INTERNATIONAL STANDARD

ISO/IEC 18013-2

First edition
2008-05-15

Information technology — Personal identification — ISO-compliant driving licence

Part 2: Machine-readable technologies

Technologies de l'information — Identification des personnes — Permis de conduire conforme à l'ISO

Partie 2: Technologies lisibles par une machine

Reference number
ISO/IEC 18013-2:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18013-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ISO/IEC 18013 consists of the following parts, under the general title *Information technology — Personal identification — ISO-compliant driving licence*:

— *Part 1: Physical characteristics and basic data set.* Part 1 defines the basic terms for ISO/IEC 18013, including physical characteristics, basic data element set, visual layout, and physical security features.

— *Part 2: Machine-readable technologies.* Part 2 defines the technologies that may be used for ISO/IEC 18013, including the logical data structure and data mapping for each technology.

— *Part 3: Access control, authentication and integrity validation.* Part 3 defines the electronic security features that may be incorporated under ISO/IEC 18013, including mechanisms for controlling access to data, verifying the origin of an ISO-compliant driving licence, and confirming data integrity.

Introduction

This part of ISO/IEC 18013 prescribes requirements for the implementation of machine-readable technology on an ISO-compliant driving licence (IDL).

One of the functions of an IDL is to facilitate international interchange. Storing IDL data in machine-readable form supports this function by speeding up data input and eliminating transcription errors. Consequently, the automation and productivity of traffic law enforcement and other traffic safety processes can be improved.

This part of ISO/IEC 18013 allows issuing authorities to customise machine-readable data for domestic use. Apart from international interchange, the use of an IDL as a domestic driving licence thus provides for domestic standardisation and creates a domestic infrastructure capable of processing IDLs issued by other issuing authorities.

Information technology — Personal identification — ISO-compliant driving licence

Part 2: Machine-readable technologies

1 Scope

ISO/IEC 18013 establishes guidelines for the design format and data content of an ISO-compliant driving licence (IDL) with regard to human-readable features (ISO/IEC 18013-1), ISO machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states in applying their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

The purpose of storing IDL data on machine-readable media on the IDL is to

- increase productivity (of data and IDL use),
- facilitate electronic data exchange, and
- assist in authenticity and integrity validation.

This part of ISO/IEC 18013 thus specifies the following:

- mandatory and optional machine-readable data;
- the logical data structure;
- encoding rules for the machine-readable technologies currently supported.

To prevent unauthorised access to the data contained on a contactless IC (e.g. by eavesdropping), provision is made to protect the privacy of the licence holder via basic access protection [requiring a human-readable and/or machine-readable key/password on the IDL to access the data on the PIC (via protected-channel communication)]. The implementation details of this function however are defined in ISO/IEC 18013-3.

Provision is made for issuing authorities to validate the authenticity and integrity of the mandatory and optional data. In addition, the option of protecting access to optional data (beyond basic access protection) is provided for. The exact mechanism used to achieve such protection (e.g. encryption and/or additional access control) is specified in ISO/IEC 18013-3.

2 Conformance

A driving licence is in conformance with this part of ISO/IEC 18013 if it meets all mandatory requirements specified directly or by reference herein. Compliance with ISO/IEC 18013-1 is not required for compliance with this part of ISO/IEC 18013, except for those parts of ISO/IEC 18013-1 directly referenced in this part of ISO/IEC 18013 outside of Clause 3. Conversely, the incorporation of a machine-readable technology which is

not compliant with this part of ISO/IEC 18013 does not necessarily render the IDL non-compliant with ISO/IEC 18013-1.

3 Normative references

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

ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO/IEC 5218:2004, *Information technology — Codes for the representation of human sexes*

ISO/IEC 7812-1:2006, *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 7816-5:2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 8859-1:1998, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 18013-1, *Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set*

ISO/IEC 19785-1:2006, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ANSI D20-2003, *Data Element Dictionary For Traffic Records Systems* (April 2003)

IAFIS-IC-0110(V3), *WSQ Gray-scale Fingerprint Image Compression Specification*, Federal Bureau of Investigation, Criminal Justice Information Services Division (1997)

4 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-1 and the following apply.

4.1
basic access protection
BAP
requiring a human-readable and/or machine-readable key/password on the IDL to access the data on the secure IC via protected-channel communication

4.2
binary coded decimal
BCD
binary coding of a sequence of integers using 4 bits for each integer (where the bit weights are 8421) and encoding two integers per byte, and where a 0 digit is appended to the left of an integer sequence containing an uneven number of digits before encoding

NOTE 1 Only unsigned BCD is used in this part of ISO/IEC 18013.

NOTE 2 For purposes of this part of ISO/IEC 18013, the definition of numeric characters in ISO/IEC 18013-1 in terms of ISO/IEC 8859-1 is deemed to be for identification purposes of the numeric characters only, and does not pertain to the manner in which numeric characters have to be encoded. Encoding rules are explicitly specified in this part of ISO/IEC 18013.

EXAMPLE

Integer	BCD
5	0000 0101
20	0010 0000
387	0000 0011 1000 0111

4.3
Biometric Data Block
BDB
block of data with a defined format that contains one or more biometric samples or biometric templates

4.4
Biometric Information Record
BIR
BioAPI Consortium Patron Format biometric record header

4.5
biometric template
biometric sample (i.e. information obtained from a biometric device, either directly or after further processing) or combination of biometric samples that is suitable for storage as a reference for future comparison

NOTE This definition is an expansion of a definition in ISO/IEC 19785-1.

4.6
card holder
person using an IDL, who is not necessarily the legitimate licence holder

4.7
Common Biometric Exchange File Format
CBEFF
file format that promotes interoperability of biometric-based applications and systems by specifying a standard structure for a BIR and a set of abstract data elements and values that can be used to create the header part of a CBEFF-compliant BIR

NOTE This definition is based on descriptive language in ISO/IEC 19785-1.

4.8
compact encoding
encoding method when the memory capacity available for the IDL application does not exceed 5 kB, typically applicable to 2D barcode symbologies, high-coercivity high-density magnetic stripe and limited memory-capacity ICs (PICs and ICs with contacts)

NOTE 1 Compact encoding generates one constructed data object containing all data groups. Selective reading is not possible and the read device reads all data at the same time, whereafter the data is parsed. Using this method for machine-readable technologies with large memory capacity is not recommended as it can result in prolonged reading time.

NOTE 2 Compact encoding may also be used where the total memory capacity exceeds 5 kB (e.g. ICs with contacts and PICs) but where the capacity available to the IDL application is limited due to capacity being reserved for other applications.

4.9
Data Group
DG
collection of related data elements

4.10
dedicated file
DF

4.11
delimiter
D
character used to separate data elements in a machine-readable data stream

4.11.1
data group delimiter
multiplication sign "×" (character D7 of ISO/IEC 8859-1)

4.11.2
field delimiter
division sign "÷" (character F7 of ISO/IEC 8859-1)

4.11.3
sub-field delimiter
sub-delimiter
semicolon ";" (character 3B of ISO/IEC 8859-1)

4.11.4
end of file delimiter
pilcrow "¶" (character B6 of ISO/IEC 8859-1)

4.12
digital signature
data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string and protects against forgery, e.g. by the recipient of the data string

[ISO/IEC 7816-4]

4.13
elementary file
EF

4.14
integrated circuit
IC

4.15
integrated circuit card
ICC

4.16
logical data structure
LDS

4.17
master file
MF

4.18
proximity integrated circuit
PIC

4.19
proximity integrated circuit card
PICC

4.20
standard encoding
encoding method when the memory capacity available for the IDL application exceeds 5 kB, typically applicable to ICs (PICs and ICs with contacts) and optical memory

5 Machine-readable functionality of IDLs

The sub-paragraphs that follow specify the functions (mandatory and optional) to be supported by any machine-readable data elements used on an IDL. The optional domestic data elements incorporated at the discretion of an issuing authority may support additional functions than those specified below.

5.1 General principles

The use of machine-readable functionality in IDLs is optional. If used, all the data elements identified in ISO/IEC 18013-1 as mandatory for international interchange, except for the signature and portrait of the licence holder, shall be included in the machine-readable data. The machine-readable data elements may also include any other data / information that appears visually on the IDL (such as the identification of the issuing country), as well as additional data elements not reflected visually on the IDL. No machine-readable data / information shall conflict with the human-readable data / information. Machine-readable data elements shall, except for optional domestic data (see clause 8.8), have the exact same meaning as the human-readable data elements on the IDL.

NOTE A conflict between human-readable data elements and machine-readable data elements may cast suspicion upon the licence holder.

Rewriting, updating, and appending functions may be supported to the extent allowed by the technology (or technologies) used. If implemented, such functions shall comply with the principles set out herein. Security options are established to support authenticity and integrity of machine-readable data.

It shall be possible to read mandatory data without restriction (with the exception of basic access protection in the case of a PIC IDL). Optional data may be protected, in which case the protection mechanism (and associated parameters) shall be noted or referenced. The various protection mechanisms are specified in ISO/IEC 18013-3. The optional domestic data may be protected in any manner without restriction.

Changes to machine-readable data elements by the issuing authority are allowed only to data-elements that do not appear in human-readable format on the IDL. Issuing authorities shall uniquely identify each new version (see clause 8.3) of optional machine-readable data (typically after changing the originally recorded optional data). Issuing authorities shall issue a new IDL when changes to machine-readable data elements will lead to inconsistencies with human-readable data elements on the IDL.

5.2 Mandatory functions

Machine-readable data elements included on an IDL shall support/enable the functions described in the sub-paragraphs that follow below.

5.2.1 Privilege to drive at time of licensing

Using the IDL to determine (from machine-readable data elements) the driving privileges (and associated restrictions, conditions and validity period(s)) granted to the licence holder by the issuing authority identified on the IDL. It is recognized that this information does not confirm that the issuing authority presently (i.e. at the time when the machine-readable data on an IDL is read by an entity trying to establish a licence holder's driving privileges) considers the licence holder's driving privileges to be valid.

5.2.2 Reference to driving privilege database

Using the machine-readable data elements (such as the licence number) on the IDL to reference records of driving privileges maintained by the issuing authority.

5.2.3 Age verification

Using the machine-readable data elements on the IDL to assure that the licence holder meets various age thresholds for certain products and services, including driving privileges (in the case where the age threshold to drive a particular category of vehicle domestically in the issuing country is lower than the age permitted internationally).

5.3 Optional functions

5.3.1 Identity verification

Using the machine-readable data elements on the IDL to confirm, by way of a visual comparison of the portrait image, that the card holder is the licence holder.

5.3.2 Biographical data verification

Using the machine-readable data elements on the IDL to confirm, by way of visual inspection of the biographical data printed on the portrait side of the card that such data have not been altered.

5.3.3 Evidence of residence

Ability to use the IDL as evidence that the licence holder resided at a specific location at the time the IDL was issued. It is recognized that this information does not confirm that the issuing authority presently considers the licence holder's residential information to be correct.

5.3.4 Biometric authentication

Ability to use a machine-readable biometric template or templates on the IDL to determine whether the card holder is the licence holder by means of a machine-assisted biometric verification process (i.e. a one-to-one match).

5.3.5 Reciprocity of driving privileges

Ability for a country other than the issuing country to use the machine-readable data elements on the IDL to establish whether a mutual recognition agreement (or agreements) exists with the issuing authority.

5.3.6 Document authentication and validation

Ability to reference items on or qualities about the IDL to verify the document is authentic (i.e. produced by the issuing authority reflected both in the human- and machine-readable data) and that no data has been altered since issuing.

6 Machine-readable technologies supported

Technologies suitable for both compact encoding and standard encoding are supported.

For compact encoding, a typical minimum capacity of 300 usable bytes is required.

Given the minimum data capacity needed to support the mandatory data requirements, the IDL may contain any or a combination of the following machine-readable technologies:

- High coercivity high density Magnetic Stripe – Compact encoding, see Annex B.
- Two-dimensional Barcode – Compact encoding, see Annex B.
- IC with contacts – Standard encoding, see Annex C (failing which, compact encoding only if limited memory capacity is available for the IDL application, see Annex B).
- PIC – Standard encoding, see Annex C (failing which, compact encoding only if limited memory capacity is available for the IDL application, see Annex B).
- Optical memory – Standard encoding, see Annex D.

7 Organization of data

Data is organized into eleven data groups, of which each contains data pertaining to a similar function. One data group is mandatory and the others are optional. One data group is reserved for future use.

NOTE Whether or not each group (or individual data element) can be accessed individually depends on the machine-readable technology used.

7.1 Mandatory data

Mandatory data is comprised of the minimum set of data elements required for international interchange (as defined in ISO/IEC 18013-1), with the exception of the signature and portrait.

7.2 Optional data

Optional data is organized into the following groups – licence holder details (DG 2), issuing authority details (DG 3), portrait image (DG 4), signature / usual mark image (DG 5), facial biometric template (DG 6), fingerprint biometric template (DG 7), iris biometric template (DG 8), and domestic data (DG 11). Provision is also made for another as yet undefined biometric template (DG 9), and an additional group reserved for future use (DG 10).

8 Data structure

Details of the data structure will vary depending upon the storage technology(s) used. Conceptually the structure can be visualized as depicted in Figure 1.

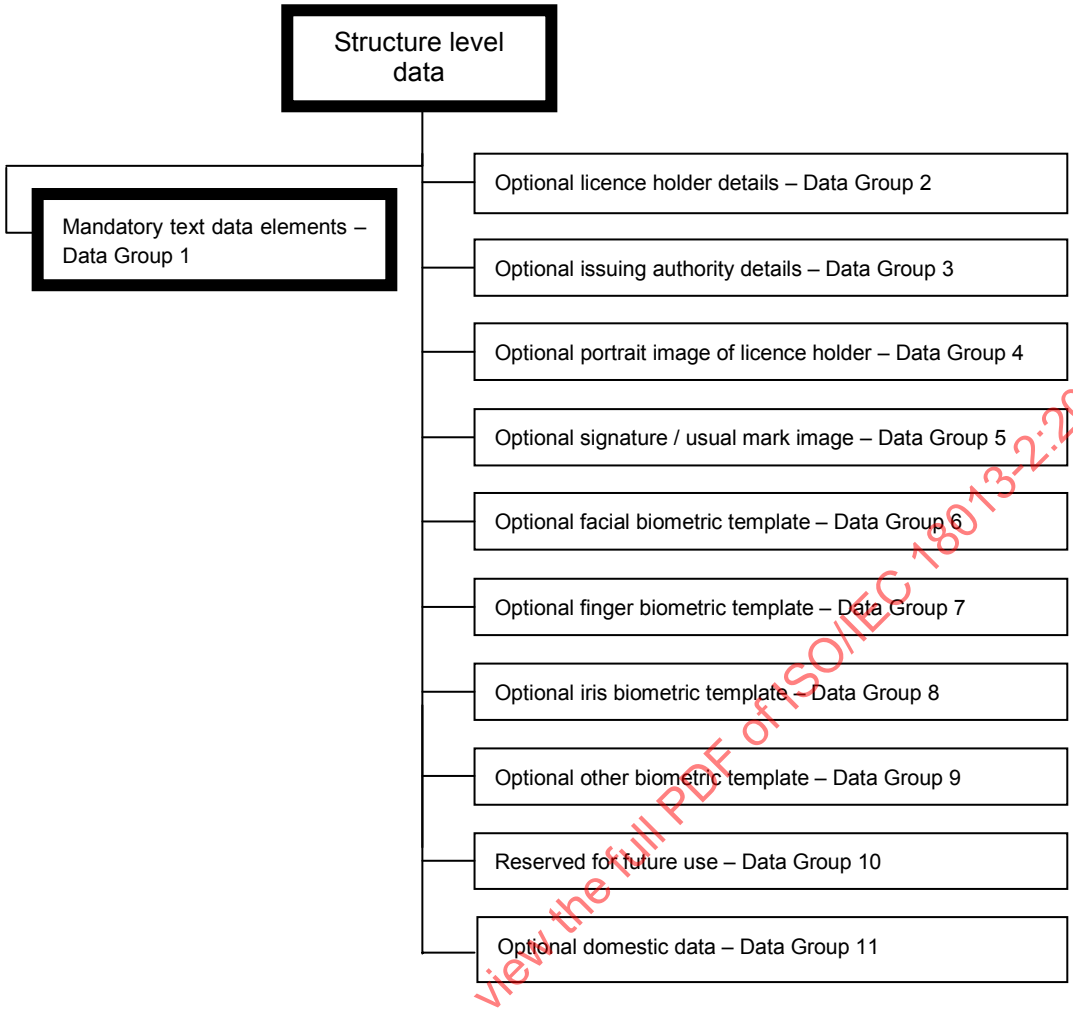

Figure 1 — Conceptual data structure

NOTE This is only a graphical representation. The actual data mapping for each of the machine-readable technologies is specified in the Annexes.

