Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St./11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

Issuing Office - Bureau de distribution
Communication Procurement Directorate/Direction de l'approvisionnement en communication
360 Albert St./ 360, rue Albert
12th Floor / 12ième étage
Ottawa
Ontario
K1A 0S5

Title - Sujet DND Security ID Cards	
Solicitation No. - N° de l'invitation W6369-18RFI1/A	**Date** 2018-08-20
Client Reference No. - N° de référence du client W6369-18-RFI1	**GETS Ref. No. - N° de réf. de SEAG** PW-$$CW-035-75307
File No. - N° de dossier cw035.W6369-18RFI1	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2018-10-01**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Buck(CW Div.), Daniel	**Buyer Id - Id de l'acheteur** cw035
Telephone No. - N° de téléphone (613) 998-8582 ( )	**FAX No. - N° de FAX** (613) 991-5870

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

DEPARTMENT OF NATIONAL DEFENCE
101 COLONEL BY DR.
OTTAWA
Ontario
K1A0K2
Canada

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée See Herein	**Delivery Offered - Livraison proposée**

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N°de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

REQUEST FOR INFORMATION

1. EXECUTIVE SUMMARY

This document provides basic information regarding the requirements of Vice Chief of the Defence Staff (VCDS)\Director General Defence Security (DGDS)\Director Personal Security and Identity Management (DPSIM) National Defence Identification Services (NDIS) to improve the efficiency of identification management related activities. To that end, NDIS is seeking solutions that could automate the management of identification across the enterprise and produce identification in accordance with the Canadian Driver Licence Agreement (CDLA) requirements with some amendments to the various fields and features of the cards. The requirement includes the follow-on replacement of expiring cards. This document includes a description of the anticipated requirements National Defence Identification card printing capacities.

2. PURPOSE

This Industry Consultation process seeks information from industry on its interest, capacity and ability to produce and deliver high-volume printers and associated blank card stock that can meet the security, technical, and distribution requirements of NDIS. This Request for Information (RFI) provides industry the opportunity to give feedback on the printing options. The information gathered through this Industry Consultation process will be used by Canada to assist in the development of a Request for Proposal (RFP) for the procurement of printer(s) used to produce National Defence Identification cards.

3. BACKGROUND

The National Defence Identification Program (NDIP) is a nationally delivered service that provides a high degree of assurance related to the identity of: DND employees; CAF members; Foreign Forces personnel employed by DND or serving with CAF, and their dependents; and individuals requiring a supplementary ID card and who are entitled to special provision by convention, legislation or policy. This mandate is carried out by the NDIS team and its internationally dispersed Identification Operators.

Identification Cards: A National Defence ID card is a document issued by DND and CAF to identify the bearer as a DND employee, CAF member or other personnel requiring official identification. DPSIM is responsible for issuing ID cards. All ID cards are produced by NDIS on behalf of DGDS. The NDIS produces both primary and specialty ID cards which are issued and used according to specific requirements, specifications and entitlements. National Defence ID cards are controlled documents and consequently must be safeguarded. Individuals in receipt of one or more cards are responsible for their protection and must keep them safe.

NDIS wishes to modernize the way it produces Identification Cards for DND/CAF. Part of this modernization includes potential linkages of attributes such as personal information and biometric data to support physical and logical access.

Business Impact Analysis: The NDIS provides the official ID cards that are utilized for all CAF and permanent DND civilian employees. The NDIS staff are located at Pearkes and receive requests for ID cards from all of the CAF bases across Canada and other locations around the world. The information for the cards is sent, via Canada Post mail from these locations to NDIS, registered into the database, a card is printed out and then mailed back to the originators for distribution. The NDI 75 Veteran's Service Card (CAF 'retirement card') will be reinstituted September 2018 in various phases along with the potential for creation of other NDI card styles (i.e. Rangers, Family) which will also increase production requirements.

These modernized ID cards may also evolve to incorporate the DND 404 (military driver's licence) so their design will need to meet CDLA standards. The NDIS database also:

- keeps track of tombstone data for all DND civilian and military members,
- produces ID cards for military spouses,
- produces ID cards for allied members, and
- keeps track of fingerprint classification for military members for identification purposes.

4. STAKEHOLDERS

Primary Stakeholders and associated projects:

- National Defence Identification Service (NDIS)
- Director Information Management End User Support (DIMEUS)
- Director Information Management Engineering and Integration (DIMEI)
- Designated Public Key Infrastructure (PKI)
- Shared Services Canada (SSC)
- Director General Cyber – Identity Credential and Access Management (ICAM) Project
- Director General Information Management Project Delivery (DGIMPD) – Digital Biometric Collection and Identity Management (DBCIDM) Project
- Director General Information Management Project Delivery (DGIMPD) – Web Security Clearance Processing System (WebSCPS)

Secondary Stakeholders and associated projects:

- Military Police
- Personnel Security Screening Office
- Facilities Management
- Linkages with Other Government Departments such as RCMP, VAC, and CRA.

5. QUESTIONS

DND/CAF Environment. When providing feedback, suppliers are asked to consider how a product would integrate into an environment with the following characteristics:

1. Complex network infrastructures with various enclaves and IT security zones requiring the use of several zone interface points and information exchange gateways;
2. Both virtualized and non-virtualized environment;
3. Various operating systems (servers and clients) including MS Windows for desktops, mobile and servers and Linux for desktops and servers;
4. Shared responsibility for the IT environment between SSC (e.g. network and server infrastructure) and DND/CAF (e.g. applications and endpoints); and
5. Storage and transmission of Protected A information that in the aggregate would become Protected B.

