{F}$***DAI***ANYTOWN$^{L}_{F}$***DAJ***VA$^{L}_{F}$***DAK***123459999ββ$^{L}_{F}$

DARDMββ$^{L}_{F}$***DAS***βββββββββββ$^{L}_{F}$***DAT***βββββ$^{L}_{F}$***DAU***509$^{L}_{F}$***DAW***175$^{L}_{F}$***DAY***BLβ$^{L}_{F}$***DAZ***BRβ$^{L}_{F}$***DBA***20011201$^{L}_{F}$

DBB19761123$^{L}_{F}$***DBC***M$^{L}_{F}$***DBD***19961201$^{C}_{R}$**ZV*ZVA***JURISDICTIONDEFINEDELEMENT$^{C}_{R}$

This data, when broken down further, can be better understood as:

HEADER,

@ the first character in any compliant 2D symbol

$^{L}_{F}$ the character to represent a Data Element Separator

$^{R}_{S}$ the character to represent a Record Separator

$^{C}_{R}$ the character used represent a Segment Terminator

ANSIβ which indicates that the symbol meets the AAMVA National Standard, and a blank space

636000 which indicates the jurisdiction (Virginia) that printed the symbol

01 which indicates that the rest of the data follows version 1 of the AAMVA National Standard

02 which indicates the number of Subfile Designators and indicates (in this example) that two follow

SUBFILE DESIGNATOR,

DL and **ZV** indicates the subfile types

DL (Drivers License)

0039 which indicates the offset from the beginning of the symbol to the start of the related subfile

0187 which indicates the length of the subfile type

ZV (Jurisdiction Defined)

0226 which indicates the offset from the beginning of the symbol to the start of the related Subfile

0031 which indicates the length of the Subfile type

SUBFILE DATA,

DL which is the Subfile Identifier

DAQ0123456789ABC$^{L}_{F}$ which is the Field Identifier (FI) for our example, which would mean a Drivers License Number follows, and a 13 position Drivers License Number, and Data Element Separator (DES)

DAAPUBLIC,JOHN,Q$^{L}_{F}$ which is the FI for Name, the Name with required separators, and DES

DAG123βMAINβSTREET$^{L}_{F}$ which is the FI for Street Address, the Street Address, and DES

DAIANYTOWN$^{L}_{F}$ which is the FI for City, and the City, and DES

DAJVA$^{L}_{F}$ which is the FI for Jurisdiction Code, and the Jurisdiction Code, and DES

DAK123459999ββ$^{L}_{F}$ which is the FI for Postal Code, the Postal Code padded to an 11 digit fixed length, and DES

DARDMββ$^{L}_{F}$ which is the FI for Class Code, the Class Code padded to 4 digit fixed length, and DES

DASβββββββββββ$^{L}_{F}$ which is the FI for the ANSI D-20 Restriction Codes, and the Restriction Codes padded to 10 digit fixed length, and the DES

DATβββββ$^{L}_{F}$ which is the FI for the ANSI D-20 License Endorsements, and the Endorsements padded to 5 digit fixed length, and the DES

DAU509$^{L}_{F}$ which is the FI for Height, and the Height (ft/in), and DES

DAW175$^{L}_{F}$ which is the FI for Weight, the weight in lbs, and DES

DAYBLβ$^{L}_{F}$ which is the FI for Eye Color, the ANSI D-20 Eye Color, and DES

DAZBRβ$^{L}_{F}$ which is the FI for Hair Color, the ANSI D-20 Hair Color, and DES

DBA20011201$^{L}_{F}$ which is the FI for Expiration Date, the Expiration Date (YYYYMMDD), and DES

DBB19761123$^{L}_{F}$ which is the FI for Birthdate, the Birthdate (YYYYMMDD), and DES

DBCM$^{L}_{F}$ which is the FI for Sex, the ANSI D-20 Sex Code, and DES

DBD19961201 which is the FI for Document Issues Date, the Date (YYYYMMDD)

$^{C}_{R}$ which is a Segment Terminator

ZV which is the Subfile Identifier

ZVA JURISDICTIONDEFINEDELEMENT which is the FI for a Jurisdiction Defined Data Element, and the data

$^{C}_{R}$ which is a Segment Terminator.

E.5 Error Detection and Correction

PDF417 symbols shall use a minimum Error Correction Level of 3. Where space allows, an Error Correction Level of 5 is recommended.

E.6 Character Sets

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

E.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.

Annex F
(normative)

Driver license/identification card compression for digital imaging

Introduction

This annex contains the required elements to use JPEG and Greyscale compression for Storage and Transmission of images between jurisdictions.

F.1 Conformance

A License or Identification Card photo and signature image that incorporates Storage and Transmission of said images shall comply with the following: ISO 10918-1 and ITU-T Group III and IV.

F.2 Definitions

F.2.1
binary
Binary refers to black and white images. The data bit is either on or off.

F.2.2
CCITT
CCITT is the current standard for binary image compression. Primarily used in fax transmissions, CCITT Groups III and IV were defined by the International Consultative Committee on Telegraph and Telephone. CCITT was reorganized in 1993 and is now known as ITU-T.

F.2.3
color
a continuous tone image that has more than one component

F.2.4
Continuous Tone Image
an image whose components have more than one bit per sample

F.2.5
Gray Scale
a continuous tone image that has only one component

F.2.6
JPEG
JPEG is the proposed compression standard for continuous tone images. It was published in 1993 as ISO 10918-1 and ITU-T T.81. It was produced by the Joint Photographic Experts Group.