Additional data groups and data elements that are applicable specifically to access control, authentication and integrity validation are specified in ISO/IEC 18013-3.

8.1 Data Group 1: Mandatory text data elements

Data Group 1 consists of nine mandatory elements – demographic data and endorsement/restriction information.

Table 1 — Data Group 1, mandatory text data elements

Name	Fixed or Variable	Field format/ length/type	Example
Family name	V	36AS	Smithe-Williams
Given[a] names	V	36AS	Alexander George Thomas
Date of birth (yyyymmdd)	F	8N	19700301
Date of issue (same format as Date of Birth)	F	8N	20020915
Date of expiry (same format as Date of Birth)	F	8N	20070930
Issuing country (per ISO 3166-1)	F	3A	JPN
Issuing authority	V	65ANS	HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION
Licence number	V	25AN	A290654395164273X
Categories of vehicles/restrictions/ conditions (refer to Annex A for field assembly rules)	V	ADNS (also refer to Annex A)	C1;20000315;20100314;93;<=;8000
NOTE Note the difference between the issuing country code specified in ISO 3166-1, and the issuing country code appearing in Zone 1 of an IDL as specified in Appendix F of ISO/IEC 18013-1.			
[a] No titles and/or suffixes shall be included.			

The assembly of the categories of vehicles/restrictions/conditions field is defined in Annex A. Encoding specifics vary slightly depending upon the technology mapping employed and is defined in Annexes B, C and D in accordance with the machine-readable medium included on the card. The following general format (repeated as necessary) is adhered to:

[category] ; [issue date] ; [expiry date] ; [restriction/condition code] ; [restriction/condition sign] ; [restriction/condition value]

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

8.2 Data Group 2: Optional licence holder details

Data Group 2 consists of seven optional data elements that provide supplemental descriptive information. Any or all data elements may be present for a particular implementation.

Table 2 — Data Group 2, Optional licence holder details

Name	Fixed or Variable	Field format/ length/type	Example
Gender (per ISO/IEC 5218)	F	1N	1 (Male = 1, Female = 2)
Height (cm)	F	3N	172
Weight (kg)	F	3N	082
Eye colour (per ANSI D20-2003)	F	3A	BLU
Hair colour (per ANSI D20-2003)	F	3A	BLD
Place of birth	V	35ADNS[a]	Frozen Foot;Minnesota;USA
Normal place of residence	V	113ADNS[b]	471 Monica Road;201 Delta Building;Lynnwood;Gauteng;0186;South Africa

NOTE ISO/IEC 18013-1 allows non-metric units to be used for the height and weight values that may appear in Zone II of an IDL.

[a] Three fields delimited by the sub-field delimiter - City; State/Province or District; Country. Addresses that cannot be expressed in the defined character set shall be transliterated.

[b] Six fields delimited by the sub-field delimiter - Street address line 1 (e.g. street name and number); Street address line 2 (e.g. apartment number); City; State/Province or District; Postal Code; Country. Addresses that cannot be expressed in the defined character set shall be transliterated.

8.3 Data Group 3: Optional issuing authority details

Data Group 3 consists of four optional data elements that can provide additional details about the IDL or issuing authority. None or all data elements need to be present for a given implementation.

Table 3 — Data Group 3, Optional issuing authority details

Name	Fixed or Variable	Field format/ length/type	Example
Administrative number	V	25ANS	123456789B
Document discriminator [a]	F	2N	01
Data discriminator [b]	F	2N	01
ISO issuer ID number [c] (per ISO/IEC 7812-1)	F	6N	636000

[a] Number assigned by the issuing authority to differentiate between additional licences (documents) or duplicate documents issued bearing the same licence number as the original, that is 01 for the original licence, 02 for the first duplicate, 03 for the second duplicate and nn for the (nn-1)th duplicate.

[b] Number assigned by the issuing authority to differentiate between machine-readable data sets on the same physical document where updates have been made to machine-readable data, that is 01 for the original data set, 02 for the first update, 03 for the second update and nn for the (nn-1)th update. The data discriminator is mandatory when any change is made to the machine-readable data (see 5.1).

[c] ISO number assigned to issuing country or licensing authority, as the case may be.

8.4 Data Group 4: Optional portrait image

Data Group 4 is comprised of one or more portrait images of the licence holder (see Annex E). An image visually similar to the image printed on the portrait side of the IDL shall be included.

Table 4 — Data Group 4, Portrait image

Name	Fixed or Variable	Field format/length/type
Portrait image timestamp [a]	F	14N yyyymmddhhmmss where yyyy=year, mm=month, dd=day, hh=hour, mm=minute, ss=second If hour, minute, and second are not available, 00 shall be used for each value.
Type of image	F	1N 2 = WSQ; 3 = JPEG; 4 = JPEG2000 (as per ISO/IEC 19794-4)
Portrait image	V	JPEG per ISO/IEC 10918-1, JPEG-2000 per ISO/IEC 15444-1, WSQ per IAFIS-IC-0110v3, as specified in Annex E.
NOTE 1 Issuing authorities may include a portrait image in a facial biometric data block in lieu of including such image in DG4 (in standard encoding). Consequently, card-reading applications should test for the presence of a portrait image in DG6. NOTE 2 Image length may be specified by the encoding scheme.		
[a] Used to date the appearance of the licence holder (as reflected on the portrait image). The timestamp reflects the date and time the picture was taken (which is not necessarily the same as the time and date that the physical image data file was created). Mandatory if more than one portrait image is included.		

8.5 Data Group 5: Optional signature / usual mark image

Data Group 5 specifies encoding of the licence holder's signature or usual mark (see Annex E). Since it is an image, signatures or usual marks using non-Latin characters are possible.

Table 5 — Data Group 5, Optional signature / usual mark image

Name	Fixed or Variable	Field format/ length/type
Type of image	F	1N 2 = WSQ; 3 = JPEG; 4 = JPEG2000 (as per ISO/IEC 19794-4)
Image of signature or mark	V	JPEG per ISO/IEC 10918-1, JPEG-2000 per ISO/IEC 15444-1, WSQ per IAFIS-IC-0110v3, as specified in Annex E.
NOTE Image length may be specified by the encoding scheme.		

8.6 Data groups 6, 7, 8 and 9: Optional facial, fingerprint, iris and other biometric templates

Any biometric template is encoded based on the "ISO/IEC JTC 1/SC37 TLV-encoded patron format, for use with smartcards or other tokens" patron format as specified in clause 11 of ISO/IEC 19785-3:2007, specifically the off-card matching implementation specified in clause 11.11.2, as amended in Table 6 below. This format uses the CBEFF structure.

Multiple biometric templates may be stored. If more than one is stored, the most recent biometric must be identified as such by supplying the BDB creation date and time.

NOTE Although the use of the CBEFF format allows individual BDBs to be signed and/or encrypted, it falls outside the scope of this Part of ISO/IEC 18013, and it is therefore recommended to refer to ISO/IEC 18013-3 and use the access control and authentication features defined there as a preference.

Table 6 — Data Group 6 - 9, Optional biometric information

Name	Fixed or Variable	Type of Encoding	Presence	Example
Entry count	V	N	Mandatory when more than one BDB is present	1 for the first entry, 2 for the second entry, the highest numbered entry being the most recent.
	For each entry			
	Name	**Fixed or Variable**	**Field format / length / type / encoding**	**Presence**	**Example**
	Patron header version	F	2 bytes, '01 01'	Mandatory (if absent, the default value applies)	'01 01'
	Biometric type	V	1-3 bytes Refer to ISO/IEC 19785-3:2007, Table 11.5	Optional	Facial = '02' Finger = '08' Iris = '10'
	Biometric subtype	F	1 byte Refer to ISO/IEC 19785-3:2007, Table 11.6	Mandatory when biometric subtype is applicable but not specified in BDB	binary xx100101 for right hand thumb (given a biometric type of '08') binary xx100010 for left eye (given a biometric type of '10')
	Biometric data creation date and time (yyyymmddhhmmss)[a]	F	14N	Mandatory when more than one BDB is present	20031215173530, representing December 15, 2003, 5:35:30 PM. Using BCD representation this is coded using 7 bytes as follows: '20 03 12 15 17 35 30'
	BIR creator	V	ANS	Optional	Hokkaido Prefectural Police Asahikawa Area Public Safety Commission
	BDB validity period (yyyymmddyyyymmdd)[b]	F	16N	Optional	2003121520081214, representing a validity period from December 15, 2003 to December 14, 2008. Using BCD representation this is coded using 8 bytes as follows: '20 31 12 15 20 08 12 14'.
	BDB product owner, product type	F	4 bytes (a concatenation of two 16 bit positive integers of value 1 to 65,535) Refer to ISO/IEC 19785-1:2006, Clauses 6.5.12 and 6.5.13, and Table 11.4 in ISO/IEC 19785-3:2007	Optional	'00 01 00 82'

	For each entry				
	Name	**Fixed or Variable**	**Field format / length / type / encoding**	**Presence**	**Example**
	BDB format owner	F	2 byte non-negative integer of value 1 to 65,535 Refer to ISO/IEC 19785-1:2006, Clause 6.5.1	Mandatory	'01 01' for ISO/IEC JTC1 SC37 - Biometrics
	BDB format type	F	2 byte non-negative integer of value 1 to 65,535 Refer to ISO/IEC 19785-1:2006, Clause 6.5.2	Mandatory	'00 09' for ISO/IEC JTC1 SC37's iris image format
	BIR index (unique identifier used to reference the biometric data set in an application context outside the IDL	V	Free format	Optional	RecId_1952686A67
	Biometric data block	V	Format and encoding as specified by BDB format owner and type.	Mandatory	Finger minutia record as specified in ISO/IEC 19794-2:2005, Clause 7
	BIR payload	V	Refer to ISO/IEC 19785-1:2006, Clause 6.5.22	Optional	Arbitrary domestic data
a	If hour, minute, second are not available, 00 shall be used for each value.				
b	Two concatenated dates where the first date is the "from date" (not after), and the second date is the "to date" (not before).				

8.7 Data Group 10: Reserved for future use

The contents of Data Group 10 have not been defined.

8.8 Data Group 11: Optional domestic data

Since Data Group 11 is dedicated for domestic (or regional) use, the contents shall be defined by the issuing authority (or supranational entity) consistent with the structure, format and principles embodied in the definition of the other data groups.

9 Application identifiers

All applications specified in this Part of ISO/IEC 18013 (including other parts of ISO/IEC 18013) are identified by a seven byte Application Identifier (AID). The AID consists of a five byte Registered Application Identifier (RID) and a two byte Proprietary Application Identifier Extension (PIX).

The RID for the *International Interchange Driving Licence Application* is 'A0 00 00 02 48'.

NOTE 1 The RID was assigned by ISO/IEC JTC1/SC17/WG5 in accordance with ISO/IEC 7816-5.

NOTE 2 Pairs of single apostrophes are used to indicate hexadecimal notation, and are not encoded.

The PIX for each of the applications involved is shown in Table 7.

Table 7 — Proprietary Application Identifier Extensions

Application	PIX
Application 1: Compact encoding (all technologies excluding ICs)	'01 00'
Application 2: Standard encoding for ICs	'02 00'
Application 3: Compact encoding for ICs	'03 00'

NOTE A PIX for optical memory is not defined since optical memory does not use version numbers.

Issuing authorities may add additional applications to the IDL. Issuing authorities may either use the range of proprietary application identifier extensions allocated for this purpose ('05 00' to '05 FF') or obtain separate RIDs from the Registration Management Group of SC17/WG5 according to the procedures defined in ISO/IEC 7816-5 for such applications.

Annex A
(normative)

Assembly rules for categories of vehicles/restrictions/conditions field

A.1 Introduction

This Annex contains the assembly rules for the categories of vehicles/restrictions/conditions field as defined in Table 1. The assembly rules include coding systems for vehicle categories (as defined in ISO/IEC 18013-1) and vehicle and driver restrictions and conditions. The use of codes facilitates language-independent implementation.

A.2 Scope

In addition to specifying the logical record format for the electronic storage of the categories of vehicles/restrictions/conditions field, this Annex also defines the codes necessary for international interchange (machine-readable data corresponds to human-readable data) in respect of the following:

- Any vehicle subcategory defined in accordance with B.4.2 of ISO/IEC 18013-1:2005.
- Supplementation of defined vehicle subcategories in accordance with B.4.3 of ISO/IEC 18013-1:2005.
- Vehicle restriction definitions in B.5 of ISO/IEC 18013-1:2005.
- Driver restriction definitions in B.5 of ISO/IEC 18013-1:2005.

The above-mentioned definitions may be expanded upon for domestic purposes by adding the following optional restrictions in Data Group 11:

- Vehicle restrictions in addition to the mandatory definitions in B.5 of ISO/IEC 18013-1:2005.
- Driver restrictions in addition to the mandatory definitions in B.5 of ISO/IEC 18013-1:2005.

A.3 Normative references

The following International Standards contain provisions, which through reference herein, constitute provisions of this Annex.

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

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

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

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

European Commission Directive 2006/126/EC of 20 December 2006 O.J. EC No L 403/18

UN Convention on Road Traffic, Geneva, 19 September 1949.

UN Convention on Road Traffic, Vienna, 8 November 1968.

A.4 Logical record format

The categories of vehicles/restrictions/conditions field consists of one or more instances of the category of vehicle/restriction/condition data object. The category of vehicle/restriction/condition data object is assembled as illustrated in Figure A.1.