Architecture/Infrastructure Questions. When providing their feedback, suppliers are asked to consider:

6. What are the software/technical requirements to integrate a solution to an existing network; and
7. Is it possible to address scalability issues in high volume card production (potentially need to address initial production capacity of 700k cards over a period of two years with steady state of approx. 60k cards per year) to reduce the impact on the network (e.g. bandwidth, availability)? What is the estimated network capacity requirement on a per end-point basis?

Security/Certification and Accreditation Questions. When providing their feedback, suppliers are asked to consider:

8. Are options available for certification/accreditation by trusted governmental organizations or large private corporations (banks or others)? If so, which certifications/accreditations have been achieved;
9. How are communications between the central authority and the devices protected? Are there products that would support CSE approve key management technologies and processes;
10. If encryption keys are employed, how are the keys safeguarded on the hosts;
11. Are there products that provide granular role-based access control and regulate permissions based on the user's responsibility;
12. Are there products that provide auditing and logging features? If so, are the logs stored (locally, centrally, both); and
13. Would these products include any additional security features? If so, list them.

Customization Questions. When providing their feedback, suppliers are asked to consider:

14. What report generation capabilities are available for these products? What format(s) are supported for these reports (e.g. PDF, RTF, MS Word, Excel, etc.)? Can these reports be customized;
15. What dashboard capabilities does your product provide? How customizable is the dashboard? Can the dashboard include input from other products from other manufacturers;
16. Are there products that allow users to build custom queries and search for specific information? What are the languages and the mechanisms used (e.g. internet search engine format, regular expressions, etc.);
17. Can these products typically make use of custom scripts to automate some of the product functionalities? What language does it use or support;
18. Are there products available that include analytics and trending analysis capabilities? If so, please provide details;
19. What languages/regional support would that these products would provide (e.g. FR-CA, EN-CA, etc.);
20. What means are used to incorporate the Human Readable Data Elements as specified in Appendix 3 of the CDLA onto an identification card;
21. What means are used to incorporate the Machine Readable Data Elements as specified in Appendix 4 of the CDLA onto an identification card;
22. What options are available for the incorporation of security devices as specified in Appendix 5 of the CDLA onto an identification card;
23. What options are available for the incorporation of card design specifications as specified in Appendix 6 of the CDLA onto an identification card;
24. What options are available for the incorporation of the Driver's Licence Security Device Index as specified in Appendix 7 of the CDLA onto an identification card; and
25. What options are available for the incorporation of the card durability test methods specifications as specified in Appendix 8 of the CDLA onto an identification card?

Vendor Support Questions. When providing their feedback, suppliers are asked to consider:

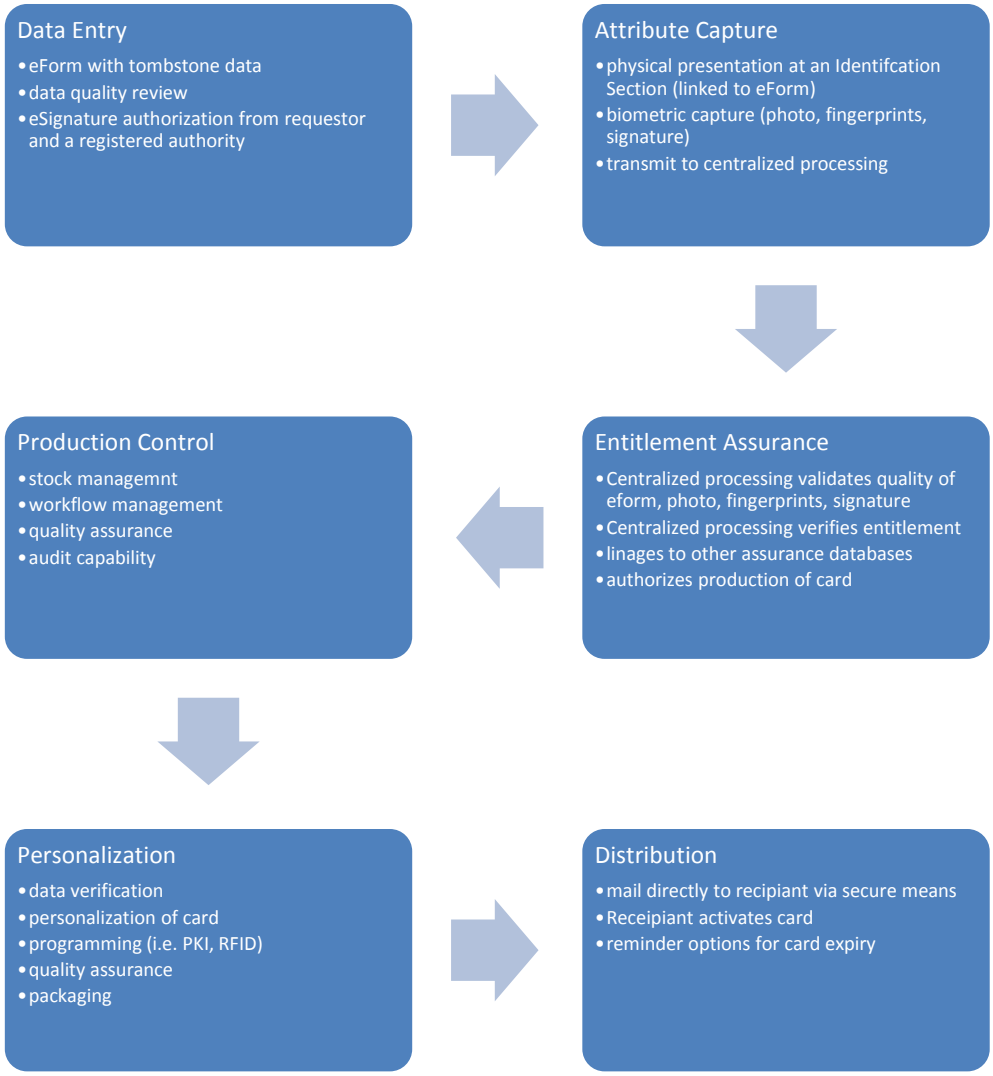
26. How frequent are product updates or new capabilities released and how long is support maintained for previous versions for these products;
27. How frequently are patches and/or service packs for these products released and what mechanism is used for patching/updates;
28. What is the process for updating/patching installations with no direct Internet connectivity;
29. What is the licensing model for these products (e.g. subscription based, perpetual with yearly fees, etc.); and
30. What are the product support models (e.g. direct to the OEM or through a third party) for these type of products?