F.2.7
pixel
a pixel is a picture element - one of an n by m matrix of picture elements, where n is across (horizontal) and m is down (vertical)

F.2.8
Still Image (Digital)
a set of two-dimensional arrays of data

F.2.9
TIFF (Tagged Image File Format)
industry accepted practice for storing image information

F.2.10
(Adaptive) (Binary) Arithmetic Encoder
an entropy encoding procedure, which codes by means of a recursive subdivision of the probability of the sequence of symbols coded up to that point

F.2.11
(Uniform) Quantization
the procedure by which discrete cosine transform (DCT) coefficients are linearly scaled in order to achieve compression

F.2.12
8x8 Block
an 8x8 array of samples

F.2.13
Component
one of the two-dimensional arrays which comprise an image

F.2.14
Compressed Image Data
a coded representation of an image

F.2.15
compression
reduction in the number of bits used to represent source image data

F.2.16
Controlled Quality (Lossy)
A descriptive term for encoding and decoding processes which are not lossless. Controlled quality compression allows for varying compression ratios at various quality levels.

F.2.17
decoding process
a process, which takes as its input, compressed image data and outputs a continuous tone image

F.2.18
encoding process
a process, which takes as its input a continuous tone image and outputs compressed image data

F.2.19
entropy decoder
a lossless procedure which recovers the sequence of symbols from the sequence of bits produced by the entropy encoder

F.2.20
entropy encoder
a lossless procedure which translates a sequence of input symbols into a sequence of bits such that the average number of bits per symbol approaches the entropy of the input symbols

F.2.21
hierarchical
A method of encoding an image in which the first frame for a given component is followed by frames which code the differences between the source data and the reconstructed data from the previous frame for that component. Resolution changes are allowed between frames.

F.2.22
Huffman Encoder
an entropy encoding procedure which assigns a variable length code to each input symbol

F.2.23
Huffman Table
the set of variable length codes required in a Huffman encoder and Huffman decoder

F.2.24
Interchange Format
the representation of compressed image data for exchange between application environments

F.2.25
interleaved
the descriptive term applied to the repetitive multiplexing of small groups of data units from each component in a scan in a specific order

F.2.26
JFIF (JPEG File Interchange Format)
JFIF is a minimal file format, which enables JPEG bit streams to be exchanged between a wide variety of platforms and applications

F.2.27
lossless
a descriptive term for encoding and decoding procedures in which it is guaranteed that no information is lost from input to output

F.2.28
non-interleaved
the descriptive term applied to the data unit processing sequence when the scan has only one component

F.2.29
Progressive (Coding)
one of the DCT-based or hierarchical processes defined in the JPEG standard in which each scan typically improves the quality of the reconstructed image

F.2.30
quantization tables
the set of 64 scalar quantization values used to the DCT coefficients

F.2.31
Run (Length)
number of consecutive symbols of the same value

F.2.32
Sample
one element in the two-dimensional array which comprises a component

F.2.33
scan
a single pass through the data for one or more of the components in an image

F.2.34
Sequential (Coding)
one of the lossless or DCT-based coding processes defined in the JPEG standard in which each component of the image is encoded within a single scan

F.3 Information Contents and Formats

F.3.1 Requirements for Photographs and Signatures

F.3.1.1 Color Photo Images

Table F.3 defines the recommended requirement for color photo images by shading in the options recommended for licensing/identification applications.

F.3.1.1.1 Image Data Formats

The image header can define the image size, the number of bits per pixel, the scan start and scan order. This allows any application to process the images appropriately. For color photo images, 16 bits per pixel or 24 bits per pixel are required. Typically, 16 bit acquisition devices are less expensive than 24 bit and give good quality results. If the compression is 16 bit Y,Cb,Cr, then the input of 16 bit 5R,6G,5B or 5R,5G,5B or 6R,6G,4B or 24 bit RGB doesn't matter.

F.3.1.1.2 Image Compression Standard

For color photo images, the JPEG baseline defined to be controlled quality, 8 bit per component, sequential DCT with Huffman coding is required.

F.3.1.1.3 Associated JPEG Parameters

F.3.1.1.3.1 Interchange Format

Tables F.1 and F.2 specify the recommended file interchange format. This file interchange format is in the spirit of JFIF and adds application specific information.

Table F.1 — Recommended File Interchange Format

Field	Length (in bytes)	Comments
SOP	2	Start of Packet
Non JPEG	2	Indicates start of non-JPEG data
Length	2	Application data segment length
* Version	3	JPEG version
Units	1	Units for the X and Y densities: units =0: no units, X & Y specific aspect ratio units =1: X & Y are dots per inch units =2: X & Y are dots per centimeter

Field	Length (in bytes)	Comments
X density	2	Horizontal pixel density
Y density	2	Vertical pixel density
X size	2	Horizontal size based on units (in/cm)
Y size	2	Vertical size based on units (in/cm)
* Color Space	1	O=Y , Cb, Cr
Scan Order	1	Orientation of Image: 0 = 0 degrees, 1 = 90, 2 = 180, 3 = 270 (degrees in navigational terms)
Annotation	1-255	NULL terminated string could include name license number, etc.
X'FF', SOI	2	Start of Image (JPEG)
** X'FF', DQT Length Quantization Table Parameters	2+N *65 (see Table F.2 Comments)	N_q = number of quantization tables
** X'FF', DHT Length Huffman Table Parameters	2+N*(17+m) (see Table F.2 Comments)	N_h = Number of Huffman tables m=Σ of number of codes of lengths 1 - 16
X'FF', SOFO Length Frame Parameters	8+3*N (see Table F.2 Comments)	N_f = Number of image components in a frame
X'FF', SOS Length Scan Parameters (entropy coded scan data)	6+2*N (see Table F.2 Comments)	N_s = Number of image components in a scan
X'FF', EOI	2	End of image
EOP	2	End of Packet

Table F.2 — Recommended file interchange format

Comments:

- All the AAMVA specific information and tables shall be "sent" once in an abbreviated stream to minimize overhead cost.
- Type of compression, number of lines, and number of samples per line are included in the frame header.
- $N_q = N_h = 2$ for color $N_q = N_h = 1$ for gray scale
  $N_f = N_s = 3$ for color $N_f = N_s = 1$ for gray scale

For Color:

- 1st component C1 = 1= Y component
- 2nd component C2 = 2 = Cb component
- 3rd component C3 = 3 = Cr component

* Information is included for flexibility in the event of future changes

** Allows for a JPEG abbreviated table stream: X'FF', SOI, X'FF', DQT, table(s), DHT, table(s), X'FF', EOI where the tables are sent once before the first image and not with subsequent images.