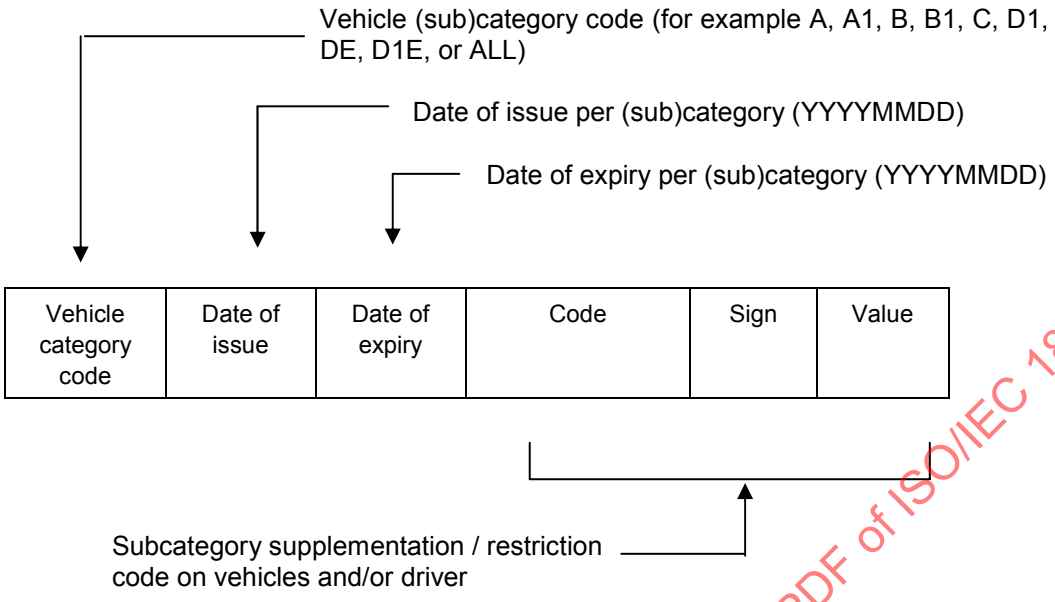

Figure A.1 — Structure of the category of vehicle/restriction/condition data object

Each data block in Figure A.1 is separated by a sub-field delimiter. Each instance of a vehicle category is followed by 5 data fields.

NOTE The number of sub-fields in the categories of vehicles/restrictions/conditions field thus always will be a multiple of 6.

The category of vehicle/restriction/condition data object is repeated as necessary to explain all the categories of vehicles/restrictions/conditions applicable to the licence holder. The manner in which multiple instances of the category of vehicle/restriction/condition data object is encoded is specified in the referring specification (i.e. Annex B, C or D).

For encoding purposes, the formatting of the fields comprising the categories of vehicles/restrictions/conditions field is as follows:

Table A.1 — Field formatting

Field	Fixed or Variable	Field format/length/type (before encoding)
Vehicle category code	V	2AN
Date of issue	F	8N
Date of expiry	F	8N
Code	V	5ANS
Sign	V	2S
Value	V	N

When a category of vehicle/restriction/condition data object is encoded (e.g. in accordance with Annex C), each field making up the data object shall be encoded individually as specified in the referring specification (i.e. Annex B, C or D).

EXAMPLE For compact encoding (as specified in Annex B), the various fields (and the delimiters) will be encoded as follows:

Field	Encoding method
Vehicle category code	As per ISO/IEC 8859-1
Date of issue	BCD
Date of expiry	BCD
Code	As per ISO/IEC 8859-1
Sign	As per ISO/IEC 8859-1
Value	BCD
Delimiters	As per ISO/IEC 8859-1

A.5 Codes

A.5.1 International interchange

The codes defined below in this clause shall be used for international interchange (in DG 1).

Each code is of the format nn where “n” is a numeric.

The codes defined in this Annex are used in the following manner:

- On its own, i.e. the code definition alone fully specifies the supplementation / restriction / condition applicable to the vehicle and/or driver.
- In association with a sign (i.e. “<”, “=”, “>” or a valid combination thereof) and a value. The unit in which the value is expressed is included in either the definition of:
  - Vehicle subcategory (i.e. cm^3, kW, kg or seats) as defined in ISO/IEC 18013-1:2005, Annex B, or
  - Code description.

The grammar used in the code definition makes it clear if the code can be read on its own, or if it has to be interpreted with additional information. The code can apply to either a driver (licence holder) or to a vehicle, as applicable.

The following list defines the description for each code.

Code	Description	Code	Description
01	Licence holder requires eye sight correction and/or protection	S02	The vehicle's authorized passenger seats, excluding the driver's seat, shall be
03	Licence holder requires prosthetic device for the limbs	S03	The vehicle's cylinder capacity (cm^3) shall be
78	Licence holder restricted to vehicles with automatic transmission	S04	The vehicle's power (kW) shall be
S01	The vehicle's maximum authorized mass (kg) shall be	S05	Licence holder restricted to vehicles adapted for physically disabled

EXAMPLE 1

The licence holder may drive category B vehicles, the licence category was issued 2003/MAY/31 and its expiry date is 2013/JUN/15. There are no restrictions.

B	20030531	20130615	Blank	Blank	Blank

EXAMPLE 2

The licence holder may drive category CE vehicles, the licence category was issued 2003/MAY/31 and its expiry date is 2013/JUN/15. Driver requires eyesight correction for this category of vehicle only and is restricted to vehicles with automatic transmission.

CE	20030531	20130615	78	Blank	Blank
CE	Blank	Blank	01	Blank	Blank

EXAMPLE 3

The licence holder may drive category BE vehicles, the licence category was issued 2003/MAY/31 and its expiry date is 2013/JUN/15. Driver requires eyesight correction when driving any category of vehicle and is restricted to vehicles with automatic transmission.

BE	20030531	20130615	78	Blank	Blank
ALL	Blank	Blank	01	Blank	Blank

EXAMPLE 4

The licence holder may drive category A1 and C1 vehicles. The licence categories were issued on 1990/NOV/23 and 2003/MAY/31 respectively. The expiry date is 2013/JUN/15 for both categories. The driver requires eyesight correction for both categories, and the following supplementation details and restrictions are applicable to each of the subcategories:

Category A1: Maximum cylinder capacity of 250 cm^3

Category C1: Maximum authorized mass less than 8 000 kg, and restricted to vehicles with automatic transmission

Since the eyesight correction is applicable to the driver rather than associated with a particular category and to make it clear that the restriction to automatic transmission is only applicable to category C1, the information is rendered as follows:

A1	19901123	20130615	S03	<=	250
C1	20030531	20130615	S01	<	8000
C1	Blank	Blank	78	Blank	Blank
ALL	Blank	Blank	01	Blank	Blank

A.5.2 Domestic use

If an issuing authority wishes to expand on the codes for international interchange to restrict a particular driving privilege, it is recommended that the codes specified in this Clause be used. Such expanded codes are applicable to domestic use only and hence limited to Data Group 11.

NOTE Depending on whether codes are used for law enforcement or driving licence administration, some of the codes in this Clause have the potential to be interpreted as being in conflict with human-readable information. Each issuing authority should determine procedures to clarify the domestic use of these codes.

Each code is of the format nn.xx where “n” and "x" are numerics, and ".xx" is optional for codes without sub-codes or with non-mandatory sub-codes.

The codes defined in this Annex can be used in the following manners:

- On its own, i.e. the code definition alone fully specifies the supplementation / restriction / condition applicable to the vehicle and/or driver.
- In association with a sign “S” (i.e. “<”, “=”, “>” or a valid combination thereof) and a value “V”. The unit in which the value is expressed is included in either the definition of:
  - Vehicle subcategory (i.e. cm^3, kW, kg or seats) as defined in ISO/IEC 18013-1:2005, Annex B, or
  - Code description.

The grammar used in the code definition makes it clear if the code can be read on its own, or if it has to be interpreted with additional information. The code can apply to either a licence holder or to a vehicle, as applicable.

The list that follows identifies the code description for each code identified. Codes in this clause may be used in addition to the codes in clause A.5.1, but shall not be used in lieu of the codes in clause A.5.1.

EXAMPLE If code 72 is used (in Data Group 11), subcategory A1 with the necessary supplementations (S03<=125, S04<=11) shall also be used (in Data Group 1).

Code	Description	Code	Description
01.	Sight correction and/or protection (sub code use obligatory)	10.	Modified transmission
01.01	Glasses	10.01	Manual transmission
01.02	Contact lens(es)	10.02	Automatic transmission
01.03	Protective glass	10.03	Electronically operated transmission
01.04	Opaque lens	10.04	Adjusted gearshift lever
01.05	Eye cover	10.05	Without secondary gearbox
01.06	Glasses or contact lenses	15.	Modified clutch
01.07	Eyesight correction when driving at night	15.01	Adjusted clutch pedal
02.	Hearing aid/communication aid	15.02	Manual clutch
02.01	Hearing aid for one ear	15.03	Automatic clutch
02.02	Hearing aid for two ears	15.04	Partitioning in front of / fold away / detached clutch pedal
03.	Prosthesis/orthosis for the limbs	20.	Modified braking systems
03.01	Upper limb prosthesis/orthosis	20.01	Adjusted brake pedal
03.02	Lower limb prosthesis/orthosis	20.02	Enlarged brake pedal
05.	Limited use (sub code use obligatory, driving subject to restrictions for medical reasons)	20.03	Brake pedal suitable for use by left foot
05.01	Limited to daytime journeys (for example: one hour after sunrise and one hour before sunset)	20.04	Brake pedal by sole
05.02	Limited to journeys within a radius of …km from holder's place of residence or only inside city/region …	20.05	Tilted brake pedal
05.03	Driving without passengers	20.06	Manual (adapted) service brake
05.04	Limited to journeys with a speed (km/h) that shall be	20.07	Maximum use of reinforced service brake
05.05	Driving authorised solely when accompanied by a holder of a driving licence	20.08	Maximum use of emergency brake integrated in the service brake
05.06	Without trailer	20.09	Adjusted parking brake
05.07	No driving on motorways	20.10	Electrically operated parking brake
05.08	No alcohol	20.11	(Adjusted) foot operated parking brake
		20.12	Partitioning in front of / fold away / detached brake pedal
		20.13	Brake operated by knee
		20.14	Electrically operated service brake

25.	Modified accelerator systems
25.01	Adjusted accelerator pedal
25.02	Accelerator pedal by sole
25.03	Tilted accelerator pedal
25.04	Manual accelerator
25.05	Accelerator at knee
25.06	Servo accelerator (electronic, pneumatic, etc.)
25.07	Accelerator pedal on the left of brake pedal
25.08	Accelerator pedal on the left
25.09	Partitioning in front of / fold away / detached accelerator pedal
30.	Modified combined braking and accelerator systems
30.01	Parallel pedals
30.02	Pedals at (or almost at) the same level
30.03	Accelerator and brake with sliding
30.04	Accelerator and brake with sliding and orthesis
30.05	Fold away/detached accelerator and brake pedals
30.06	Raised floor
30.07	Partitioning on the side of the brake pedal
30.08	Partitioning for prosthesis on the side of the brake pedal
30.09	Partitioning in front of the accelerator and brake pedals
30.10	Heel/leg support
30.11	Electrically operated accelerator and brake
35.	Modified control layouts (Lights switches, windscreen wiper/washer, horn, direction indicators, etc.)
35.01	Control devices operable without negative influence on the steering and handling
35.02	Control devices operable without releasing the steering wheel and accessories (knob, fork, etc.)
35.03	Control devices operable without releasing the steering wheel and accessories (knob, fork, etc.) with the left hand
35.04	Control devices operable without releasing the steering wheel and accessories (knob, fork, etc.) with the right hand
35.05	Control devices operable without releasing the steering wheel and accessories (knob, fork, etc.) and the combined accelerator and braking mechanisms
40.	Modified steering
40.01	Standard assisted steering
40.02	Reinforced assisted steering
40.03	Steering with backup system
40.04	Lengthened steering column
40.05	Adjusted steering wheel (Larger and/or thicker steering wheel section, reduced diameter steering wheel, etc.)
40.06	Tilted steering wheel
40.07	Vertical steering wheel
40.08	Horizontal steering wheel
40.09	Foot operated driving
40.10	Alternative adjusted steering (joy-stick, etc.)
40.11	Knob on the steering wheel
40.12	Hand orthesis on the steering wheel
40.13	With orthesis tenodese
42.	Modified rear view mirror(s)
42.01	External (left or) right-side rear-view mirror

42.02 External rear-view mirror set on the wing

42.03 Additional inside rear-view mirror permitting view of traffic

42.04 Panoramic inside rear-view mirror

42.05 Blind spot rear-view mirror

42.06 Electrically operated outside rear-view mirror(s)

43. Modified driver seat

43.01 Driver seat at a good viewing height and in normal distance from the steering wheel and the pedal

43.02 Driver seat adjusted to body shape

43.03 Driver seat with lateral support for good sitting stability

43.04 Driver seat with armrest

43.05 Lengthening of sliding driver's seat

43.06 Seat-belt adjustment

43.07 Harness-type seat-belt

44. Modifications to motorcycles (subcode use obligatory)

44.01 Single operated brake

44.02 (Adjusted) hand operated brake (front wheel)

44.03 (Adjusted) foot operated brake (back wheel)

44.04 (Adjusted) accelerator handle

44.05 (Adjusted) manual transmission and manual clutch

44.06 (Adjusted) rear-view mirror(s)

44.07 (Adjusted) commands (direction indicators, braking light, etc)

44.08 Seat height allowing the driver, in sitting position, to have two feet on the road at the same time

45. Motorcycle with sidecar only

50. Restricted to vehicle with the specific vehicle/chassis number (vehicle identification number, VIN)

51. Restricted to vehicle with the specific vehicle/registration plate (vehicle registration number, VRN)

70. Exchange of licence No …issued by …(Value "V" shall consist of a concatenation of the licence number and the 2-digit country code as specified in ISO 3166-1, separated by a period.)

EXAMPLE The value "V" for licence number 70.A0123456789 issued by the Netherlands shall be 70.A0123456789.NL. The preceding sign field shall be empty.

71. Duplicate of licence No …(Value "V" shall consist of a concatenation of the licence number and the 2-digit country code as specified in ISO 3166-1, separated by a period.)

72. Restricted to category A vehicles having a maximum cylinder capacity of 125 cc and maximum power of 11 KW (A1)[1]

73. Restricted to category B vehicles of the motor tricycle or quadricycle type (B1)

74. Restricted to category C vehicles the maximum authorised mass of which does not exceed 7 500 kg (C1)[2]

75. Restricted to category D vehicles with not more than 16 seats, excluding the driver's seat (D1)[3]

76. Restricted to category C vehicles the maximum authorised mass of which does not exceed 7 500 kg (C1), attached to a trailer the maximum authorised mass of which exceeds 750 kg, provided that the maximum authorised mass of the vehicle train thus formed does not exceed 12 000 kg, and that the maximum authorised mass of the trailer

[1] Note that code 72 is equivalent to subcategory A1 with the supplementations 95<=125, 96<=11.

[2] Note that code 74 is equivalent to subcategory C1 with the supplementation 93<=7500.