Procurement Questions:

31. Are there any limitations or issues that would limit that potential suppliers? Please explain any limitations that are identified.
32. Which environmental initiatives have been implemented by the industry and which environmental initiatives could the industry plan to implement in the near future (recycling/reusing initiatives, etc.?) Please explain and specify.
33. In regards to environmental standards, what environmental standards are typically included as as a rated criteria in the solicitation process?
34. Does the industry conform to recognize to environmental standards such as ENERGY STAR, or others? Please explain and specify.
35. Is there any other information or recommendations that should be considered? Please explain.

6. PROCESS MAP

Below is a process map of the anticipated identification request process. The objective of showing this is to demonstrate where the printing solution fits into the identification process.



7. ENQUIRIES

Respondents with questions regarding this RFI may direct their enquiries to:

Name: Daniel Buck
Title: Supply Specialist
Communication Procurement Directorate
Acquisitions Branch
Public Services and Procurement Canada
Address: 360 Albert Street, 12th Floor
Ottawa, Ontario K1A 0S5
Telephone: (613) 990-4033
Facsimile: (613) 998-8582
E-mail: Daniel.buck@pwgsc-tpsgc.gc.ca or TPSGC.padgamiace-appbmpace.PWGSC@tpsgc-pwgsc.gc.ca

Because this is not a bid solicitation, Canada may publish additional questions for the purposes of gaining additional information. Canada asks Respondents to visit Buyandsell.gc.ca regularly to check for changes, if any.

8. SUBMISSION OF RESPONSES

Time and Place for Submission of Responses: Suppliers interested in providing information to the specific questions listed in Section 5 should send the responses directly to the contact identified in Section 7 Enquiries, by the time and date indicated on page 1 of this RFI. Responses can be submitted by mail, by fax or by email.

9. NOTES TO INTERESTED FIRM(S)

This Industry Consultation process is not a bid solicitation and a contract will not result from this request.

Potential respondents are advised that any information submitted to Canada in response to this Industry Consultation process may be used by Canada in the development of a subsequent competitive RFP. However, the Government is not bound to accept any Expression of Interest or to consider it further in any associated documents such as a RFP.

The issuance of this Industry Consultation process does not create an obligation for Canada to issue a subsequent RFP, and does not bind Canada legally or otherwise, to enter into any agreement or to accept any suggestions from organizations. Canada reserves the right to accept or reject any or all comments received.

There will be no short listing of firms for purposes of undertaking any future work, as a result of this request. Similarly, participation in this Industry Consultation process is not a condition or prerequisite for participation in any RFP(s).

Companies participating in this Industry Consultation process should identify any submitted information that is to be considered as either company confidential or proprietary.

All enquiries and other communications related to this Industry Consultation process shall be directed exclusively to the PSPC Procurement Authority.

CDLA APPENDIX 1: HUMAN READABLE DATA ELEMENTS SPECIFICATION

1. Scope

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

This specification supersedes the AAMVA DL/ID 2000 Standard published June 6, 2000. Requests for interpretation, suggestions for improvement or addenda, or defect reports are welcome. They should be sent to the CCMTA Secretariat for review and consultation with AAMVA for possible inclusion in subsequent iterations.

A DL/ID is in conformance with this standard if it meets all mandatory requirements specified directly or by reference herein, including requirements contained in Appendices 2, 3, 4, 5, 6, 7 and 8.