F.3.1.1.3.2 Color Space Translation

TIFF and JFIF (JPEG File Interchange Format) suggest the CCIR recommendation 601-1 and the associated translation to Y,Cb,Cr as shown below:

Y = 0.299R + 0.587G + 0.114B

Cb = 128 - 0.1687R - 0.3313G + 0.5B

Cr = 128 + 0.5R - 0.4187G - 0.0813B

If the numbers exceed 255, they shall be clamped at 255. Similarly, if they under flow, they shall be clamped at zero (0).

Table F.3 — Required for color images

CATEGORY	DECISION POINTS	
Image Data Formats	• Size • Scan Start • Scan Order • Pixel Format	
Bits Per Pixel	16 or 24	8, 10, 12, 32
Standard	JPEG Baseline • Controlled Quality • 8 Bit per Component; • Sequential DCT; • Huffman Coding; and • Restart Codes	JPEG Extension • Lossless; • Progressive DCT; • Arithmetic Coding; & • Greater than 8 bits
Conversion Scheme	Left Justify	
Color Space Translation	R,G,B to Y, Cb, Cr	Other Color Space Options • RGB CMYK HIS Others
Interleaved	Yes	No
Subsampling ratio	2 Horizontal & 2 Vertical 2 Horizontal No Subsampling	Any Combination of • 1, 2, 3, or 4 Horizontal & • 1, 2, 3, or 4 Vertical
Huffman Tables	Send Once	Send with Each Data Stream
Quantization tables	Send Once	Send with Each Data Stream

F.3.1.1.4 Options to Optimize Performance

F.3.1.1.4.1 Sub sampling

It is required that the CrCb band subsampling be one of the following two options.

NOTE The intensity band Y is never subsampled.

— Every other sample in the horizontal and the vertical directions.

— Every other sample in the horizontal direction only, no subsampling in the vertical direction.

F.3.1.1.4.2 Interleaving

It is required that the data be interleaved and compressed as Y, then Cb, then Cr.

F.3.1.1.4.3 Table Signaling

It is required that both the Huffman Tables and Quantization Tables be sent one time.

F.3.1.2 Signatures

Tables F.4 and F.5 define the specifications for signatures by shading in the required elements for licensing / identification applications.

F.3.1.2.1 Image Data Formats

The image header can define the image size, the number of bits per pixel, the scan start and scan order. This allows any application to process the images appropriately. For signature images, 8 bits per pixel gray scale *or binary* images are required.

F.3.1.2.2 Image Compression Methods

— For Gray Scale signatures use the shaded portions of Table F.4.

— For binary signatures use the shaded portions of Table F.5.

Table F.4 — Requirements for signatures gray scale

CATEGORY	DECISION POINTS				
Image Type	Gray Scale			Binary	
Bits per Pixel	8	• 4 • 10 • 12		1	
Standards *	JPEG Baseline • Controlled Quality; • 8 Bit per Component; • Sequential DCT; and • Huffman Coding	JPEG Extension • Lossless; • Progressive DCT; • Arithmetic Coding; and • Greater than 8 bits		CCITT Group III	CCITT Group IV
Conversion Scheme	Left Justify			Not Applicable	
Quantization Tables	Send Once	Send with each Data Stream		Not Applicable	
Huffman Tables	Send Once	Send with each Data Stream		Not Applicable	
Image Data Formats	• Size • Scan Start • Scan Order • Pixel Format				
Dimensionality	Not Applicable		1	2	2 Only

Table F.5 — Requirements for Signatures Binary

CATEGORY	DECISION POINTS				
Image Type	Gray Scale			Binary	
Bits per Pixel	8	• 4 • 10 • 12		1	
Standards *	JPEG Baseline • Controlled Quality; • 8 Bit per Component; • Sequential DCT; and • Huffman Coding	JPEG Extension • Lossless; • Progressive DCT; • Arithmetic Coding; and • Greater than 8 bits		CCITT Group III	CCITT Group IV
Conversion Scheme	Left Justify			Not Applicable	
Quantization Tables	Send Once	Send with each Data Stream		Not Applicable	
Huffman Tables	Send Once	Send with each Data Stream		Not Applicable	
Image Data Formats	• Size • Scan Start • Scan Order • Pixel Format				
Dimensionality	Not Applicable		1	2	2 Only

F.3.1.3 Associated JPEG Parameters

F.3.1.3.1 Interchange Format

The recommended file interchange can be found in Table F.2. This interchange file format is intended to give the receiver of image transmission a method of converting the images from one Pre-JPEG or JPEG image format to another for viewing or printing.

F.3.1.4 Options to Optimize Performance

F.3.1.4.1 Table Signaling

It is required that both the Huffman Tables and Quantization Tables be sent one time.

F.4 Signature Compressed Vector Format

Signatures collected from digital signature tablets where the data takes the form of a list of x, y coordinates, the compressed vector format may be used to losslessly store and transmit this data. The Signature Compressed Vector Data format shall consist of a file header followed by a variable length field containing the vector data. The top left coordinate of a signature shall be taken as the origin (0, 0). The x coordinate shall be defined as the horizontal coordinate increasing to the right. The y coordinate shall be defined as the vertical coordinate increasing in the downward direction.