[3] Note that code 75 is equivalent to subcategory D1 with the supplementation 94<=16.

does not exceed the unladen mass of the drawing vehicle (C1+E)[4]

77. Restricted to category D vehicles with not more than 16 passenger seats, excluding the driver's seat (D1), attached to a trailer the maximum authorised mass of which exceeds 750 kg provided that (a) the maximum authorised mass of the vehicle train thus formed does not exceed 12 000 kg and the maximum authorised mass of the trailer does not exceed the unladen mass of the drawing vehicle and (b) the trailer is not used to carry passengers (D1+E)[5]

79. Restricted to vehicles which comply with the specifications indicated in brackets (value "V" shall contain a description of the specifications applicable).

90.xx The codes that follow are used in combination with codes defining modifications of the vehicle

90.01: to the left

90.02: to the right

90.03: left

90.04: right

90.05: hand

90.06: foot

90.07: usable

95 Driver holding certificate meeting the obligation of professional aptitude (value "V" shall contain the certificate expiry date and optionally a reference to or description of the enabling legislation/rules)

96 Driver having completed training or having passed a test of skills and behaviour (value "V" shall contain a reference to test specification)

[4] Note that code 76 is equivalent to subcategory C1E with the supplementations 93<=7500, 603<=12000, where 603 is an additionally defined domestic code (see Appendix A to Annex A).

[5] Note that code 77 is equivalent to subcategory D1E with the supplementations 94<=16, 603<=12000, where 603 is an additionally defined domestic code (see Appendix A to Annex A).

Appendix A to Annex A
(normative)

Supplementation / restriction / condition codes for domestic use

A.A.1 Format of code

An issuing authority may add additional domestic codes to the list in clause A.5.2. Such codes shall be of the format nnn where “n” is a numeric and the smallest value of nnn is 100.

A.A.2 Examples

The following informative list contains examples of domestic codes defined by various issuing authorities. Codes duplicating the supplementation / restriction / condition specified in clause A.5.2 have been omitted.

Code	Description	Code	Description
202	The vehicle’s number of gears shall be	506	The vehicle’s total number of cylinders shall be
350	The maximum authorised (pay) load mass (kg) (excluding the unladen vehicle mass) shall be	507	The vehicle’s total number of rotors shall be
401	The vehicle’s authorized length (m) shall be	509	The vehicle’s turbo (super charger) boost pressure (kPa) shall be
402	The vehicle’s authorized width (m) shall be	601	No trailer (including light trailers of which the authorised mass does not exceed 750 kg)
403	The vehicle’s authorized height (m) shall be	602	The trailer’s authorized mass (kg) shall be
406	The vehicle’s authorized total number of wheels shall be	603	The combined (Tractor + Trailer(s)) authorized mass (kg) of the vehicles shall be
407	The vehicle’s authorized wheel base (m) shall be	604	The combined (Tractor + Trailer(s)) vehicle length (m) shall be
408	The vehicle’s authorized vehicle tread length (m) shall be	605	The authorized total number of trailers shall be
409	The vehicle’s authorized total number of axles shall be	606	Tractor mass >= Trailer mass
501	The vehicle’s cylinder capacity (cm3) shall be	607	Tractor mass > Trailer mass
502	Electrical propulsion	608	Full trailer
504	The vehicle’s torque (Nm) shall be	609	Semi-trailer
505	The vehicle’s engine speed (r/min) shall be	610	Camping trailer

701	No passenger
702	The vehicle's authorized power to weight ratio (kW/kg) shall be
703	The vehicle's authorized torque to weight ratio (Nm/kg) shall be
704	With sidecar
705	Without sidecar
706	The seat height (m) shall be
707	The handlebar height (m) shall be
708	Left hand operated brake
709	Right hand operated brake
711	Hand operated front/rear brakes
801	Power steering
806	Hand operated accelerator
808	Modified side mirror
901	Business purposes only
902	Employment purposes only
903	The vehicle's speed (mile/h) shall be
999	There is (are) other restriction(s). Ask the Authority

Annex B
(normative)

Compact encoding

B.1 Scope

This Annex provides the compact encoding scheme when limited memory capacity is available for the IDL application (not exceeding 5 kB). This scheme requires the read device to read all data at the same time, after which the data is then parsed.

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

- 2D bar codes,
- high coercivity high density magnetic stripes, and
- PICs and ICs with contacts with limited capacity available for the IDL application.

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

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

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

B.2 Normative References

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

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

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

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

B.3 Overview

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

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

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

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

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

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

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

B.4 Character set encoding

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

Table B.1 — Encoding rules

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

B.5 Structure

B.5.1 Data file

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

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

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

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

B.5.2 Header

The header consists of the following components:

[AID] [version] [length]

where

AID = Application identifier, 7 bytes. Consists of a 5 byte Registered Application Identifier (RID), and a 2 byte Proprietary Application Identifier Extension (PIX).

NOTE Separate PIXs are used for compact encoding (depending on the media used) and standard encoding – see clause 9 for the values of the RID and the PIX.

Version = 2 byte number. The first byte is assigned by ISO/IEC JTC1/SC17 WG10 for each new version of this part of ISO/IEC 18013. The value of the byte for this version shall be '01'. The second byte is assigned by the issuing authority for each new version of their specification controlling the coding of domestic data (Data Group 11).

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

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

EXAMPLE

Suppose that:

RID	=	A0 00 00 02 48 (number assigned to *International Interchange Driving Licence Application*)
PIX	=	01 00 (Application 1: Compact encoding – all technologies, excluding ICs and optical memory)
WG10 version level	=	1
Domestic version level	=	not specified (defaults to 0)
Total length	=	1598 bytes ('82 06 3E' in ASN.1 hexadecimal representation)

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

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

B.5.3 Type 1 data group

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

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

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

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

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

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

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

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

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

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

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

B.5.4 Type 2 data group

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

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

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

B.6 Implementation

B.6.1 Data Group 1: Mandatory data

Data Group 1 is a Type 1 data group.

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

EXAMPLE 1

Assume the following:

Family name	=	Smithe-Williams
Given name	=	Alexander George Thomas
Date of birth	=	1 March 1970
Date of issue	=	15 September 2002
Date of expiry	=	30 September 2007
Issuing country	=	Japan
Issuing authority	=	HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION
Licence number	=	A290654395164273X

Categories of vehicles, restrictions:

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

The above data group will be coded as follows:

[header]×Smithe-Williams÷Alexander George Thomas÷'19 70 03 01'÷'20 02 09 15'÷'20 07 09 30'÷JPN÷HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION÷A290654395164273X÷B;19910901;20350301;;;×[next data group]

Where

Smi…ams	=	Family name
Ale…mas	=	Given names
'19 70 03 01'	=	BCD encoding of birthday, 1 March 1970
'20 02 09 15'	=	BCD encoding of IDL issue date, 15 September 2002
'20 07 09 30'	=	BCD encoding of IDL expiry date, 30 September 2007
JPN	=	Issuing country
HOK…SION	=	Issuing authority
A29….73X	=	Licence number
B	=	Category B vehicles
'19 91 09 01'	=	BCD encoding of issue date of category B, 1 September 1991
'20 35 03 01'	=	BCD encoding of expiry date of category B, 1 March 2035

EXAMPLE 2

Assume the same data as Example 1 with the following vehicle subcategories and restrictions:

Subcategory A1, with maximum cylinder capacity of 250 cm^3, issued 15 September 2002, expires 30 September 2017.

Subcategory C1 with a maximum authorised mass less than 8000 kg, restricted to vehicles with automatic transmission.

Eyesight correction required for both vehicle subcategories.

The above data group will be coded as follows:

[header] × Smithe-Williams ÷ Alexander George Thomas ÷ '19 70 03 01' ÷ '20 02 09 15' ÷ '20 07 09 30' ÷ JPN ÷ HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION ÷ A290654395164273X ÷ A1;'20 02 09 15';'20 17 09 30';S03;<=;'32 35 30';C1;;;S01;<=;'38 30 30 30';C1;;;78;;;ALL;;;01;; × [next data group]

Where

A1	=	Category A1 vehicles
'20 02 09 15'	=	Issue date for category A1
'20 17 09 30'	=	Expiry date for category A1
S03	=	Code for "The vehicle's cylinder capacity (cm^3) shall be"
<=	=	Less than or equal to
'32 35 30'	=	250 cm^3
C1	=	Category C1 vehicles. Note that the validity period for the category C1 licence is the same as for the IDL.
S01	=	Code for "The vehicle's maximum authorized mass (kg) shall be".
<=	=	Less than or equal to
'38 30 30 30'	=	8000 kg
C1	=	Continuation of category C1 vehicles
78	=	Code for "Restricted to vehicles with automatic transmission"
ALL	=	Start of restriction that applies to all categories
01	=	Code for "Sight correction and/or protection"

B.6.2 Data Group 2: Optional licence holder information

Data Group 2 is a Type 1 data group.

EXAMPLE

Assume the following:

Gender = Male

Height = 172 cm

Weight = 82 kg

Eye colour = Blue

Hair colour = Bald

Normal place of residence = 471 Monica Road, 201 Delta Building, Lynnwood, Gauteng, 0186, South Africa

The above data group will be coded as follows:

[previous data group] × 1 ÷ '01 72' ÷ '00 82' ÷ BLU ÷ BLD ÷ ÷ 471 Monica Road;201 Delta Building;Lynnwood;Gauteng;0186;South Africa × [next data group]

Where

1 = male (per ISO/IEC 5218)

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

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

BLU = Blue eyes (per ANSI D20)

BLD = Bald (per ANSI D20)

471 Mo…rica = Residence information

NOTE No place of birth included.

B.6.3 Data Group 3: Optional issuing authority details

Data Group 3 is a Type 1 data group.

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

EXAMPLE

Assume the following:

Administrative number = 123456789B

Document discriminator = 01

ISO issuer ID number = 636000

The above data group will be coded as follows:

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

Where

123456789B = Administrative number

'01' = Document discriminator

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

NOTE No data discriminator included.

B.6.4 Data Group 4: Optional Portrait images

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

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

Where

[type of image] is a fixed length field

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

[image] is a variable length field

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

EXAMPLE

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

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

Where

'03' = image type 3 (JPEG)

'82 08 1B' = ASN.1 encoding of the image length of 2075 bytes

..image... = Image field including definition details and binary data

B.6.5 Data Group 5: Optional signature / mark image

Data Group 5 is not supported in compact encoding.

B.6.6 Data Group 6: Optional facial biometric template

Data Group 6 is not supported in compact encoding.

B.6.7 Data Group 7: Optional finger template

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

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

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

Where

[BDB format owner] is a fixed length field

[BDB format type] is a fixed length field

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

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

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

Table B.2 — BDB format owner and type combinations

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

EXAMPLE

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

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

Where

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

B.6.8 Data Group 8: Optional iris biometric template

Data Group 8 is not supported in compact encoding.

B.6.9 Data Group 9: Optional other biometric template

Data Group 9 is not supported in compact encoding.

B.6.10 Data Group 10: Reserved for future use

Data Group 10 is not currently supported in compact encoding.

B.6.11 Data Group 11: Optional Domestic Use

This data group is reserved for domestic use and hence the encoding is defined domestically.

B.6.12 Overall example

John Bull (a male) was born on the 29th of February 1976 in Campbeltown, Scotland. On 29 February 2000, the Driver and Vehicle Licensing Agency of the UK Department for Transport issued John an IDL (number BTCB20996) that expires after 4 years. The IDL authorises John to drive motorcycles (since 15 March 1992) and passenger cars (since 8 May 1996), provided that he wears his glasses.

The issuing authority has also assigned an administrative number (102T776) to the IDL.

One portrait image (1003 bytes) using JPEG2000 compression is included. The minutiae of his right index finger are stored as well (613 byte data block; compact size, with ridge skeleton end and ridge skeleton bifurcation points).

The above information will logically be written as set out below (square brackets and spaces are used where appropriate to improve readability; single quotes signify hexadecimal numbers):

> ['A0 00 00 02 48 01 00'] ['01 00'] [1794] × [Bull] ÷ [John] ÷ [19760229] ÷ [20000229] ÷ [20040228] ÷ [GBR] ÷ [Driver and Vehicle Licensing Agency] ÷ [BTCB20996] ÷ [A;19920315;;;;;B;19960508;;;;;ALL;;01;;;] × [1] ÷ ÷ ÷ ÷ ÷ [Campbeltown;Scotland;United Kingdom] ÷ × [102T776] ÷ ÷ ÷ × [4] [1003] [portrait image] × × × ['01 01'] ['00 06'] [613] [biometric data] ¶

The above fields will be encoded as follows (all numbers are hexadecimal):

> [A0 00 00 02 48 01 00] [01 00] [82 07 02] × [42 75 6C 6C] ÷ [4A 6F 68 6E] ÷ [19 76 02 29] ÷ [20 00 02 29] ÷ [20 04 02 28] ÷ [47 42 52] ÷ [44 72 69 76 65 72 20 61 6E 64 20 56 65 68 69 63 6C 65 20 4C 69 63 65 6E 73 69 6E 67 20 41 67 65 6E 63 79] ÷ [42 54 43 42 32 30 39 39 36] ÷ [41 3B 19 92 03 15 3B 3B 3B 3B 3B 42 3B 19 96 05 08 3B 3B 3B 3B 3B 41 4C 4C 3B 3B 30 31 3B 3B] × [01] ÷ ÷ ÷ ÷ ÷ [43 61 6D 70 62 65 6C 74 6F 77 6E 3B 53 63 6F 74 6C 61 6E 64 3B 55 6E 69 74 65 64 20 4B 69 6E 67 64 6F 6D] × [31 30 32 54 37 37 36] ÷ ÷ ÷ × [04] [82 03 EB] [portrait image] × × × [01 01] [00 06] [82 02 65] [biometric data] ¶

The final byte stream will be as follows:

> A0 00 00 02 48 01 00 01 00 82 07 02 D7 42 75 6C 6C F7 4A 6F 68 6E F7 19 76 02 29 F7 20 00 02 29 F7 20 04 02 28 F7 47 42 52 F7 44 72 69 76 65 72 20 61 6E 64 20 56 65 68 69 63 6C 65 20 4C 69 63 65 6E 73 69 6E 67 20 41 67 65 6E 63 79 F7 42 54 43 42 32 30 39 39 36 F7 41 3B 19 92 03 15 3B 3B 3B 3B 3B 42 3B 19 96 05 08 3B 3B 3B 3B 3B 41 4C 4C 3B 3B 30 31 3B 3B D7 01 F7 F7 F7 F7 F7 43 61 6D 70 62 65 6C 74 6F 77 6E 3B 53 63 6F 74 6C 61 6E 64 3B 55 6E 69 74 65 64 20 4B 69 6E 67 64 6F 6D D7 31 30 32 54 37 37 36 F7 F7 F7 D7 04 82 03 EB [portrait image byte stream] D7 D7 D7 01 01 00 06 82 02 65 [biometric data byte stream] B6

B.7 File structure for ICCs with contacts and for PICCs

Information on an ICC with contacts and on a PICC is stored in a file system defined by ISO/IEC 7816-4. The card file system is organized hierarchically into DFs and EFs. DFs contain other DFs and/or EFs. A MF, if present, is the root of the file system. Additional DF and EF structures other than the IDL application DF may be included to meet the requirements of ISO/IEC 24727 [6]. These do not affect the basic IDL application DF structures. The detail required to manage access conditions and interoperability is specified in ISO/IEC 18013-3.