1.1. Normative reference(s)

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

- European Commission Directive 2000/56/EC of 14 September 2000 O.J. EC No. L 237/45
- European Union Council Directive 97/26/EC of 2 June 1997 O.J. EC No. L 150/41
- European Union Council Directive 96/47/EC of 23 July 1996 O.J. EC No. L 235/1
- European Union Council Directive 91/439/EEC of 29 July 1991 O.J. EC No. L 237/1
- ANSI D-20: *Data Element Dictionary - Traffic Records System*ANSI INCITS 385: - *Digital Image Attributes, Face Interchange Format (Human and Automated)*ISO/IEC 18013-1: *ISO compliant driving licence - Part 1: Physical Characteristics and Basic Data Set*ISO/IEC 7810: *Identification cards - Physical characteristics*
- ISO/IEC 7811: *Identification cards - Recording Techniques*
- ISO/IEC 7812: *Identification cards - Registration Numbers*
- ISO/IEC 10373: *Identification cards - Test methods*
- ISO/IEC 10918: JPEG 2000
- ISO/IEC 11693: *Identification cards - Optical Memory - General Characteristics*
- ISO/IEC 11694: *Identification cards - Optical Memory - Linear Recording Method*
- ISO/IEC 15438: *Automatic Identification and Data Capture Techniques - International Two-dimensional Symbology Specification - PDF417*
- ANSI/ASQZ Z1.4: *Military standard, sampling procedures and tables for inspection by attributes*
- MIL-L-61002 *Labels, Pressure Sensitive Adhesive, for Bar-Codes and other Markings*
- UN Convention on Road Traffic (*Geneva - 19 September 1949), amended 22 October 1964*
- UN Convention on Road Traffic (*Vienna - 8 November 1968), Amendment 1 amended 3 September 1993 (E/CONF.56/16/REV.1/Amend.1)*

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

1.2 Term(s) and definition(s)

For the purpose of this CCMTA specification, the terms and definitions given in the following apply:

1.2.a alphabetic (A)

Alpha characters (UPPERCASE letters from A to Z).

1.2.b alphanumeric (ANS)

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

1.2.c cardholder

An individual to whom a driver licence or identification card is issued.

1.2.d country of distinguishing sign

Abbreviation used on the licence document (human-readable) for countries that issue driver licences.

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

1.2.f data element

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

1.2.g digital

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

1.2.h document recognition

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

1.2.i driver licence (DL)

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

1.2.j DL/ID

Refers generally to both or either driver licences (DL) and identification cards (ID).

1.2.k first line inspection (level 1)

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

1.2.l human-readable

Data or information that is printed or engraved that is visually present on a driver licence.

1.2.m identification card (ID)

For the purposes of this document, "identification card" shall be defined as "A card issued to a person whose identity is verified in the same manner as required for the issuance of a driver licence by a licensing authority for identification purposes only." This definition does not include any other identification provided by the department [of motor vehicles], such as provincial/territorial employee identification, senior citizen cards, etc.

1.2.n image

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

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

1.2.p issuing authority

A statutorily authorized agent organization that issues driver licences and/or identification cards such as s Ministry of Transport, Department of Motor Vehicles, or Police Agency.

1.2.q machine-readable

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

1.2.r mutual recognition agreements

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

1.2.s non-portrait side of card

The opposite face from the portrait side.

1.2.t numeric(N)

Digits 0 to 9.

1.2.u portrait side of card

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

1.2.v second line inspection (level 2)

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

1.2.w signature panel

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

1.2.x third line inspection (level 3)

Inspection by forensic specialists conducting detailed examination allows for more in-depth evaluation and may require special equipment to provide true certification.

1.2.y visual special characters (S)

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

1.3. Human Readable Data Elements

1.3.1 Data Elements Table

Table 1 in section 1.3 describes the mandatory data elements that must visually appear on compliant DL/ID documents. Jurisdictions may go beyond these minimum mandatory requirements, as long as each mandatory requirement is met. Table 2 in section 1.4 describes optional data elements that may visually appear on compliant DL/ID documents. Jurisdictions may include additional data elements and features on their compliant DL/ID document. However, if any of the optional data elements are included on the document, they should appear as described by the rules in this specification.

1.3.2 Mandatory Data Elements

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

Column 2 (**On card reference**): the reference number may be visibly included as text on the DL/ID to identify the data element for purposes of interpreting the data and other international interchange requirements. If no on card reference is listed in this specification, then no number shall be used.

Column 3 (**Zone placement**): indicates the location on the DL/ID where the data element must be placed. The location of the zones is provided in Appendix 6 of this specification. In some cases, data elements may appear in a choice of zones, or be repeated in another zone. Such data elements are marked with the appropriate multiple zone placements. If no zone is listed for a data element, it may be placed anywhere on the card as long as it does not interfere with the required placement of other data elements.

Column 4 (**Data element**): common name or phrase that designates what information is to be inscribed on the card. These **data elements, if used**, must be labeled using text on the card (If the jurisdiction uses French, the French translations of the data elements and their abbreviations are provided.) When abbreviations are provided in bold, they are available for use by jurisdictions. If a jurisdiction uses an abbreviation to designate a data element, the abbreviation must conform to the bold abbreviations when provided. Unless otherwise specifically stated, formatting rules of *ANSI D20 Data Dictionary for Traffic Record Information Systems* must be followed.

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

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

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

Table 1 - Mandatory Data Elements

Data Ref.	On card reference	Zone placement	Data element English / French	Definition	Card type	Field maximum length / type
a.	1	Zone II	Family Name[1] / Nom de famille	Family name (commonly called surname or last name), or primary identifier, of the individual who has been issued the driver licence or identification document. If the individual has only one name, it will be placed in this data element. Collect full name for record, print as many characters as possible on front of DL/ID.	Both	V40ANS

Data Ref.	On card reference	Zone placement	Data element English / French	Definition	Card type	Field maximum length / type
b.	2	Zone II	Given names[1] / Prénoms	Given name or names (includes all of what are commonly referred to as first and middle names), or secondary identifier, of the individual who has been issued the driver licence or identification document. If Suffix is used, the Given Names and the Suffix must be separated by a comma and a space. Collect full name for record, print as many characters as possible on front of DL/ID.	Both	V80ANS
c.	3	Zone II	Date of birth **DOB** / Date de naissance **DDN**	Year, Month, Day (If unknown, approximate DOB). Format: CCYY/MM/DD	Both	F10NS