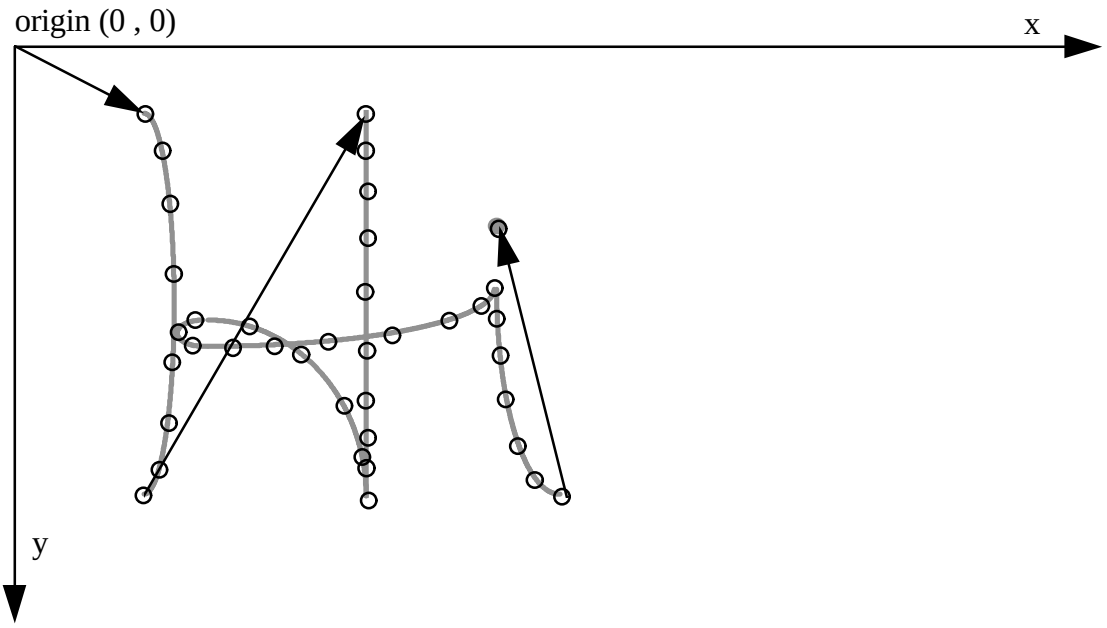


Figure F.1 Signature format

F.4.1 File Header Format

The file header shall consist of the identifying 3 byte tag “SIG” (hexadecimal values 53, 49, 47) followed by the x and y resolution of the tablet and the number of points in the vector data portion.

F.4.1.1 Horizontal Resolution

The horizontal resolution of the signature shall be recorded in 2 bytes as an integer number representing pixels per inch.

F.4.1.2 Vertical Resolution

The vertical resolution of the signature shall be recorded in 2 bytes as an integer number representing pixels per inch.

F.4.1.3 Number of Vectors

The number of vectors contained in the vector data shall be recorded as an integer number in 2 bytes.

F.4.2 Vector Data Format

The list of x, y coordinates shall be processed in the order recorded during the signature. All coordinates shall be represented as a vector from the previously recorded point (X – previous X, Y – previous Y). The first vector of a signature shall be considered to be taken from the top left coordinate (0, 0). Each vector shall be recorded with the offset in x first, then the offset in y. Each offset shall be recorded either as a small offset or a large offset. Both offsets in a vector need not be recorded using the same offset format. Each vector shall indicate a pen movement of nonzero distance. It is not allowed to represent no movement of the pen using a vector of (0, 0), because this is reserved to indicated the lifting of the pen.

F.4.2.1 Small Offset

A small offset shall be any difference greater than or equal to –63 and less than or equal to 63. A small offset shall be recorded in one byte, where the most significant bit set 0 and the next significant bit is the sign bit followed by 6 bits of magnitude. The sign bit shall be set to 1 if the offset is negative, 0 otherwise.

F.4.2.2 Large Offset

A large offset shall be any difference less than –63 or greater than 63. A larger offset shall be recorded in two bytes, where the most significant bit set 1 and the next significant bit is the sign bit, followed by 14 bits of magnitude. The sign bit shall be set to 1 if the offset is negative, 0 otherwise.