The IDL application is defined as one DF. The DF for compact encoding is identified as follow:

'A0 00 00 02 48 03 00'

The DF is selected using its AID. If other applications exist on the card, they would be contained within their own DF and would be accessed via their separate AID.

The DF comprises one EF only.

The compact encoded data string is stored in the one EF, named EF.CE, with short EF identifier = '0D', EFID = '000D' and Tag = '53'. The tag is followed by the compact encoded data string.

NOTE Implementers may see Appendix B to Annex C for a full list of data objects and tags.

For compact encoding, EF.COM will not be present. Refer for Figure B.1 for a graphical depiction of the file structure.

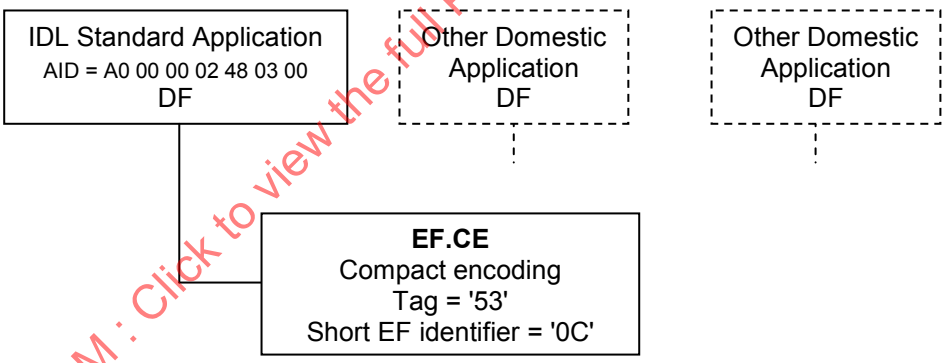

Figure B.1 — Logical data structure

NOTE 1 Although the header and the data group delimiter between the header and DG1 (in the compact encoding constructed data object) are strictly speaking not necessary, it is nevertheless retained for consistency purposes.

NOTE 2 In order to improve clarity, in the example that follows tags are printed in *RED ITALICS* and values are printed in BLACK.

EXAMPLE

Assume a compact encoding constructed data object that commences with 'A0 00 00 02 48 01 00 03 00 82 07 0A' (the header) and concludes with 'B6' (the end of file delimiter). Encoding would be (spaces, italics and colours are included for legibility only, and are not encoded):

'*53*' 'A0 00 00 02 48 03 00 01 00 82 07 0A … B6'

[6] ISO/IEC 24727 provides an alternate mechanism for identifying applications and application capability as well as card capability via discoverable card and application capability containers which may optionally be included on the IDL.

Where,

'*53*'	=	Tag the CE Data Group
'A0 00 … B6'	=	Compact encoding constructed data object.

The requirements of the following clauses in Annex C also apply to B.7:

- C.1.1
- C.1.2
- C.1.3
- C.2 (to the extent that the references are applicable to either an ICC with contacts or a PICC)
- C.3, with the exception of C.3.8
- C.5

Annex C
(normative)

Standard encoding for ICCs with contacts and for PICCs

C.1 Introduction

Standard encoding is designed for random access and is suitable for use on documents employing ICCs with contacts and PICCs based on ISO/IEC 7816 and ISO/IEC 14443 respectively.

C.1.1 Design considerations

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

- A wide variety of implementations must be supported to satisfy specific needs of different issuing authorities. More specifically the data structure must efficiently support:
    - Mandatory and optional sets of data elements.
    - Multiple occurrences of specific data elements that may exist within a data group.
    - A range of possible access conditions in respect of optional data elements as required by different issuing authorities (due to significant variance in business requirements driven by privacy and other statutory requirements).
    - The unconditional availability of mandatory data.
    - An optional mechanism to verify one or more digital signatures.
    - Discovery of the interoperability and security requirements in respect of the optional data elements from the card.
- The structure supports at least two (2) application data sets:
    - The IDL application, which has the following properties:
        - Contains data elements with the following properties:
            - Includes information that would enable a reading authority to identify the access control, authentication and integrity validation mechanisms present on the card.
            - Write protected.
            - Modifiable by the issuing authority (or trusted agent of the issuing authority), subject to the requirements in 5.1 (for example the machine-readable data may not differ from the human-readable data).
        - Optionally protected with one or more digital signatures (defined in ISO/IEC 18013-3).
    - DDL application(s) – outside the scope of this standard.

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

C.1.2 Interoperability considerations

To provide global interoperability this Annex defines:

- Physical characteristics
- Location and dimensions of the contacts or coupling areas
- Electrical signals to support communication between the IC and the interface device
- Transmission protocols
- Application selection and discovery of optional data elements and security requirements
- Encoding rules
- The file structure and tag assignments for the IDL Logical Data Structure
- Command set
- Data element mappings to the files

NOTE Although it is important for interoperability, this Part does not define the human-readable properties of the IDL, which are defined in ISO/IEC 18013-1.

C.1.3 Security requirements

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

C.2 Normative References

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

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

ISO/IEC 7501-1:—[7]: *Identification cards — Machine readable travel documents — Part 1: Machine readable passport*

ISO/IEC 7816-1:1998, *Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics*

ISO/IEC 7816-1:1998/Amd.1:2003, *Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics — Amendment 1: Maximum height of the IC contact surface*

7) To be published. Revision of ISO/IEC 7501-1:2005.

ISO/IEC 7816-2:2007, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*

ISO/IEC 7816-3:2006, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-6:2004, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-6:2004/Cor.1:2006, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange — Technical Corrigendum 1*

ISO/IEC 14443-1:—[8], *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 1: Physical characteristics*

ISO/IEC 14443-2:2001, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-2:2001/Amd.1:2005, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface — Amendment 1: Bit rates of fc/64, fc/32 and fc/16*

ISO/IEC 14443-3:2001, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision*

ISO/IEC 14443-3:2001/Amd.1:2005, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision — Amendment 1: Bit rates of fc/64, fc/32 and fc/16*

ISO/IEC 14443-3:2001/Amd.1:2005/Cor.1:2006, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision — Amendment 1: Bit rates of fc/64, fc/32 and fc/16 — Technical Corrigendum 1*

ISO/IEC 14443-3:2001/Amd.3:2006, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision — Amendment 3: Handling of reserved fields and values*

ISO/IEC 14443-4:2001, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*

ISO/IEC 14443-4:2001/Amd.1:2006, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol — Amendment 1: Handling of reserved fields and values*

C.3 Compatibility with existing standards

C.3.1 Approach

This standard is based on supporting infrastructure provided by a number of other key ISO Standards:

- Existing manufacturing standards ISO/IEC 7816 and ISO/IEC 14443 (for ICC and PICC devices respectively) that ensure support for a broad range of cards and devices by multiple manufacturers.
- ISO/IEC 24727, which may optionally be used.

8) To be published. Revision of ISO/IEC 14443-1:2000.

- Biometric standards under development by ISO JTC1/SC37.
- Other identification document standards such as those under development and ISO JTC1/SC17/WG3 and by ICAO.

C.3.2 Physical characteristics

The physical characteristics of the card shall adhere to ISO/IEC 7816-1 for ICCs with contacts and ISO/IEC 14443-1 for PICCs.

C.3.3 Location and dimensions of contacts or coupling area

Contact size and location for ICCs with contacts shall adhere to ISO/IE 7816-2. Location and size of contactless coupling area for PICCs shall adhere to ISO/IEC 14443-1.

C.3.4 Electronic signals

Electronic signals for ICCs with contacts shall adhere to ISO/IEC 7816-3. Magnetic fields and radio frequency power for PICCs shall adhere to ISO/IEC 14443-2.

C.3.5 Transmission protocols

C.3.5.1 ICCs with contacts

The IDL shall as a minimum support T = 0 or T = 1 as specified by ISO/IEC 7816-3.

NOTE Application design and hardware used to support high-speed transmission is recommended.

C.3.5.2 PICCs

The IDL shall be compatible with ISO/IEC 14443-1 to ISO/IEC 14443-4 and support half-duplex transmission protocol specified by ISO/IEC 14443-4.

C.3.6 Application selection

The IDL supports the following applications:

- One application shall consist of data recoded by the issuing authority in accordance with ISO/IEC 18013.
- One or more applications may be added for other domestic or regional applications, such as applications provided for in ISO/IEC 24727. Such applications shall be loaded under the control of the issuing authority.

The applications shall be selected by use of the seven byte Application Identifier (AID) as a reserved DF name. The AID shall consist of the Registered Application Identifier (RID), 'A0 00 00 02 48' which has been assigned by ISO/IEC JTC1/SC17/WG5 in accordance with ISO/IEC 7816-5, and two additional bytes comprising a Proprietary Application Identifier Extension (PIX) (see clause 9).

C.3.7 Security

The security mechanisms specified in ISO/IEC 18013-3 support the objectives described in clause 5.

All data groups shall be write protected. Only the issuing authority (or the issuing authority's trusted agent) shall have write access (subject to the requirements in clause 5.1). It is left to the issuing authority to define the write protection.

Issuing authorities may optionally either:

- Allow free read access to all data groups, or
- Set specific access control rules under ISO/IEC 18013-3 to any or all optional data groups. The mechanism for setting and discovering the appropriate access controls is specified in ISO/IEC 18013-3.

C.3.8 Character set encoding

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

Table C.1 — Encoding rules

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

C.4 File structure

Information on an ICC with contacts and on a PICC is stored in a file system defined by ISO/IEC 7816-4. The card file system is organized hierarchically into DF and EFs. DFs contain other DFs and/or EFs. A MF, if present, is the root of the file system. Additional DF and EF structures other than the IDL application DF may be included to meet the requirements of ISO/IEC 24727[9]. These do not affect the basic IDL application DF structures. The detail required to manage access conditions and interoperability is specified in ISO/IEC 18013-3.

The IDL application is defined as one DF. The DF for standard encoding is identified as follow:

'A0 00 00 02 48 02 00'

The DF is selected using its AID. If other applications exist on the card, they would be contained within their own DF and would be accessed via their separate AID.

Each DF consists of a number of EFs. The DF for standard encoding consists of one EF containing common data, and one EF for each of the data groups defined in this Annex.

[9] ISO/IEC 24727 provides an alternate mechanism for identifying applications and application capability as well as card capability via discoverable card and application capability containers which may optionally be included on the IDL.

All EFs are in the form of data templates as defined in clause C.6 and have individual ASN.1 tags to support direct retrieval (see Appendix A to Annex C). The structure and coding of data objects are defined in ISO/IEC 7816-4 and ISO/IEC 7816-6. The assigned tags conform to a co-existent tag structure as defined by ISO/IEC 7816-4. Whenever possible inter-industry tags are used. Refer to Appendix B to Annex C for a list of data objects and tags.

The EF that contains the common information for the IDL application is named EF.COM. The short EF identifier for this file is '1E'. This file contains the LDS version number and a list of the data groups (tag list) that are present for any given implementation. In addition, this file may contain information related to data access control, authentication and integrity validation.

For standard encoding, each data group shall be stored in one EF with a short EF identifier as shown in Table C.2. The names for the files shall be EF.DG*n*, where *n* is the data group number, e.g., EF.DG1, EF.DG4. Refer for Figure C.1 for a graphical depiction of the file structure.

Table C.2 — Assignment of file identifiers and Data Group tags

Elementary file	Name	Short EF Identifier	EFID	Tag
EF.COM	Common data	'1E'	'001E'	‘60’
EF.DG1	Mandatory data	'01'	'0001'	‘61’
EF.DG2	Optional licence holder details	'02'	'0002'	‘6B’
EF.DG3	Optional issuing authority details	'03'	'0003'	‘6C’
EF.DG4	Optional portrait image	'04'	'0004'	‘65’
EF.DG5	Optional signature/usual mark image	'05'	'0005'	‘67’
EF.DG6	Optional facial biometric template	'06'	'0006'	‘75’
EF.DG7	Optional finger biometric template	'07'	'0007'	‘63’
EF.DG8	Optional iris biometric template	'08'	'0008'	‘76’
EF.DG9	Optional other biometric template	'09'	'0009'	‘70’
EF.DG10	Reserved for future use	'0A'	'000A'	
EF.DG11	Optional domestic application data	'0B'	'000B'	[a]
NOTE Selected tag assignments are aligned with ISO/IEC 7501-1 (ICAO Doc 9303-1).				
[a] The tag for EF.DG11 is to be assigned by the issuing authority in line with (and not in conflict with) ISO/IEC 7501-1 (ICAO Doc 9303-1). In case ISO/IEC 7501-1 does not provide any guidance, the tag for EF.DG11 is to be assigned by the issuing authority according to ISO/IEC 7816 Parts 4 and 6. Tags already defined and assigned to other data groups in either this International Standard or in ISO/IEC 18013-3 shall not be re-used.				

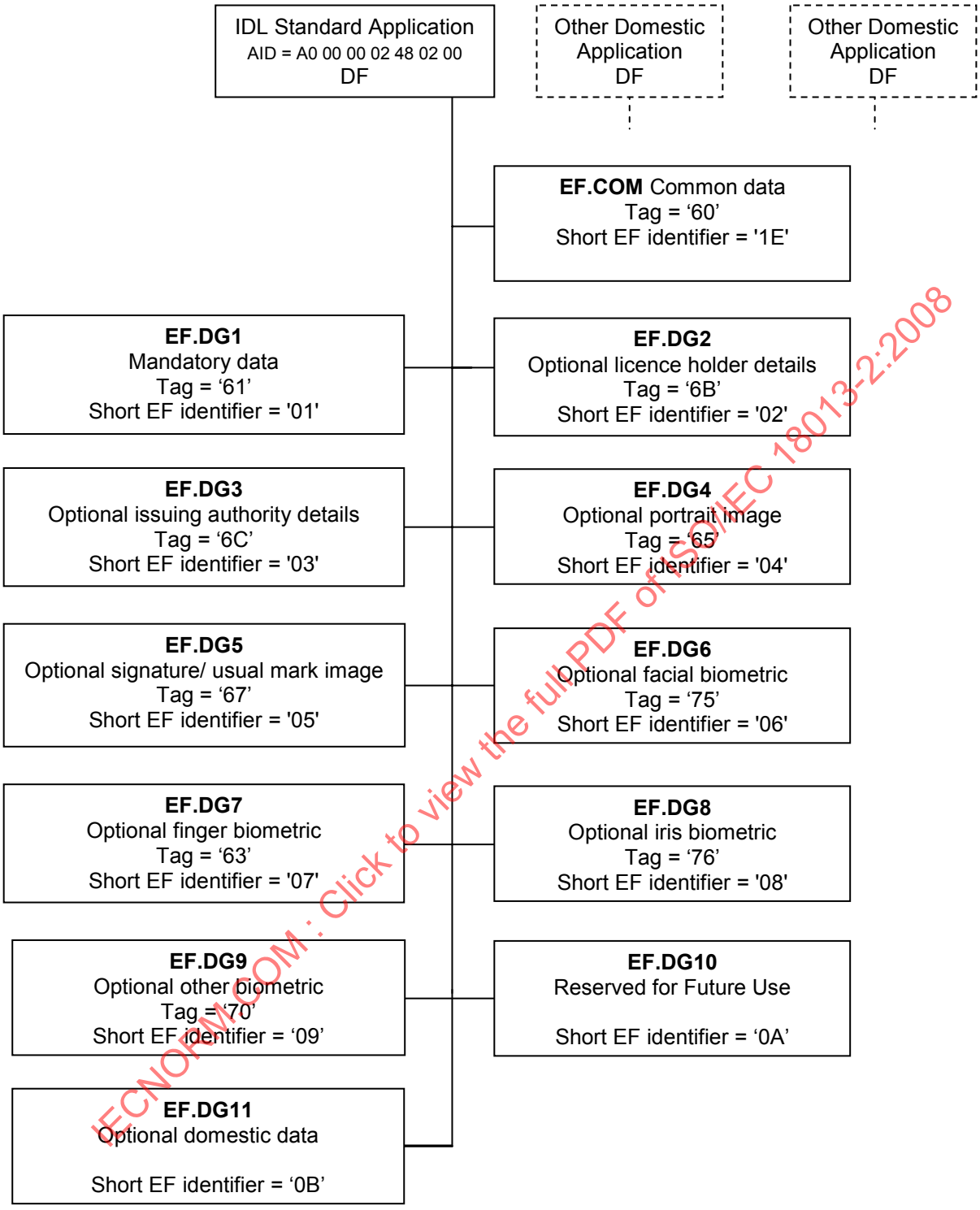

Figure C.1 – Logical data structure

C.5 Command set

The minimum command functions are described in Appendix C to Annex C, with the exception of the security related command set which is described in ISO/IEC 18013-3.