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

d.	4a	Zone II	Date of Issue **Iss** / Date de délivrance **Dél.**	Date DL/ID was issued. Format: MM/DD/CCYY U.S., CCYY/MM/DD Canadian	Both	F10NS
e.	4b	Zone II	Date of Expiry **Exp** / Date d'expiration **Exp.**	Date DL/ID expires. Format: MM/DD/CCYY U.S, CCYY/MM/DD Canadian	Both	F10NS
f.	4d	Zone II	Customer identifier / Identificateur de client	The alphanumeric string assigned or calculated by the issuing authority	Both	V25ANS
g.	5	Zone II	Document Discriminator **DD** / Discriminateur de document **Réf**	Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.	Both	V25ANS
h.		Zone III	Portrait / Portrait	A reproduction of the licence holder's photograph. The portrait must be in colour unless laser engraving card production is used.	Both	- (Image)

Data Ref.	**On card reference**	**Zone placement**	**Data element** **English / French**	**Definition**	**Card type**	**Field maximum length / type**
i.		Zone II / III	Signature / Signature	A reproduction of the licence holder's signature. The signature may overlap the portrait image. If the signature overlaps the portrait, it may be in Zone III. Otherwise, it must be in Zone II.	Both	- (Image)

j.	8	Zone II	Cardholder address[2] / Adresse du détenteur/de la détentrice	The place where the cardholder resides and/or may be contacted (street/house number, municipality, etc.). The issuing jurisdiction may choose to use either the mailing or physical address. If P.O. Box is used on front of document, the residence address must be collected for the record.	Both	V108ANS
k.	9	Zone II / IV	Vehicle classifications/ categories / Classifications/ catégories de véhicules	Vehicle types the driver is authorized to operate. Each vehicle classification / category denoted on the DL/ID must be described in Zone IV.	DL	V4ANS
l.	9a	Zone II / IV	Endorsements **End** / Endossement **Endoss.**	Jurisdiction-specific codes denoting additional privileges granted to the cardholders, such as hazardous materials, passengers, doubles/triples trailers, motorcycles, chauffeur, emergency vehicles, and farm vehicles. Each endorsement denoted on the DL/ID must be described in Zone IV.	DL	V4ANS

Data Ref.	**On card reference**	**Zone placement**	**Data element** **English / French**	**Definition**	**Card type**	**Field maximum length / type**
m.	12	Zone II / IV	Restrictions/ conditions/ information codes / Codes d'information sur les restrictions/ conditions	Jurisdiction-specific codes used by the issuing jurisdiction to indicate restrictions or conditions that apply to the cardholder (shown as alphanumeric codes or pictographs). Other medical, administrative, or legal limitations applying to the cardholder are also to be displayed in this area. Restrictions or conditions denoted in Zone II must be described in Zone IV. If no restrictions or other conditions apply to the cardholder, "NONE" shall be indicated.	DL	V4ANS (Image)

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

n.	15	Zone II	Cardholder sex **Sex** / Sexe du détenteur/de la détentrice **Sexe**	Cardholder's sex: M for male, F for female.	Both	F1A
o.	16	Zone II	Height **Hgt** / Hauteur **Haut.**	Inches (in): number of inches followed by "in" ex. 6'1" = " 73 in" Centimeters (cm): number of centimeters followed by " cm" ex. 181 centimeters = " 181 cm"	Both	F6AN
p.	18	Zone II	Eye Colour **Eyes /** Couleur des yeux **Yeux**	Blue, brown, black, hazel, green, gray, pink, dichromatic. If the issuing jurisdiction wishes to abbreviate colours, the three character codes provided in ANSI D20 must be used.	Both	V12A
q.	-	Zone I	Issuing jurisdiction / Administration délivrante	The province, or territory responsible for the issuance of the DL/ID, and has the power to revoke or restrict the holder's driving and identification privileges. The appropriate two-character code as specified by ANSI D 20, Annex B, must be used.	Both	F2A

3.4 Optional data elements Table 2 - Optional Data Elements

Data Ref.	On card reference	Zone placement	Data Element / label	Definition	Card type	Field length / type
a.	19	Zone II	Hair Colour **hair** / Couleur des cheveux **cheveux**	Brown, black, blonde, gray, red/auburn, sandy, white. If the issuing jurisdiction wishes to abbreviate colours, the threecharacter codes provided in ANSI D20 must be used.	Both	V12A
b.	3a	Zone II	Place of birth / Lieu de naissance	Country and municipality and/or state/province/territory.	Both	V33A

c.	21	-	Inventory control number / Numéro de contrôle d'inventaire	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licences and ID cards.	Both	V25ANS
d.	10	Zone II / IV	Date of first issue per category[3] / Date de délivrance pour la première fois, par catégorie	The date of first issue for a specific class of vehicle if it is before the date of issue of the licence document (same format as DOB). If this information is not available, indicate "**unavail.**"	DL	F10ANS
e.	11	Zone II / IV	Separate expiry dates for vehicle classifications / Dates d'expiration séparées pour les catégories de véhicule	If driving privilege for certain vehicle classifications expire before the base document, the date(s) must be noted on the document as indicated in Appendix 6. Format: CCYY/MM/DD	DL	F10NS
Data Ref.	**On card reference**	**Zone placement**	**Data Element / label**	**Definition**	**Card type**	**Field length / type**