F.4.2.3 Pen Lift

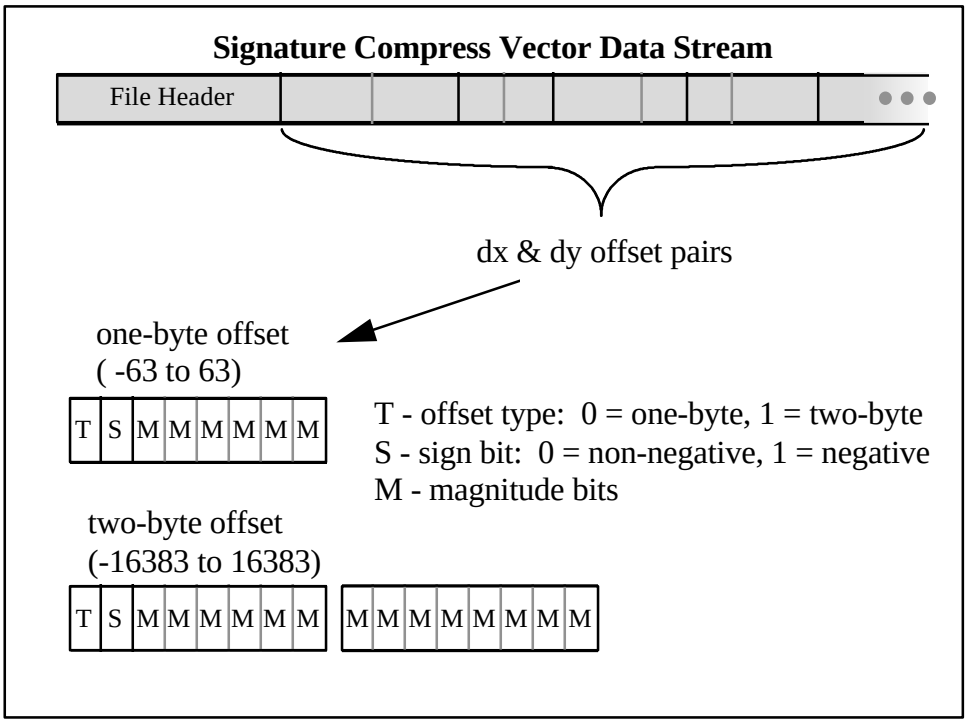


Figure F.2 Signature data stream

The lifting of the pen shall be represented as a vector of (0, 0) in the vector data. The vector following an pen lift vector (0, 0) shall indicate the jump to the next pen down of the signature from the point just before the pen lift vector. The pen lift offset shall be counted as a vector for the number of vectors parameter in the file header. There is no requirement to end the signature with a pen lift offset.

F.5 Digital Images

Digital Images shall be placed in, but not limited to, four categories:

- Category A: Digital Facial Portrait Images
- Category B: Digital Signature Images
- Category C: Digital Finger Images (See Finger Imaging Annex C)
- Category D: Ghosted Images

F.5.1 Category A - Facial Portrait Image (Capture)

F.5.1.1 Pose

The full-face or frontal pose is the most commonly used pose in driver licenses.

F.5.1.2 Depth of Field

The subject's captured facial image shall always be in focus from the nose to the ears.

F.5.1.3 Centering

The facial image being captured (full-face pose) shall be positioned to satisfy all of the following conditions:

a) The approximate horizontal midpoints of the mouth and of the bridge of the nose shall lie on an imaginary vertical straight line positioned at the horizontal center of the image. See line AA in Figure 3.

b) An imaginary horizontal line through the center of the subject's eyes shall be located at approximately the 55% point of the vertical distance up from the bottom edge of the captured image. See line BB in Figure 3.

c) The width of the subject's head shall occupy approximately 50% of the width of the total image width. This width shall be the horizontal distance between the midpoints of two imaginary vertical lines. Each imaginary line shall be drawn between the upper and lower lobes of each ear and shall be positioned where the external ear connects to the head. See line CC in Figure 3.

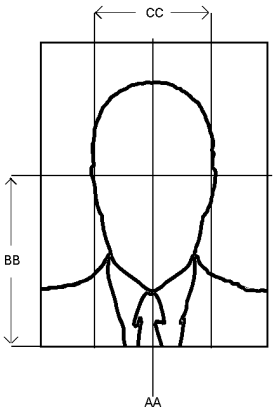


Figure F.3 Centering facial image

F.5.1.4 Lighting

Adequate lighting shall be used to fully illuminate the subject during capture. Appropriate techniques shall also be employed and light(s) positioned to minimize shadows and hot spots on the facial image.

F.5.1.5 Background

The subject whose image is being captured for the purposes of issuing a general drivers license document shall be positioned in front of a blue background.

It is desired that utilization of a single color backdrop will allow for easier exchange and usage of previously captured images between jurisdictions.

NOTE Currently 48 US and 8 Canadian jurisdictions utilize a blue color background for general driver licenses.

F.5.1.6 Aspect Ratio

The Width:Height aspect ratio of the facial portrait image shall be in accordance with the universal camera standard of 1:1.333 for portrait images.

Cropping of the original captured image prior to compression and storage is permissible provided that the cropping technique maintains the specified aspect ratio of 1:1.333 and the minimum and maximum pixel width:height requirement and the image is stored with the defined aspect ratio above.

Applications outside of Driver Licensing utilizing the images for reproduction, display, etc. shall adhere to the defined aspect ratio.

F.5.1.7 Color Space

Captured electronic color facial images shall adhere to the Color Space Translation requirements in F.3.1.1.3.2.

Additional color management techniques are available from the International Color Consortium. Information regarding these techniques can be downloaded from the following URL: http://www.color.org

F.5.1.8 Compression Algorithm

The algorithm used to compress facial portrait images shall conform to the JPEG Sequential Baseline mode of operation as described in Table F.3.

NOTE Applications which utilize the compressed JPEG facial portrait image may have to perform an analysis of the information contained within the graphic file for external purposes. (i.e., Facial Recognition Matching Algorithm) A significant loss of data resulting from image compression may interfere with these processes. The compression and lossy values utilized should accommodate such external uses as may be necessary.

F.5.1.9 File Format

Please refer to the Transmission section F.3 of this Annex.

F.5.2 Category A - Facial Portrait Image (Document)

F.5.2.1 Aspect Ratio

The width:height aspect ratio of the printed facial portrait image shall be 1:1.333, in accordance with the capture aspect ratio in Section F.5.1.6.

F.5.2.2 Facial Portrait Image Dimensions

The minimum width:height of a facial portrait image printed on a driver license document shall be 25.4 millimeters (1.000 inches) in the horizontal direction by 33.9 millimeters (1.333 inches) in the vertical direction.

F.5.2.3 Borders

Colored borders or frames surrounding the facial portrait image are optional and may present useful purposes in distinguishing various driver license types. These borders shall adhere to the following rules:

a) Borders shall not overlap nor interfere with the human-readable functionality of the facial portrait image.

b) Borders shall not obstruct the data contained within the image nor reduce or alter the image aspect ratio of 1.1.333.

c) Borders shall not form part of the original captured, stored or compressed facial portrait image, but shall be applied through utilization of preprinting or another method during the production of the finished document.