C.6 Data groups

C.6.1 EF.COM – Common data elements, Tag = '60', short EF identifier = '1E'

This template has two data elements, the LDS version level ('5F01') and a tag list ('5C'). The tag list, as the name implies, is a list of the tags of the data groups present for any given implementation, and also specifies the access protection applicable.

Table C.3 — EF.COM

<table>
<tr><th>Tag</th><th>Length</th><th colspan="3">Value</th></tr>
<tr><td rowspan="3">'60'</td><td rowspan="3">X</td><td colspan="3">EF.COM contents</td></tr>
<tr><td>Tag</td><td>Length</td><td>Value</td></tr>
<tr><td>'5F01'</td><td>X</td><td>Version number with format aabb, where aa defines the major revision level and bb defines the release level. aa and bb are numeric and encoded as 2 bytes in BCD. The major revision level is assigned by ISO/IEC JTC1/SC17 WG10 for each new version of this Part of ISO/IEC 18013, and shall be 01 in this version. The release level is assigned by the issuing authority for each new version of their specification controlling coding of domestic data.</td></tr>
<tr><td>'5C'</td><td>X</td><td>DG tag list as per Table C.2</td></tr>
</table>

The template structure has been defined to support future developments. Supporting specifications may require the inclusion of additional tags within EF.COM. Additional tags relating to security are defined in ISO/IEC 18013-3.

NOTE In order to improve clarity, in the examples that follow tags are printed in *RED ITALICS*; lengths are printed in UNDERLINED BLUE and values are printed in BLACK.

EXAMPLE Assume an implementation using LDS Version 1.0 having the following data content – mandatory data, optional licence holder data, optional issuing authority information, a portrait image, and an optional signature/mark image. Encoding would be (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*60*' '0C'
'*5F01*' '02' 0100
'*5C*' '05' '61' '6B' '6C' '65' '67'

C.6.2 EF.DG1 Data Group 1 Mandatory data, Tag = '61', short EF identifier = '01'

This EF contains the mandatory demographic data elements and vehicle categories/restrictions/conditions. Since all data elements are mandatory and the sequence is known, the first 8 data fields are concatenated into one primitive data object. This primitive data object has Tag = '5F1F'. Vehicle categories/restrictions/conditions are encoded as a constructed data object with Tag = '7F63'.

Table C.4

Tag	Length	Value
'5F1F'	X	Primitive data object of mandatory demographic data elements. Refer to Table C.5.
'7F63'	X	Constructed data object of vehicle categories/ restrictions/conditions. Refer to Table C.6.

C.6.2.1 Mandatory demographic data Tag = '5F1F'

Table C.5 specifies the fields that comprise the primitive data object. Each variable length field is preceded by its length (specified using ASN.1 notation). The object thus has the following structure:

[family name field length] [family name] [given names field length] [given names] [date of birth] [date of issue] [date of expiry] [issuing country] [issuing authority field length] [issuing authority] [licence number field length] [licence number]

NOTE No delimiters are used between the fields.

Table C.5

Name	Fixed / variable	Format	Example
Family name	V	36AS	Smithe-Williams
Given[a] names	V	36AS	Alexander George Thomas
Date of birth (yyyymmdd)	F	8N	19700301
Date of issue (same format as date of birth)	F	8N	20020915
Date of expiry (same format as date of birth)	F	8N	20070930
Issuing country (per ISO 3166-1)	F	3A	JPN
Issuing authority	V	65ANS	HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION
Licence number	V	25AN	A290654395164273X
NOTE Note the difference between the Issuing Country code specified in ISO 3166-1, and the Issuing Country code appearing in Zone 1 of an IDL as specified in Appendix F of ISO/IEC 18013-1.			
a No titles and/or suffixes shall be included.			

C.6.2.2 Categories of vehicles/restrictions/conditions – Tag = '7F63'

The following general format is adhered to:

'Tag' 'Overall Length'

'Number of Entries'

'Tag' 'Length' 'Category of vehicle/restriction/condition data object$_1$'

'Tag' 'Length' 'Category of vehicle/restriction/condition data object$_2$'

'Tag' 'Length' 'Category of vehicle/restriction/condition data object$_n$'

Each category of vehicle/restriction/condition data object entry is a variable length data element of ADNS format and constructed as specified in Annex A. All delimiters are included regardless of whether or not the associated optional fields are present. The number of entries is denoted immediately after the total length of Tag '7F63.' Each entry is labelled with a Tag '87'. The length of the entry immediately follows its tag.

Table C.6

Tag	Length	Value
'02'	'01'	Integer (N) – Number of entries
'87'	X	Category of vehicle/restriction/condition data object, repeated for each category/ restriction/ condition listed

EXAMPLE 1

The licence holder may drive category A1 and C1 vehicles. The licence categories were issued on 1990/NOV/23 and 2003/MAY/31 respectively. The expiry date is 2013/JUN/15 for both categories. The driver requires eyesight correction for both categories, and the following supplementation details and restrictions are applicable to each of the subcategories:

Category A1: Maximum cylinder capacity of 250 cm^3

Category C1: Maximum authorized mass less than 8 000 kg, and restricted to vehicles with automatic transmission

This will be coded as follows (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*7F63*' '47'
'*02*' '01' '04'
'*87*' '16' A1;'19 90 11 23';'20 13 06 15';S03;<=;'32 35 30'
'*87*' '17' C1;'20 03 05 31';'20 13 06 15';S01;<=;'38 30 30 30'
'*87*' '09' C1;;;78;;
'*87*' '0A' ALL;;;01;;

where

'*7F63*'	=	vehicle category/restrictions/conditions tag
'47'	=	length of the data following the tag (71_{10})
'*02*' '01' '04'	=	four data objects are contained in the tag, with the number of objects encoded using BCD
'*87*'…35 30	=	first category of vehicle/restriction/condition data object; licensed for category A1 vehicles not exceeding 250 cm^3 from 23 November 1990 to 15 June 2013
'*87*'…30 30	=	second category of vehicle/restriction/condition data object; category C1 vehicles of less than 8 000 kg valid from 31 May 2003 to 15 June 2013
'*87*'…78;;	=	third category of vehicle/restriction/condition data object; category C1 vehicles restricted to automatic transmission
'*87*'…01;;	=	fourth category of vehicle/restriction/condition data object; driver (i.e. all categories) requires sight correction and/or protection

EXAMPLE 2

The example data noted in Table C.5 can be coded as follows (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*61*' '81AE'
'*5F1F*' '818D' '0F' Smithe-Williams '17' Alexander George Thomas '19 70 03 01 20 02 09 15 20 07 09 30' JPN '43' HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION '11' A290654395164273X
'*7F63*' '1D'
'*02*' '01' '01'
'*87*' '18' C1;'20 00 03 15';'20 10 03 14';S01;<=;'38 30 30 30'

Where,

'*61*'	=	Tag for Data Group 1
'81AE'	=	Overall length of data group (174_{10})
'*5F1F*'	=	Tag for mandatory demographic data
'818D'	=	Overall length of demographic data (141_{10})
'0F'	=	Length of variable length family name(s) (15_{10})
Sm…ams	=	Value of family name(s) field
'17'	=	Length of variable length given name(s) (23_{10})
Alex..mas	=	Value of given name(s) field
'19 70 03 01'	=	Date of birth field (BCD encoded)
'20 02 09 15'	=	Date of issue field (BCD encoded)
'20 07 09 30'	=	Date of expiry field (BCD encoded)
JPN	=	Issuing country field
'43'	=	Length of variable length Issuing Authority field (67_{10})
HOK...ION	=	Issuing authority field
'11'	=	Length of variable length licence number (17_{10})
A290…X	=	Value of licence number field
'*7F63*'	=	Tag for categories/ restrictions data object
'1D'	=	Overall length of categories/ restrictions (29_{10})
'*02*'	=	Tag for integer
'01'	=	Length of number of entries (1_{10})
'01'	=	Number of entries (BCD encoded)
'*87*'	=	Tag for first entry
'18'	=	Length of first entry (24_{10})
C1;	=	Vehicle category C1 field and delimiter
'20 00 03 15';	=	Date of issue field (BCD encoded) and delimiter
'20 10 03 14';	=	Date of expiry field (BCD encoded) and delimiter
S01…'30 30'	=	Limited to vehicles with an authorised mass not exceeding 8 000 kg

The fully encoded version of tag '*5F1F*' is as follows (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*5F1F*' '818D' '0F' '53 6D 69 74 68 65 2D 57 69 6C 6C 69 61 6D 73' '17' '41 6C 65 78 61 6E 64 65 72 20 47 65 6F 72 67 65 20 54 68 6F 6D 61 73' '19 70 03 01 20 02 09 15 20 07 09 30' '4A 50 4E' '43' '48 4F 4B 4B 41 49 44 4F 20 50 52 45 46 45 43 54 55 52 41 4C 20 50 4F 4C 49 43 45 20 41 53 41 48 49 4B 41 57 41 20 41 52 45 41 20 53 41 46 45 54 59 20 50 55 42 4C 49 43 20 43 4F 4D 4D 49 53 53 49 4F 4E' '11' '41 32 39 30 36 35 34 33 39 35 31 36 34 32 37 33 58'

The fully encoded version of tag '*7F63*' is as follows (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*7F63*' '1D' '*02*' '01' '01' '*87*' '18' '43 31 3B 20 00 03 15 3B 20 10 03 14 3B 53 30 31 3B 3C 3D 3B 38 30 30 30'

C.6.3 EF.DG2 Data Group 2 Optional licence holder information, Tag = '6B', short EF identifier = '02'

Data Group 2 contains optional information about the licence holder.

Table C.7

Tag	Length	Value	Value format	Example
5C	X	Tag list	binary	List of all data elements present
5F35	'01'	Gender *(per ISO/IEC 5218)*	1N	1 (Male = 1, Female = 2)
5F64	'02'	Height (cm)	3N	172
5F65	'02'	Weight (kg)	3N	082
5F66	'03'	Eye colour *(per ANSI D20-2003)*	3A	BLU
5F67	'03'	Hair colour *(per ANSI D20-2003)*	3A	BLD
5F11	X	Place of birth	35ADNS[a]	Frozen Foot;Minnesota;USA
5F42	X	Normal place of residence	113ADNS[b]	471 Monica Road;201 Delta Building;Lynnwood;Gauteng;0186;South Africa

NOTE ISO/IEC 18013-1 allows non-metric units to be used for the height and weight values that may appear in Zone II of an IDL.

[a] Three fields delimited by the sub-field delimiter - City; State/Province or District; Country. Addresses that cannot be expressed in the defined character set shall be transliterated.

[b] Six fields delimited by the sub-field delimiter - Street address line 1 (e.g. street name and number); Street address line 2 (e.g. apartment number); City; State/Province or District; Postal Code; Country. Addresses that cannot be expressed in the defined character set shall be transliterated.

EXAMPLE

The example data noted in Table C.7 can be coded as follows (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*6B*' '8186'
'*5C*' '0E' '5F 35 5F 64 5F 65 5F 66 5F 67 5F 11 5F 42'
'*5F35*' '01' 1
'*5F64*' '02' 172
'*5F65*' '02' 082
'*5F66*' '03' BLU
'*5F67*' '03' BLD
'*5F11*' '19' Frozen Foot;Minnesota;USA
'*5F42*' '45' 471 Monica Road;201 Delta Building;Lynnwood;Gauteng;0186;South Africa

Where,

'*6B*'	=	Tag for Data Group 2
'8186'	=	Overall length of data group (134_{10})
'*5C*'	=	Tag for tag list
'0E'	=	Overall length of tag list
'5F 35…5F 42'	=	List of tags of data fields included in this data group
'*5F35*' '01' 1	=	Tag, length (of BCD encoding), gender (male). The gender will be encoded as '01'.
'*5F64*' '02' 172	=	Tag, length (of BCD encoding), height of 172 cm. The height will be encoded as '01 72'.
'*5F65*' '02' 082	=	Tag, length (of BCD encoding), weight of 82 kg. The weight will be encoded as '00 82'
'*5F66*' '03' BLU	=	Tag, length, eye colour blue. The eye colour will be encoded (using ISO/IEC 8859-1) as '42 4C 55'.

'*5F67*' '03' BLD = Tag, length, hair colour bald. The hair colour will be encoded (using ISO/IEC 8859-1) as '42 4C 44'.

'*5F11*' '19' 'Fro…USA = Tag, length (25_{10}), place of birth. The place of birth will be encoded (using ISO/IEC 8859-1) as '46 72 6F 7A 65 6E 20 46 6F 6F 74 3B 4D 69 6E 6E 65 73 6F 74 61 3B 55 53 41'.

'*5F42*' '45' '471….rica = Tag, length (69_{10}), normal place of residence. The normal place of residence will be encoded (using ISO/IEC 8859-1) as '34 37 31 20 4D 6F 6E 69 63 61 20 52 6F 61 64 3B 32 30 31 20 44 65 6C 74 61 20 42 75 69 6C 64 69 6E 67 3B 4C 79 6E 6E 77 6F 6F 64 3B 47 61 75 74 65 6E 67 3B 30 31 38 36 3B 53 6F 75 74 68 20 41 66 72 69 63 61'.