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

f.	17	Zone II	Weight **Wgt** / Poids **Poids**	Indicate the approximate weight range of the cardholder: 0 = up to 31 kg (up to 70 lbs) 1 = 32 - 45 kg (71 - 100 lbs) 2 = 46 - 59 kg (101 130 lbs) 3 = 60 - 70 kg (131 - 160 lbs) 4 = 71 - 86 kg (161 - 190 lbs) 5 = 87 - 100 kg (191 - 220 lbs) 6 = 101 - 113 kg (221 - 250 lbs) 7 = 114 - 127 kg (251 - 280 lbs) 8 = 128 - 145 kg (281 - 320 lbs) 9 = 146 + kg (321 + lbs)	Both	F1N
g.		Zone II	Name suffix[1]/ Suffixe	Name suffix of the individual who has been issued the driver licence or identification document. If Suffix is used, the Given Names and the Suffix must be separated by a comma and a space. Collect full name for record, print as many characters as possible on front of DL/ID.	Both	V5ANS
h.	20	-	Audit information / Renseignements de vérification	A string of letters and/or numbers that identifies when, where, and by whom a driver licence/ID card was made. If audit information is not used on the card or the MRT, it must be included in the driver record.	Both	V25ANS

1.4. Quality control

1.4.1 Quality Control Inspections

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

1.4.2 Quality Control Guidelines

The following guidelines will help jurisdictions establish an effective quality control program:
Basic quality control testing. Ideally, basic quality control testing should be performed on every card produced.

The purpose of this testing is to ensure that the cards conform to the design and includes all required elements (bar code, security devices, digital image, etc.) This could be as simple as a visual inspection prior to releasing the card to the cardholder. In high volume printing operations, it may be necessary to use statistical sampling or automated quality control checking.

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

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

CDLA APPENDIX 2: MACHINE READABLE DATA ELEMENTS SPECIFICATION (normative)

Mandatory PDF417 Bar Code Standard

2.1 Scope

This appendix defines mapping of the driving licence/identification (DL/ID) card machine-readable information elements onto a two dimensional bar code.

2.2 Functional requirements

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

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

2.3 Mandatory machine-readable technology - PDF417

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

2.4 Optional machine-readable technologies

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

2.5 Technical requirements for PDF417

2.5.1 Conformance

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

2.5.2 Symbology

The PDF 417 symbology (see ISO/IEC 15438 *Automatic Identification and Data Capture Techniques International Two-dimensional Symbology Specification - PDF417*) shall be used for the Drivers Licence applications.

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

- Compact PDF417
- MicroPDF417
- MacroPDF417

2.5.3 Symbology Characteristics

The symbology characteristics shall conform to ISO/IEC 15438.

2.5.4 Dimensions and Print Quality

2.5.4.1 Narrow element dimension

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

2.5.4.2 Row height

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

2.5.4.3 Quiet Zone

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

2.5.4.4 Print Quality

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

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

- Recommended Print Quality grade 3.5 (A) at the point of printing the symbol before lamination and a Print Quality Grade of 2.5 (B) after lamination.
- Measurement Aperture = .250mm (0.010 inch)
- Light Source Wavelength = 660 nanometers (nm) $\pm$ 10nm

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

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

2.5.4.5 Error Correction

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

2.6 Character sets

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

2.7 Compression

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

2.8 Sampling

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

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

2.9 Symbol Durability

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

2.10 Bar code area

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

2.11 Orientation and Placement

2.11.1 PDF417 Orientation

All PDF417 symbols and linear bar codes shall have the same orientation. The bars of the PDF417 symbol shall be perpendicular to the natural bottom of the card. (See Figure 2.1)

The symbol skew shall not be more then $\pm$ 5 degrees.

2.11.2 Designing the Card Layout

Figure 2.1 - Orientation of PDF417 Symbol on bottom

Plan for the maximum amount of data:

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

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

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

2.12 Data encoding structure

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

Each 2-dimensional bar code shall begin with a file header that will identify the bar code as complying with the standard. The header shall be followed by a subfile designator “DL” to identify the DL/ID data type stored in the file. Each data element contained in a subfile shall be prefaced by a data element identifier (Element ID) as defined in Tables 4.3 and 4.4. The use of a field separator character shall serve to both terminate a field and indicate the presence of a following field identifier.

2.12.1 Header

Compliant 2D symbols must begin with a Fixed Header in the following format (Note: The number of bytes for each field is fixed and must be present. The numbers must be zero filled.):
Table 2.1 - 2D symbols header format:

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

2	1	**Data Element Separator**: The Data Element Separator is used in this standard to indicate that a new data element is to follow, *and* that the current field is terminated. Whenever a Data Element Separator is encountered (within a Subfile type which uses Data Element Separators), the next character(s) shall either be a Segment Terminator or shall define the contents of the next field according to the template of the specific Subfile. The Data Element Separator as defined by this standard is the Line Feed character ("L_F" ASCII/ISO 646 Decimal "10") (ASCII/ISO 646 Hex "0A"). The Data Element Separator is the second character of the symbol.
3	1	**Record Separator**: The Record Separator as defined by this standard is the Record Separator character ("R_S" ASCII/ISO 646 Decimal "30") (ASCII/ISO 646 Hex "1E"). As this report is presented for ratification, there is no special case defined for when this field will be used. It is embodied within the recommendation for future growth. The Record Separator is the third character of the symbol and shall always be reflected within the header in a compliant symbol.
4	1	**Segment Terminator**: As used in this standard the Segment Terminator is used to end Subfiles where Field Identifiers are employed. The Segment Terminator as defined by this standard is the Carriage Return character ("C_R" ASCII/ISO 646 Decimal "13") (ASCII/ISO 646 Hex "0D"). The Segment Terminator is the fourth character of the symbol.
5	5	**File Type**: This is the designator that identifies the file as an AAMVA compliant format. The designator is defined as the 5 byte upper character string "ANSI", with a blank space after the fourth character.
6	6	**Issuer Identification Number (IIN)**: This number uniquely identifies the issuing jurisdiction and can be obtained by contacting the ISO Issuing Authority (AAMVA). The full 6-digit IIN should be encoded.
7	2	**AAMVA Version Number**: This is a decimal value between 00 and 99 that specifies the version level of the PDF417 bar code format. Version "0" and "00" is reserved for bar codes printed to the specification of AAMVA prior to the adoption of the AAMVA DL/ID-2000 standard. All bar codes compliant with the AAMVA DL/ID-2000 standard are designated Version "01". All barcodes compliant with AAMVA specification version 1.0, dated 9-25-2003 shall be designated Version "02". All barcodes compliant with this current AAMVA specification shall be designated Version "03". Should a need arise requiring major revision to the format, this field provides the means to accommodate additional revision.
Field	**Bytes (Fixed)**	**Contents**

8	2	**Jurisdiction Version Number**: This is a decimal value between 00 and 99 that specifies the jurisdiction version level of the PDF417 bar code format. Notwithstanding iterations of this specification, jurisdictions implement incremental changes to their bar codes, including new jurisdiction-specific data, compression algorithms for digitized images, digital signatures, or new truncation conventions used for names and addresses. Each change to the bar code format within each AAMVA version (above) must be noted, beginning with Jurisdiction Version 00.
9	2	**Number of Entries**: This is a decimal value between “01 and 99" that specifies the number of different Subfile types that are contained in the bar code. This value defines the number of individual subfile designators that follow. All sbufile designators (as defined below) follow one behind the other. The data related to the first subfile designator follows the last Subfile Designator.

2.12.2 Subfile Designator

All compliant 2D bar code symbols must contain the “DL” subfile structure as defined below immediately after the Header as defined in 4.12.1. The subfile designator is a fixed element, as well as the number of bytes, and the numbers must be zero-filled. All subfile and headers must follow one another.

Table 2.2 – Sub-file designator format

Field	Bytes	Contents
1	2	**Subfile Type**: This is the designator that identifies what type of data is contained in this portion of the file. The 2-character uppercase character field “DL” is the designator for DL/ID subfile type containing mandatory and optional data elements as defined in tables 4.3 and 4.4. Jurisdictions may define a subfile to contain jurisdiction-specific information. These subfiles are designated with the first character of “Z” and the second character is the first letter of the jurisdiction’s name. For example: “ZN” would be the designator for a New Brunswick or Nova Scotia jurisdiction-defined subfile; “ZQ” would be the designator for a Quebec jurisdictiondefined subfile.
2	4	**Offset**: These bytes contain a 4 digit numeric value that specifies the number of bytes from the head or beginning of the file where the data related to the particular sub-file is located. The first byte in the file is located at offset 0.
3	4	**Length**: These bytes contain a 4 digit numeric value that specifies the length of the Subfile in bytes. The segment terminator must be included in calculating the length of the subfile. A segment terminator = 1. Each subfile must begin with the twocharacter Subfile Type and these two characters must also be included in the length.

2.12.3 Data Elements

Tables 4.3 and 4.4 define mandatory and optional data elements that are accommodated in the “DL” subfile type. Jurisdiction-specific data elements may also be encoded, provided the bar code ID is a 3character uppercase character field beginning with “Z*X*” where “*X*” is the first letter of the jurisdiction. Each data element field within the jurisdiction-defined subfile should follow consecutively in alphabetic order. For example, data elements in a Alberta subfile would be ZA*A*, ZA*B*, etc.; a Ontario subfile would be ZO*A*, ZO*B*, etc.).

Mandatory data elements for which no data exits for a given cardholder are to be encoded with the word “NONE”. In the event data is *not available* for a mandatory data element, “unavail” is to be encoded.

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

2.12.3.1 Minimum mandatory elements

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

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

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

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

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

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

Data Ref.	Element ID	Data Element	Definition	Card type	Length / type
a.	DCA	Jurisdiction specific vehicle class	Jurisdiction-specific vehicle class / group code, designating the type of vehicle the cardholder has privilege to drive.	DL	V4ANS
b.	DCB	Jurisdiction specific restriction codes	Jurisdiction-specific codes that represent restrictions to driving privileges (such as airbrakes, automatic transmission, daylight only, etc.)	DL	V10ANS

c.	DCD	Jurisdiction specific endorsement codes	Jurisdiction-specific codes that represent additional privileges granted to the cardholder beyond the vehicle class (such as transportation of passengers, hazardous materials, operation of motorcycles, etc.)	DL	V5ANS