F.5.3 Category B - Signature Images (Capture)

F.5.3.1 Digitization

Any method of converting a handwritten signature into a digital format for the purpose of inclusion on a driver license document must meet the following criteria:

Manual or automatic resizing or cropping of the captured image shall not alter the width:height aspect ratio of the original signature.

a) A target aspect ratio of 4:1 width:height shall be utilized.

b) Cropping of the signature shall maintain the target 4:1 width/height aspect ratio.

c) The minimum (100 pixels per inch) resolution requirements shall be met.

F.5.3.2 Compression and Storage

Refer to section F.3 of this annex.

F.5.3.3 File Format

Refer to section F.3 of the annex.

F.5.4 Category B - Signature Images (Document)

F.5.4.1 Aspect Ratio

The target width:height aspect ratio of the printed signature image shall be 4:1, in accordance with the capture aspect ratio in Section F.5.3.1 above.

F.5.4.2 Signature Image Dimensions

The minimum width:height of a printed signature image on a driver license document shall be 25.4 millimeters (1.000 inches) in the horizontal direction by 6.35 millimeters (0.25 inches) in the vertical direction.

F.5.4.3 Borders

Colored borders or frames surrounding the signature image are optional and may present useful purposes in distinguishing various driver license types. These borders shall adhere to the following rules:

a) Borders shall not overlap nor interfere with the human-readable functionality of the signature image.

b) Borders shall not obstruct the data contained within the image nor reduce or alter the signature image aspect ratio of 4:1.

c) Borders shall not form part of the original captured, stored or compressed signature image, but shall be applied through utilization of preprinting or another method during the production of the finished document.

F.5.5 Category C - Finger Images (Capture)

F.5.5.1 Standards

The electronic capture and storage of finger image data is relatively new to the digital imaging industry and as such there remains a lack of internationally recognized standards for the capture, quality, minutiae extraction, storage, security, and exchange of resulting data. However, the following standards have been established and form a basis for the capture and storage of electronic finger image data, and provide the image formats necessary to perform future applications that may be required:

— *ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information*, ANSI, November 22, 1993.

— *WSQ Gray-Scale Fingerprint Image Compression Specification*, IAFIS-IC-0110V2, Criminal Justice Information Services (CJIS), Federal Bureau of Investigation, February 16, 1993.

Refer to annex C of this document for finger imaging standards.

F.5.6 Category C - Finger Images (Document)

Please refer to the applicable machine readable Annex sections of this document in regard to storing finger image data on a document.

F.5.7 Category D - Ghosted Images (Capture)

Ghosted images refer to the increased reduction in data of an existing facial portrait image that has been decreased in intensity, contrast and often overall dimensions.

Ghosted images used in a driver license document are utilized as an added form of security. For this purpose the “ghosted” image shall refer to a duplication of the Facial Portrait Image manipulated during the card personalization process and shall utilize those specifications in subclause F.5.1. in regard to capture and storage.

The ghosted image is not generally a separate image for the purposes of storage but most commonly a mechanical or electrical manipulation of the existing primary facial portrait image.

F.5.8 Category D - Ghosted Images (Document)

No standards exist for the utilization of ghosted images; however, the following guidelines shall be applied when ghosted images are applied to a driver license document:

a) The ghosted image utilized in a driver license document shall utilize the exact same Facial Portrait Image that appears on the same document.

b) The ghosted image shall be easily recognizable by human-readable means as a replication of the Facial Portrait Image contained elsewhere on the same document.

c) The ghosted image shall not interfere with the ability to recognize and decipher any human-readable or machine-readable data contained elsewhere on the document.

d) The ghosted image shall maintain the aspect ratio specified in subclause F.5.1, consistent with the facial portrait image.

Annex G
(normative)

Test Methods

Introduction (informative)

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

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

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

G.1 Scope

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

G.2 Conformance

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

G.3 Normative references

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

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

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

G.4 Terms and definitions

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

G.4.1 card service life

period of time between card issuance and expiration date

G.5 Test methods and sample size

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

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

ANSI NCITS 322 recommended sample size (Informative)

Clause	Test description	Card orientation NA = not applicable	Typical sample size # cards
5.1	Delamination-90 degrees	NA	6
5.2	Delamination-180 degrees	NA	6
5.3	Delamination-Heat Transfer Film Layers	NA	6
5.4	ID-1 Card Flexure	axis A, face up	4
		axis A, face down	4
		axis B, face up	4
		axis B, face down	4
5.5	ID-1 Card Static Stress	axis A, face up	25
		axis A, face down	25
		axis B, face up	25
		axis B, face down	25

5.6	ID-1 Card Stress and Plasticizer Exposure	axis A, face up	4
		axis A, face down	4
		axis B, face up	4
		axis B, face down	4
5.7	Impact Resistance	NA	25
5.8	Card Structural Integrity	NA	15
5.9	Surface Abrasion	NA	6
5.10	Bar Code Abrasion	NA	6
5.11	Mag Stripe Abrasion	NA	6
5.12	Image Abrasion	NA	6
5.13	Temperature and Humidity Induces Dye Migration	NA	6
5.14	Plasticizer Induced Dye Migration	NA	6 sets of 5
5.15	Ultraviolet (UV) Light Exposure Stability	test both sides of card	6
5.16	Daylight Image Stability-Xenon Arc	test both sides of card	6
5.17	Laundry Test	NA	6
5.18	Embossed Character Retention-Pressure	NA	6
5.19	Embossed Character Retention-Heat	NA	6

ISO 10373-1 recommended sample size (Informative)

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

G.6 Test report

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

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

Annex H
(informative)

Physical security features for the driver license/identification card

Introduction

This annex represents a sample of possible physical security features that may be used in the construction of a DL/ID. This is NOT an all inclusive list and is for informational purposes only.

H.1 Features

(**C** = Covert, **O** = Overt, **1** = First Line Inspection, **2** = Second Line Inspection, **3** = Third Line Inspection)

(O1) Core Inclusion - It is possible to manufacture a plastic document with several different layers of core stock. A colored core material can be added to the card construction to create a colored edge along the card. This technique is currently used in the new INS Work Permit Card as a means of identifying a genuine document.