The information will be fully encoded as follows (spaces, underlining, italics and colours are included for legibility only, and are not encoded):

'*6B*' '86'
'*5C*' '0E' '5F 35 5F 64 5F 65 5F 66 5F 67 5F 11 5F 42'
'*5F35*' '01' '01'
'*5F64*' '02' '01 72'
'*5F65*' '02' '00 82'
'*5F66*' '03' '42 4C 55'
'*5F67*' '03' '42 4C 44'
'*5F11*' '19' '46 72 6F 7A 65 6E 20 46 6F 6F 74 3B 4D 69 6E 6E 65 73 6F 74 61 3B 55 53 41'
'*5F42*' '45' '34 37 31 20 4D 6F 6E 69 63 61 20 52 6F 61 64 3B 32 30 31 20 44 65 6C 74 61 20 42 75 69 6C 64 69 6E 67 3B 4C 79 6E 6E 77 6F 6F 64 3B 47 61 75 74 65 6E 67 3B 30 31 38 36 3B 53 6F 75 74 68 20 41 66 72 69 63 61'

C.6.4 EF.DG3 Data Group 3 Optional issuing authority details, Tag = 6C, short EF identifier = '03'

Data Group 3 contains optional document details. All data elements are optional. A tag list is used to indicate which data elements are present.

Table C.8

Tag	Length	Value	Value format	Examples
5C	X	Tag list		
5F68	'19'	Administrative number	25ANS	123456789B
5F69	'01'	Document discriminator[a]	2N	01
5F6D	'01'	Data discriminator[b]	2N	01
5F6A	'03'	ISO issuer ID number[c] (per ISO/IEC 7812-1)	6N	636000

a Number assigned by the issuing authority to differentiate between additional licences (documents) or duplicate documents issued bearing the same licence number as the original, that is 01 for the original licence, 02 for the first duplicate, 03 for the second duplicate and nn for the (nn-1)th duplicate.

b Number assigned by the issuing authority to differentiate between machine-readable data sets on the same physical document where updates have been made to machine-readable data, that is 01 for the original data set, 02 for the first update, 03 for the second update and nn for the (nn-1)th update. The data discriminator is mandatory when any change is made to the machine-readable data (see 5.1).

c ISO number assigned to issuing country or licensing authority, as the case may be.

EXAMPLE

The example data noted in Table C.7 can be coded as follows:

'*6C*' '21'
'*5C*' '09' '5F 68 5F 69 5F 6D 5F 6A'
'*5F68*' '0A' 123456789B
'*5F69*' '01' 01
'*5F6D*' '01' 01
'*5F6A*' '03' 636000

Where,

'*6C*'	=	Tag for Data Group 3
'21'	=	Overall length of data group (33_{10})
'*5C*'	=	Tag list
'09'	=	Overall length of tag list
'5F 68…5F 6A'	=	List of tags of data fields included in this data group
'*5F68*' '0A' 123456789B	=	Tag, length, administrative number. The administrative number will be encoded (using ISO/IEC 8559-1) as '31 32 33 34 35 36 37 38 39 41'.
'*5F69*' '01' 01	=	Tag, length (of BCD encoding), document discriminator of 01. The document discriminator will be encoded as '01'.
'*5F6D*' '01' 01	=	Tag, length (of BCD encoding), data discriminator of 01. The data discriminator will be encoded as '01'.
'*5F6A*' '03' '636000	=	Tag, length (of BCD encoding), issuer ID number. The issuer ID number will be encoded (using ISO/IEC 8859-1) as '36 33 36 30 30 30'.

C.6.5 EF.DG4 Data Group 4 Optional Portrait image, Tag = '6C', short EF identifier = '04'

Data Group 4 contains one or more JPEG and/or WSQ images, Tag = 5F40. The images are encoded according to the settings defined in Annex E. An integer defines the number present. Each instance is headed by an image template Tag.

Table C.9

Tag	Length	Value		
'02'	'01'	Integer, number of portraits encoded		
'A2'	X	Instance of portrait template, repeated for every image included		
		Tag	**Length**	**Value**
		'88'	'07'	Image timestamp
		'89'	'01'	Type of image
		'5F40'	X	JPEG per ISO/IEC 10918-1, JPEG-2000 per ISO/IEC 15444-1, WSQ per IAFIS-IC-0110v3, as specified in Annex E.

EXAMPLE

Assume two portraits have been encoded. Portrait one is a JPEG image with a length of 2035 bytes and a timestamp of 20 February 2007 14:22:23, and portrait two is a JPEG2000 image with a length of 3698 bytes and a timestamp of 21 February 2002 (no time is available for the second portrait),

Then,

‘*65*’ ’821692’
’*02*’ ’01’ 2
‘*A2*’ ’820804’
’*88*’ ’07’ 20070220142223
’*89*’ ’01’ 3
’*5F40*’ ’8207F3’ 2035 byte JPEG image
‘*A2*’ ’820E83’
’*88*’ ’07’ 20020221000000
’*89*’ ’01’ 4
’*5F40*’ ’820E72’ 3698 byte JPEG2000 image

Where,

‘*65*’ ’821692’	=	Tag and overall length of Data Group 4 (5778_{10})
‘*02*’ ’01’ 2	=	Tag, length and number of entries (2). The number of entries will be encoded as '02'.
‘*A2*’ ’820804’	=	Tag and length of the portrait image template
‘*88*’ ’07’ 20070220142223	=	Tag, length and image timestamp.
‘*89*’ ’01’ 3	=	Tag, length and image type (3 = JPEG). The image type will be encoded as '03'.
‘*5F40*’ ’8207F3’…image	=	Tag for image, length and image
‘*A2*…image’	=	Second entry

C.6.6 EF.DG5 Data Group 5, Optional signature/mark image, Tag = ‘67’, short EF identifier = '05'

Data Group 5 contains a signature or usual mark image, Tag = ‘5F43’.

Table C.10

Tag	Length	Value
'89'	'01'	Type of image
'5F43'	X	JPEG per ISO/IEC 10918-1, JPEG-2000 per ISO/IEC 15444-1, WSQ per IAFIS-IC-0110v3, as specified in Annex E.

C.6.7 EF.DG6 Data Group 6, Optional facial biometric template, Tag = ‘75’, short EF identifier = '06'

Data Group 6 contains one or more facial biometric templates. The biometric template is encoded according to the biometric information template used for off-card matching as defined in ISO/IEC 19785-3:2007, clause 11. Regardless of the number of biometric templates present, the nested off-card structure defined in Table 2 of ISO/IEC 7816-11:2004 shall be used.

Table C.11

<table>
<tr><th>Tag</th><th>L</th><th colspan="5">Value</th></tr>
<tr><td>'75'</td><td>X</td><td colspan="5">Data group & optional biometric identification ('75' for Facial, '63' for Finger, '76' for Iris, etc)</td></tr>
<tr><td></td><td></td><td>Tag</td><td>L</td><td colspan="3">Value</td></tr>
<tr><td></td><td></td><td>'7F 61'</td><td>X</td><td colspan="3">Biometric group template</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Tag</td><td>L</td><td>Value</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'02'</td><td>X</td><td>Number of biometric templates in the group</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'7F 60'</td><td>X</td><td>Biometric template (see Table C.12)</td></tr>
</table>

Table C.12

Tag	L	Value							
'7F 60'	X	Biometric template							
		Tag	**L**	**Value**					
		'A1'	X	Biometric Header Template (BHT)					
				Tag	**L**	**Value**	**Presence**	**Value format**	**Example**
				'80'	'02'	Patron header version	Mandatory (if absent, the default value applies)	2 bytes	'01 01'
				'81'	'01' - '03'	Biometric type	Optional	1-3 bytes	Facial = '02' Finger = '08' Iris = '10'
				'82'	'01'	Biometric subtype	Mandatory when applicable	1 byte	binary xx100101 for right hand thumb (given a biometric type '08') binary xx100010 for left eye (given a biometric type of '10')
				'83'	'07'	Biometric data creation date and time (yyyymmddhhmmss)[a]	Optional	14N	20031215173530, representing December 15, 2003, 5:35:30 PM
				'84'	X	BIR creator	Optional	ANS	Hokkaido Prefectural Police Asahikawa Area Public Safety Commission
				'85'	'08'	BDB validity period (yyyymmddyyyymmdd)[b]	Optional	16N	2003121520081214, representing a validity period from December 15, 2003 to December 14, 2008
				'86'	'02'	BDB product owner, product type	Optional	4 bytes (a concatenation of two 16 bit positive integers of value 1 to 65,535)	'00 01 00 82'
				'87'	'02'	BDB format owner	Mandatory	2 byte non-negative integer of value 1 to 65,535	'01 01'
				'88'	'02'	BDB format type	Mandatory	2 byte non-negative integer of value 1 to 65,535	'00 09'

Tag	L	Value							
		Tag	L	Value					
				Tag	L	Value	Presence	Value format	Example
				'90'	X	BIR index (unique identifier used to reference the biometric data set in an application context outside the IDL	Optional	Free format	RecId_1952686A67
		'5F2E' or '7F2E'	X	Biometric data block This data is normally stored in the clear in '5F2E', but it may be enciphered and stored in template '7F2E'.			Mandatory	Format and encoding as specified by BDB format owner and type.	Finger minutia record as specified in ISO/IEC 19794-2:2005, Clause 7
		'53' / '73'	X	BIR payload			Optional		Arbitrary domestic data

[a] If hour, minute, second are not available, 00 shall be used for each value.

[b] Two concatenated dates where the first date is the "from date" (not before), and the second date is the "to date" (not after).

EXAMPLE

Two biometric templates as follows:

Template 1: Facial biometric, created 15 December 2003 at 5:35:30pm, valid from 15 December 2003 through 14 December 2008, product owner number = 1, product type number = 130, format owner number = 271, format type number = 3, biometric data block length = 12634_{10} bytes.

Template 2: Facial biometric, created 7 January 1999 at 10:27:44am, valid from 7 January 1999 through 6 January 2004, product owner number = 1, product type number = 130, format owner number = 271, format type number = 3, biometric data block length = 12711_{10} bytes

Then,

'*75*' '82 63 77'
'*7F 61*' '82 63 72'
'*02*' '01' '02'

'*7F 60*' '82 31 8C'
'*A1*' '2B'
'*80*' '02' '01 01'
'*81*' '01' '02'
'*82*' '01' '00'
'*83*' '07' '20 03 12 15 17 35 30'
'*85*' '08' '20 03 12 15 20 08 12 14'
'*86*' '04' '00 01 00 82'
'*87*' '02' '01 01'
'*88*' '02' '00 03'
'*5F 2E*' '82 31 5A' '.....12634 byte Biometric Data Block....'

'*7F 60*' '82 31 D9'
'*A1*' '2B'
'*80*' '02' '01 01'

'81' '01' '02'
'82' '01' '00'
'83' '07' '19 99 01 07 10 27 44'
'85' '08' '19 99 01 07 20 04 01 06'
'86' '04' '00 01 00 82'
'87' '02' '01 0F'
'88' '02' '00 03'
'5F 2E' '82 31 A7' '.....12711 byte Biometric Data Block....'

Where,

'75'	=	Tag for DG6, Optional facial biometric
'82 63 77'	=	Overall length of data group (25463_{10} = '82 63 77')
'7F 61'	=	Tag for biometric group template
'82 63 72'	=	Overall length of biometric group (25458_{10} = '82 63 72')
'02' '01' '02'	=	Number of entries
'7F 60'	=	Tag for biometric template
'82 31 8C'	=	Overall length of biometric template (12684_{10} = '82 31 8C')
'A1' '2B'	=	Biometric header tag and length (43_{10} = '2B')
'80' '02' '01 01'	=	Patron version
'81' '01' '02'	=	Facial biometric type
'82' '01' '00'	=	Biometric subtype (none for face)
'83' '07' 20031215173530	=	Date and time of creation 15 December 2003. This will be encoded as '20 03 12 15 17 35 30'.
'85' '08' 2003121520081214	=	Validity period. This will be encoded as '20 03 12 15 20 08 12 14'.
'86' '04' '00 01 00 82'	=	Product owner and type (130_{10} = '82')
'87' '02' '01 0F'	=	Format owner (271_{10} = '01 0F')
'88' '02' '00 03'	=	Format type (3_{10} = '00 03')
'5F 2E' '82 31 5A'	=	Length of biometric data block (12634_{10} = '82 31 5A')
..Biometric..	=	Biometric data block encoded per above defined owner and format
'7F 60'	=	Tag for biometric template
'82 31 D9'	=	Overall length of biometric template (12761_{10} = '82 31 D9')
'A1' '2B'	=	Biometric header tag and length (43_{10} = '2B')
'80' '02' '01 01'	=	Patron version
'81' '01' '02'	=	Facial biometric type
'82' '01' '00'	=	Biometric subtype (none for face)
'83' '07' 19990107102744	=	Date and time of creation 7 January 1999. This will be encoded as '19 99 01 07 10 27 44'.
'85' '08' 1999010720040106	=	Validity period. This will be encoded as '19 99 01 07 20 04 01 06'.
'86' '04' '00 01 00 82'	=	Product owner and type (130_{10} = '82')
'87' '02' '01 0F'	=	Format owner (271_{10} = '01 0F')
'88' '02' '00 03'	=	Format type (3_{10} = '00 03')
'5F 2E' '82 31 A7'	=	Length of biometric data block (12711_{10} = '82 31 A7')
..Biometric..	=	Biometric data block encoded per above defined owner and format

NOTE Tags for biometric templates are defined and assigned in ISO/IEC 7816-11. Any tag in the above example that is not listed in Table C.12 originates from ISO/IEC 7816-11.

C.6.8 EF.DG7 Data Group 7, Optional finger biometric, Tag = '63', short EF identifier = '07'

Data Group 7 is encoded the same as Data Group 6. Specific data elements will have different values as the biometric is for fingers rather than faces.

EXAMPLE

Finger biometric (right hand thumb), created 15 December 2003 at 5:36:12pm, valid from 15 December 2003 through 14 December 2008, product owner number = 13, product type number = 99, format owner number = 21, format type number = 7, biometric data block length = 834_{10} bytes

Then,

'*63*' '82 03 81'

'*7F 61*' '82 03 7C'
'*02*' '01' '01'

'*7F 60*' '82 03 74'
'*A1*' '2B'
'*80*' '02' '01 01'
'*81*' '01' '08'
'*82*' '01' '05'
'*83*' '07' '20 03 12 15 17 36 12'
'*85*' '08' '20 03 12 15 20 08 12 14'
'*86*' '04' '00 0D 00 63'
'*87*' '02' '00 15'
'*88*' '02' '00 07'
'*5F 2E*' '82 03 42' '….834 byte Biometric Data Block….'