(C2/3) Deliberate Errors or Known Flaws - A feature or attribute known only to the manufacturer or inspection officials.

(O2) Directional Metamerism - Directional metamerism refers to the use of colors that differ in spectral composition but match one another under certain lighting conditions. Using this technique, designs can be created that will show colors that appear to be identical under incandescent light but, under colored light, appear as different colors and patterns.

(O1) Embossed Characters - Embossing is the impressing of raised characters to render a tactile pattern. The raised characters will also render the card uneven/not flat, thereby making the card more difficult to reprint. It is possible to develop unique embossing characters or logos that would not be included in commercially available embossers.

(C1/2) Fine Line Background - Commonly called "guilloche patterns," this detailing prevents accurate reproduction by copiers or standard document scanners, especially when used in conjunction with Rainbow Printing. A fine line background is constructed by using two or more intricately overlapping bands that repeat a lacy, web-like curve pattern on fine unbroken lines.

(O1) Ghost Image or Ghost Printing - Digital printing technology has made possible the printing of a "ghost" image, a half tone reproduction of the original image, which is typically printed in the same area as the personal data. The second image appears as a light background to text data, significantly increasing the difficulty of altering the photo image or the data.

(O1) Holograms - A hologram is a microscopically fine diffraction structure by which two or three-dimensional images are generated. The metallized reflective hologram has been a security feature for Visa and MasterCard cards for more than 10 years. The intrinsic security of the hologram results from a moveable image when viewed from different angles. It is not receptive to photography, photocopying, or scanning, and it requires highly specialized equipment to replicate designs.

(C2/3) Ink Taggants - Special inks have been formulated with specific elements called "taggants." These elements react to electromagnetic energy sourced from a remote reader. By using these inks and measuring their reflection, it is

possible to identify designated card groupings or types. These taggant-carrying products are known as “smart” (or “intelligent”) inks.

(O1) Kinegrams - Kinegrams, like holograms, can be produced on a reflective or transparent material. However, unlike holograms, Kinegrams have only two-dimensional effects, and effects are observable under a wider variety of lighting conditions. Also, Kinegrams can incorporate asymmetric optical effects that is, different optical variable effects are viewable as the Kinegram is completely rotated (360 degrees).

(O1/3) Laser-Encoded Optical Image - The image and text files used to personalize and issue a document is laser-encoded on to optical WORM media as a visible diffraction pattern image that is eye-readable under a variety of lighting conditions. The personalized laser-encoded optical image is extremely difficult to simulate as it has a two-dimensional appearance and the encoding registration on to the optical WORM media is at a sub-micron level of accuracy. The laser-encoded optical image cannot be removed from the reflective optical WORM media nor can it be duplicated or simulated by photocopying, photography or scanning. The laser-encoded optical image can be updated by incorporating new diffraction pattern images or alphanumeric text as the document is updated or processed. Furthermore, covert physical protection can be added by interleaving a copy of the digital file within the laser-encoded optical image. This personalized security feature is currently used in the Permanent Resident Card ("Green Card”) issued by the U.S. Immigration and Naturalization Service and the Border Crossing Card issued by the U.S. Department of State.

(O1/2) Laser Engraving - Laser engraving has been used in Europe for more than 10 years on high-security plastic cards for printing highly tamper-resistant variable data on a card. Using an intense laser beam, data is burned (or “engraved”) into the inner core of the card. The information cannot be mechanically or chemically removed without damaging the surface of the card, thereby providing an extremely effective tamper-resistant barrier. Laser engraving can be performed with alpha-numeric characters, digitized images (such as photos or signatures), or bar-codes and OCR characters.

(O1/2) Laser Perforation - This is the perforation of a document using laser technology. Unlike mechanical punching techniques, the holes made by the laser beam are free from burrs and can easily be confirmed by feeling. The holes created are also conical shape, with the entrance being larger than the exit.

(C2/3) Machine-Readable Technologies - The card design can incorporate inclusion of many machine-readable technologies such as magnetic stripe, integrated circuit, 1D or 2D bar-codes, OCR, optical WORM media, machine-readable holograms, etc. Verification of the authenticity of the document, the data, and/or the person presenting the document can be accomplished with a card reader, depending on the technology employed. Common techniques to ensure data integrity include:

– Check digits and data encryption (presumably with public key encryption)

– For IC cards, tamper detection and chip disabling; and digital signatures for all data written to the chip.

(O1) Metallic and Pearlescent Inks - Special iridescent inks fluctuate in brilliance depending upon the angle of illumination and viewing. The typical appearance of metallic or pearl luster inks cannot be mimicked by color copiers or reproduced by scanning and reprinting.

(O1/2) Micro Optical Imaging - Text, line art, gray scale images and multi-reflectivity images can be engineered into optical WORM media at a resolution over 12,000dpi. This extremely high resolution is over 4 times higher than current security printing techniques and therefore extremely difficult to simulate. The micro optical images cannot be removed from the reflective optical WORM media nor can it be duplicated or simulated by photocopying, photography or scanning. Micro optical imaging is mainly made up of visible images but can also incorporate digital data that can be used for covert machine-readable security. Micro optical imaging is currently used in the U.S. Permanent Resident Card, Border Crossing Card and several other commercial applications.

(O2) Microprinting - Miniature lettering, which is discernible under magnifying readers, can be incorporated into the fine line background or can be placed to appear as bold lines. Visa, MasterCard, and American Express include

microprint as a standard security feature. Microprint was also added to U. S. currency in 1990. Accurate reproduction of microprint cannot be accomplished as yet by photocopying or by commercially available color photography or color scanners.

(C1/2) Moiré Pattern - A new pattern formed by the superpositioning of two patterns whose periodicities are not identical. Security designs can be made so that a scanner or copier will only display part of the pattern, resulting in a visible effect different from the original document. The original image can be designed so that a copy would reveal indication of reproduction - typically showing the word “VOID” or “COPY”. This process is also referred to as aliasing.

(O1) Opacity Mark - The opacity mark, which is similar to a watermark, is a plastic that contains a unique translucent opacity mark. It is similar in principle and effect to a watermark found in paper documents and enjoys a high level of familiarity as a security feature.

(O1/2) Optical Variable Device - Optically Variable Device (OVD) is a general term describing a security feature which changes appearance in some way when the angle of illumination or observation is changed. OVDs derive their significance for valuable documents and goods from the impossibility of copying them with usual reproduction techniques like color scanners and copiers. OVDs are often distinguished by being identified as either iridescent or non-iridescent.

(O1/2) Optical Watermark - Fine line images can be engineered into optical WORM media at a resolution over 12,000dpi. The optical watermark is then overwritten with a laser-encoded optical image, interlocking in sub-micron register, a preformatted document security feature with a laser encoded personalization security feature. This extremely high resolution is over 4 times higher than current security printing techniques and therefore extremely difficult to simulate. The optical watermark cannot be removed from the reflective optical WORM media nor can it be duplicated or simulated by photocopying, photography or scanning. Attempting to tamper or alter the optical watermark destroys the laser-encoded optical image. The optical watermark is currently used in the U.S. Permanent Resident Card and Border Crossing Card.

(O1) Optically Variable Inks - Optically variable inks (OVI) can be incorporated into designs to create a striking color shift (for example, green to purple, gold to green, etc.) depending on the angle of light used in viewing the card. This material consists of a transparent colorless ink containing microscopic, advanced multi-layer interference structures. OVI is precious, and production is available to secure printers only. Since the availability of these inks is highly restricted, true counterfeiting is unlikely.

(O1) Overlapping Data - Variable data, such as a digitized signature or text, can be “overlapped” with another field, such as a photo image. This technique makes it necessary to alter both fields if either one of them is changed, thereby increasing the tamper resistance of the card by making it more difficult to alter.

(C2/3) Radio Frequency Technology - Use of radio frequency waves to activate and retrieve information from another source.

(O1) Rainbow Printing - Sometimes called “iris printing,” involves a very subtle shift in color across a document. Well-designed patterns cannot be accurately reproduced on color copiers or through the use of document scanners. Widely perceived in Europe and Asia as an element of a secure document design, it is commonly used in conjunction with a fine line or medallion pattern in the background of the document.

(O1) Redundant Data - Data can be displayed in more that one location on the ID, thereby raising the resistance to alteration. A simple visual inspection is required to determine if all data fields match. Redundant data can also be displayed in differing colors or fonts.

(O2) Retroreflective Devices - Optical constructions that reflect light such that covert logos become visible over the entire document, and/or overt logos become more visible and reflective, when the document is viewed using a focused light source.

(O1) Seal/Signature over Photo/Information - A type of unique identification that overlaps the photo and text area. It can be a specific equipment number, state seal, coat of arms, flag, etc. The significance of this is to deter substituting the photo and/or personal information.

(C2) Security Bonding - The card periphery on an optical memory card can incorporate a security bonding material with known characteristics to bond all layers together. Tampering with the card periphery in an attempt to access internal structures damages the known characteristics within the security bonding. This creates a tamper evident feature.

(C2/3) Security Code - It is possible for high-resolution color printing systems to print a security code within the body of the color printed photograph. For example, a security code can be printed in a non-proportional font that can imbed characters on the edge or the bottom of the printed picture. The text can be printed on the image in colors that are complementary to the image or in black.

(O1/2) Security Laminate - Transparent layers or films with an integrated security feature can be applied to a document with an adhesive or fused by heat. Available in a number of forms security laminates are designed to protect a document from alteration and provide tamper evidence.

(O1/2) Security Thread - First seen in U.S. banknotes the thread is visible by viewing in reflected or transmitted light and can have text (positive or reverse) or other features on/in the thread. Security threads can be metal or plastic, transparent or opaque, colored or colorless. With special metallized film, demetallized text is invisible in reflected light and therefore cannot be copied reprographically. When viewed in transmitted light, however, the opaque aluminum letters are clearly visible.

(C2/3) Specialized Inks - Special inks have been formulated with specific elements called “taggants.” These elements can be detected by a remote reader or viewer. By using these inks and measuring their presence, it is possible to identify designated card groupings or types. These taggant-carrying products are known as “smart” (or “intelligent”) inks.

(O2) Thin-Film Interference Filters - Multiple-layer structures that produce color effects by interference.

(O1/2) Transparent Holograms - It is possible to incorporate holographic effects in a clear, transparent topcoat that can be applied over variable printing. Through careful design and physical registration, the clear holographic topcoat can serve as a deterrent to alteration in addition to its counterfeit protection features. If an attempt is made to remove or alter the topcoat, tampering will be detectable without the need of special equipment. Because the transparent hologram design reflects light at differing angles, accurate reproduction with a copier or scanner is cannot be accomplished.

(C2) Ultraviolet (UV) Printing - Ultraviolet ink, which can be applied either through offset or silk screen techniques, has long been accepted as a security feature for plastic cards. This invisible printing can be produced with the availability of a color shift when viewed under long-wave UV light sources. UV radiation is not visible to the human eye, but becomes visible when irradiated with a UV light. Custom UV fluorescing colors can be formulated that are not normally available commercially, thereby increasing resistance to counterfeiting.

(C2) Void Pattern - A security device consisting of a period structure as an overt but not visible feature. When copied on a machine with a different periodicity, the resulting moiré pattern displays the word “VOID” or some other message.