Where,

'*63*'	=	Tag for DG7, Optional finger biometric
'82 03 81'	=	Overall length of data group (897_{10} = '82 03 81')
'*7F 61*'	=	Tag for biometric group template
'82 03 7C'	=	Overall length of biometric group (892_{10} = '82 03 7C')
'02' '01' '01'	=	Number of entries
'*7F 60*'	=	Tag for biometric template
'82 03 74'	=	Overall length of biometric template (884_{10} = '82 03 74')
'*A1*' '2B'	=	Biometric header tag and length (43_{10} = '2F')
'*80*' '02' '01 01'	=	Patron version
'*81*' '01' '08'	=	Finger biometric type
'*82*' '01' '05'	=	Biometric subtype: right hand thumb
'*83*' '07' 20031215173612	=	Date and time of creation 15 December 2003. This will be encoded as '20 03 12 15 17 36 12'.
'*85*' '08' 2003121520081214	=	Validity period. This will be encoded as '20 03 12 15 20 08 12 14'.
'*86*' '04' '00 0D 00 63'	=	Product owner and type (13_{10} = '0D', 99_{10} = '63')
'*87*' '02' '00 15'	=	Format owner (21_{10} = '00 15')

'*88*' '02' '00 07'	=	Format type (7_{10} = '00 07')
'*5F 2E*' '82 03 42'	=	Length of biometric data block (834_{10} = '82 03 42')
..Biometric..	=	Biometric data block encoded per above defined owner and format

NOTE Tags for biometric templates are defined and assigned in ISO/IEC 7816-11. Any tag in the above example that is not listed in Table C.11 originates from ISO/IEC 7816-11.

C.6.9 EF.DG8 Data Group 8, Optional iris biometric, Tag = '76', short EF identifier = '08'

Data Group 8 is encoded the same as Data Group 6. Specific data elements will have different values as the biometric is for irises rather than faces.

C.6.10 EF.DG9 Data Group 9, Optional other biometric, Tag = '70', short EF identifier = '09'

Data Group 9 is encoded the same as Data Group 6. Specific data elements will have different values as the biometric is not for faces.

C.6.11 EF.DG10, Data Group 10 Reserved for future use, No Tag assigned, short EF identifier = '0A'

This data group is reserved for future use and the content will be defined at a future stage.

C.6.12 EF.DG11, Data Group 11 Optional domestic data, Tag to be assigned by issuing authority, short EF identifier = '0B'

This data group is reserved for domestic use and hence the encoding is defined domestically.

Appendix A to Annex C
(informative)

Use of basic encoding rules of ASN.1[10]

C.A.1 BER-TLV data object

Each BER-TLV data object (see ISO/IEC 8825-1) shall consist of 2 or 3 consecutive fields.

- The tag field T consists of one or more consecutive bytes. It encodes a class, a type and a number.
- The length field consists of one or more consecutive bytes. It encodes an integer L.
- If L is not null, then the value field V consists of L consecutive bytes. If L is null, then the data object is empty: there is no value field.

Neither '00' nor 'FF' is used as tag values.

NOTE Before, between or after BER-TLV data objects, '00' or 'FF' bytes without any meaning may occur (e.g., due to erased or modified TLV-coded data objects).

C.A.2 Tag field

The bits b8 and b7 of the leading byte of the tag field shall encode the tag class, i.e., the class of the data object.

- b8-b7=00 introduces a tag of universal class.
- b8-b7=01 introduces a tag of application class.
- b8-b7=10 introduces a tag of context-specific class.
- b8-b7=11 introduces a tag of private class.

The bit b6 of the leading byte of the tag field shall encode the tag type, i.e., the type of the data object.

- b6=0 introduces a primitive data object.
- b6=1 introduces a constructed data object.

If the bits b5 to b1 of the leading byte are not all set to 1, then they shall encode an integer equal to the tag number which therefore lies in the range from 0 to 30. Then the tag field consists of a single byte.

Otherwise (b5 to b1 set to 1 in the leading byte), the tag field shall continue on one or more subsequent bytes.

- The bit b8 of each subsequent byte shall be set to 1, unless it is the last subsequent byte.
- The bits b7 to b1 of the first subsequent byte shall not be all set to 0.

[10] Abstract from clause 5.2.2 of ISO/IEC 7816-4: 2005

- The bits b7 to b1 of the first subsequent byte, followed by the bits b7 to b1 of each further subsequent byte, up to and including the bits b7 to b1 of the last subsequent byte, shall encode an integer equal to the tag number (thus strictly positive).

C.A.3 Length field

In short form, the length field consists of a single byte where the bit b8 shall be set to 0 and the bits b7 to b1 shall encode an integer equal to the number of bytes in the value field. Any length from 0 to 127 can thus be encoded by 1 byte. In long form, the length field consists of a leading byte where the bit b8 shall be set to 1 and the bits b7 to b1 shall not be all equal, thus encoding a positive integer equal to the number of subsequent bytes in the length field. Those subsequent bytes shall encode an integer equal to the number of bytes in the value field. Any length within the APDU limit (up to 65 535) can thus be encoded by 3 bytes.

NOTE ISO/IEC 7816 does not use the indefinite lengths specified by the basic encoding rules of ASN.1 (see ISO/IEC 8825-1).

Table C.A.1 — ASN.1 Length encoding rules

Range	# of bytes	1st byte	2nd byte	3rd byte
0 to 127	1	binary value	none	None
128 to 255	2	'81'	binary value	None
256 to 65,535	3	'82'	binary value	
			most significant byte	least significant byte

Appendix B to Annex C
(normative)

List of Tags used

‘02’	Integer
'53'	EF.CE – Compact encoded object
‘5C’	Tag list
‘5F01’	LDS version number
‘5F11’	Place of birth
‘5F1F’	Data Object of Mandatory Demographic Data Objects
‘5F35’	Gender
‘5F40’	Portrait image
‘5F42’	Place of residence
‘5F43’	Signature/mark image
'5F64’	Height
'5F65’	Weight
‘5F66’	Eye colour
‘5F67’	Hair colour
‘5F68’	Administrative number
‘5F69’	Document discriminator
‘5F6A’	ISO issuer ID
'5F6D'	Data discriminator
‘60’	EF.COM
‘61’	EF.DG1 – Mandatory data
‘63’	EF.DG7 - Optional finger biometric template
‘65’	EF.DG4 – Optional portrait image
‘67’	EF.DG5 – Optional signature/usual mark image
‘6B’	EF.DG2 – Optional licence holder details
‘6C’	EF.DG3 – Optional issuing authority details

‘75’	EF.DG6 – Optional facial biometric template
‘76’	EF.DG8 – Optional iris biometric template
‘70’	EF.DG9 – Optional other biometric template
‘7F63’	Constructed data object of categories of vehicles/restrictions/conditions
'87'	Driving Licence category of vehicle/restriction/condition data object
'88'	Image timestamp
'89'	Type of image
'A2'	Image template

Additional tags are defined in Table C.11 and Table C.12 for use within Data Groups 6, 7 and 8.

Appendix C to Annex C
(normative)

Command set

C.C.1 Command structure

Command APDU, of which the basic command structure is shown below, is a message structure to transmit a command. The message structure is defined in ISO/IEC 7816-4.

NOTE 1 Additional commands other than those specified below may be used where such use does not detract from the intended function of the command set.

NOTE 2 The command set should be updated in conjunction with the periodic revision of ISO/IEC 7816-4, but care shall be taken to ensure that the functions remain backwards compatible.

NOTE 3 The commands governing security are described in ISO/IEC 18013-3.

Header				Body		
CLA	INS	P1	P2	Lc	Data field	Le

Lc : length (in bytes) of data field of command APDU (command data)

Le : expected maximum length (in bytes) of data field of response APDU (response data)

C.C.1.1 Command APDU

Command APDU is classified into the following four cases depending on command

Case 1: without command data and response data

Header

Case 2: without command data but with response data

Header	Body
	Le

Case 3: with command data but without response data

Header	Body	
	Lc	Data field

Case 4: with command data and response data

Header	Body		
	Lc	Data field	Le

It is possible to specify Lc/Le (the length is expressed in 1 byte) or used extended Lc/Le.

C.C.1.2 Response APDU

Response APDU, of which structure is shown below, is a message structure of a response to command APDU.

Case without response data (Case 1 and 3 of command APDU)

Trailer	
SW1	SW2

Case with response data (Case 2 and 4 of command APDU)

Body	Trailer	
Data	SW1	SW2

C.C.2 Command list

The minimum command set shall be as follows:

SELECT Command

The SELECT command sets a current file.

DF selection shall be used for the function with 'AID'='A0 00 00 02 48 02 00' for the Standard Application or with 'AID'='A0 00 00 02 48 03 00' for the Compact Application.

EF selection shall be used for the function EFID or Short EFID.

NOTE Short EFID function includes in READ BINARY command.

READ BINARY Command

This command reads out binary data in a transparent structured WEF.

This command is executed for EF specified by a valid short EF identifier or for a current EF.

Reading data is less than 256 bytes: INS='B0' and relative address (8 bits + short EFID in P1 and P2) shall be used for beginning reading address.

Reading data is less than 32KB: INS='B0' and relative address (15 bits in P1 and P2) shall be used for beginning reading address.

Reading data is more than 32KB: INS='B1' and relative address (32 bits in Tag'54' in data field) shall be used for beginning reading address.

The details of the commands specified in this specification are shown in the table below.

Item number	Command name	CLA	INS	Case number			
				1	2	3	4
1	SELECT	0X	A4	X		X	X
2	READ BINARY		B0/B1		X		

Note: Write command functions are out of scope in this standard.

C.C.3 Class byte

The value for CLA shall be '0X' in this Part of ISO/IEC 18013 to confirm that:

- Command chaining is not supported

- Secure messaging is not supported

- Logical channel at least 'Channel 0' is supported

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	X	-	-	-	-	**Command chaining control**
0	0	0	0	-	-	-	-	The command is the last or only command of a chain
0	0	0	0	x	x	-	-	**Secure messaging indication**
0	0	0	0	0	0	-	-	No secure messaging or no indication
0	0	0	0	0	0	X	X	**Logical channel number from zero to three**

NOTE: Command chaining and secure messaging is specified in ISO/IEC 18013-3.

C.C.4 Commands

C.C.4.1 SELECT command

C.C.4.1.1 Definition and application area

SELECT FILE command sets a current file. Subsequent commands are able to refer to current files implicitly. After a DF is selected, there is no currently selected EF and an EF must be selected. The EF may be selected by use of the SELECT command or by use of a short EF identifier in the READ command.

C.C.4.1.2 Use and security conditions

Security status is changed when status byte of response APDU to the SELECT FILE command indicates a sign: "process completed".

C.C.4.1.3 Command APDU

DF selection (without request for FCI) (Case 3)

CLA	INS	P1	P2	Lc	Data field
'0x'	'A4'	'04'	'0C'	'06'	'AID'='A0 00 02 48 02 00'

EF selection (without request for FCI) (Case 3)

CLA	INS	P1	P2	Lc	Data field
'0x'	'A4'	'02'	'0C'	'02'	(EF-ID)

P1 coding

b8	b7	b6	b5	b4	b3	b2	b1	Description
0	0	0	0	0	0	x	x	Selection by file ID
						1	0	EF directly under current DF(data division=EF-ID)
0	0	0	0	0	1	0	0	Direct selection by DF name(Data field=DF name)

P2 coding

b8	b7	b6	b5	b4	b3	b2	b1	Description
0	0	0	0	0	0			FCI option template reply
0	0	0	0	1	1			No FCI reply
						0	0	Selection of the first or the only file

Note: No FCI response is expected at P2 setting for compatibility.

C.C.4.1.4 Response APDU

SW1	SW2

C.C.4.1.5 Status byte list

Status		Status description	Execution state	
SW1	SW2			
“ 90”	“ 00”	Normal termination	Normal termination	Process completed
“ 62”		Status of non-volatile memory is unchanged	Warning processing	
	“ 83”	DF is blocked		
“ 64”		Status of non-volatile memory is unchanged	Execution error	Process discontinued
	“ 00”	Control data of a file is abnormal		
“ 67”	“ 00”	Incorrect Lc/Le	Command error	
“ 68”		No CLA function is provided		
	“ 81”	No access is provided by specified logical channel number		
	“ 82”	No secure messaging is provided		
“ 6A”		Incorrect parameter		
	“ 81”	No function is provided		
	“ 82”	No file to access		
	“ 86”	Value of P1-P2 is incorrect		
	“ 87”	Value of Lc is inconsistent with P1-P2		
“ 6D”	“ 00”	No INS is provided		
“ 6E”	“ 00”	No class is provided		

C.C.4.2 READ BINARY command

C.C.4.2.1 Definition and application area

This command reads out binary data in a transparent structured EF.

C.C.4.2.2 Use and security conditions

This command is executed for EF specified by a valid short EF identifier or for a current EF. The specified EF becomes a current EF when "process completed" is indicated as to status byte of response APDU to this command.

"Process discontinued" would be indicated when DF is blocked.

C.C.4.2.3 Command APDU for up to 32kB (Case2)

CLA	INS	P1	P2	Le
'0x'	'B0'			

(Parameter of Read Binary command)

Parameter name	Length	Description	Remarks
P1-P2	2	Relative address of the first binary data to read and, optionally, a short EF identifier	See the table below
Le	1 or 3	The number of bytes to read	

(P1-P2 coding (15-bit relative address is specified))

P1								P2								Description
b8	B7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
0																15-bit relative address is specified
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Relative address (15 bits)
	~							~								
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

(P1-P2 coding (8-bit relative address is specified))

P1								P2								Description
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0														8-bit relative address is specified
			0	0	0	0	0									Current EF is specified
			0	0	0	0	1									Short EF identifier is specified
			~													
			1	1	1	1	0									
								0	0	0	0	0	0	0	0	Relative address (8 bits)
								~								
								1	1	1	1	1	1	1	1	

C.C.4.2.4 Command APDU for more than 32kB (Case4)

CLA	INS	P1	P2	Lc	Data field	Le
'0x'	'B1'				offset data object	

If bit 1 of INS is set to 1, then P1-P2 shall identify an EF. If the first eleven bits of P1-P2 are set to 0 and if bits 5 to 1 of P2 are not all equal and if the card and/or the EF supports selection by short EF identifier, then bits 5 to 1 of P2 encode a short EF identifier (a number from one to thirty). Otherwise, P1-P2 is a file identifier. P1-P2 set to '0000' identifies the current EF. At least one offset data object with Tag '54' shall be present in the command data field. When present in a command or response data field, data shall be encapsulated in a discretionary data object with Tag '53' or '73'.

C.C.4.2.5 Response APDU

Data	SW1	SW2

Le = '00', the command reads all bytes in the EF starting at the relative address. The maximum number of bytes depends on the type of length field used, short length (256 bytes) or extended length (65,536 bytes).

C.C.4.2.6 Status byte list

Status		Status description	Execution state	
SW1	SW2			
" 90"	" 00"	Normal termination	Normal termination	Process completed
" 62"		Status of non-volatile memory is unchanged	Warning processing	
	" 83"	DF is blocked		
" 64"		Status of non-volatile memory is unchanged	Execution error	Process discontinued
	" 00"	Control data of a file is abnormal		
" 67"	" 00"	Incorrect Lc/Le	Command error	
" 68"		No CLA function is provided		
	" 81"	No access is provided by specified logical channel number		
	" 82"	No secure messaging is provided		

Status		Status description	Execution state	
SW1	SW2			
“ 69”		Command is not permitted		
	“ 81”	Inconsistent command with file structure		
	“ 82”	Security status is unsatisfied		
	“ 86”	No current EF exists		
“ 6A”		Incorrect parameter		
	“ 82”	No file to access		
	“ 86”	Value of P1-P2 is incorrect		
“ 6B”	“ 00”	Offset is specified outside EF range		
“ 6D”	“ 00”	No INS is provided		
“ 6E”	“ 00”	No class is provided		