Data Ref.	Element ID	Data Element	Definition	Card type	Length / type
d.	DBA	Document Expiration Date	Date on which the driving and identification privileges granted by the document are no longer valid. (CCYYMMDD).	Both	F8N
e.	DCS	Customer Family Name	Family name of the cardholder. (Family name is sometimes also called “last name” or “surname”.) Collect full name for record, print as many characters as possible on front of DL/ID.	Both	V40ANS
f.	DCT	Customer Given Names	Given names of the cardholder. (Given names include all names other than the Family Name. This includes all those names sometimes also called “first” and “middle” names.) Collect full name for record, print as many characters as possible on front of DL/ID.	Both	V80ANS
g.	DBD	Document Issue Date	Date on which the document was first issued. (CCYYMMDD)	Both	F8N
h.	DBB	Date of Birth	Date on which the cardholder was born. (CCYYMMDD)	Both	F8N
i.	DBC	Physical Description - Sex	Gender of the cardholder. 1 = male, 2 = female.	Both	F1N
j.	DAY	Physical Description - Eye Colour	Colour of cardholder’s eyes. (ANSI D-20 codes)	Both	F3A
k.	DAU	Physical Description Height	Height of cardholder. Inches (in): number of inches followed by “in” ex. 6'1" = “ 73 in” Centimeters (cm): number of centimeters followed by “ cm” ex. 181 centimeters = “ 181 cm”	Both	F6AN

l.	DAG	Address - Street 1	Street portion of the cardholder address.	Both	V35ANS
m.	DAI	Address - City	City portion of the cardholder address.	Both	V20ANS
n.	DAJ	Address - Jurisdiction Code	Province/territory portion of the cardholder address.	Both	F2A
o.	DAK	Address - Postal Code	Postal code portion of the cardholder address Canada.	Both	F11AN
p.	DAQ	Customer ID Number	The number assigned or calculated by the issuing authority.	Both	V25ANS
Data Ref.	**Element ID**	**Data Element**	**Definition**	**Card type**	**Length / type**
q.	DCF	Document Discriminator	Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.	Both	V25ANS
r.	DCG	Country Identification	Country in which DL/ID is issued. Canada = CAN.	Both	F3A
s.	DCH	Federal Commercial Vehicle Codes	Federally established codes for vehicle categories, endorsements, and restrictions that are generally applicable to commercial motor vehicles. If the vehicle is not a commercial vehicle, “NONE” is to be entered.	DL	F4AN

2.12.3.2 Optional Data Elements

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

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

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

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

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

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

Data Ref	Element ID	Data Element	Definition	Card type	Length / type
a.	DAH	Address - Street 2	Second line of street portion of the cardholder address.	Both	V35ANS
b.	DAZ	Hair colour	Brown, black, blonde, gray, red/auburn, sandy, white	Both	V12A
c.	DCI	Place of birth	Country and municipality and/or state/province/territory	Both	V33A

length, V=variable length) in the related application. Use of padding for variable length fields is optional.

Data Ref	Element ID	Data Element	Definition	Card type	Length / type
d.	DCJ	Audit information	A string of letter and/or numbers that identifies when, where, and by whom a driver licence/ID card was made. If audit information is not used on the card or the MRT, it must be included in the driver record.	Both	V25ANS
e.	DCK	Inventory control number	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licences and ID cards.	Both	V25ANS
f.	DBN	Alias / AKA Family Name	Other family name by which cardholder is known.	Both	V10ANS
g.	DBG	Alias / AKA Given Name	Other given name by which cardholder is known.	Both	V15ANS
h.	DBS	Alias / AKA Suffix Name	Other suffix by which cardholder is known.	Both	V5ANS
i.	DCU	Name Suffix	Name Suffix (If jurisdiction participates in systems requiring name suffix (PDPS, CDLIS, etc.), the suffix must be collected and displayed on the DL/ID and in the MRT). Collect full name for record, print as many characters as possible on front of DL/ID.	Both	V5ANS
j.	DCE	Physical Description Weight Range	Indicate the approximate weight range of the cardholder: = up to 31 kg (up to 70 lbs) = 32 - 45 kg (71 - 100 lbs) = 46 - 59 kg (101 - 130 lbs) = 60 - 70 kg (131 - 160 lbs) = 71 - 86 kg (161 - 190 lbs) = 87 - 100 kg (191 - 220 lbs) = 101 - 113 kg (221 - 250 lbs) = 114 - 127 kg (251 - 280 lbs) = 128 - 145 kg (281 - 320 lbs) = 146 + kg (321 + lbs)	Both	F1N
k.	DCL	Race / ethnicity	Codes for race or ethnicity of the cardholder, as defined in ANSI D20.	Both	F2N

l.	DCM	Standard vehicle classification	Standard vehicle classification code(s) for cardholder. This data element is a placeholder for future efforts to standardize vehicle classifications.	DL	F4AN
m.	DCN	Standard endorsement code	Standard endorsement code(s) for cardholder. This data element is a placeholder for future efforts to standardize endorsement codes.	DL	F5AN

Data Ref	Element ID	Data Element	Definition	Card type	Length / type
n.	DCO	Standard restriction code	Standard restriction code(s) for cardholder. This data element is a placeholder for future efforts to standardize restriction codes.	DL	F12AN
o.	DCP	Jurisdiction specific vehicle classification description	Text that explains the jurisdiction-specific code(s) for types of vehicles cardholder is authorized to drive.	DL	V50ANS
p.	DCQ	Jurisdiction specific endorsement code description	Text that explains the jurisdiction-specific code(s) that indicates additional driving privileges granted to the cardholder beyond the vehicle class.	DL	V50ANS
q.	DCR	Jurisdiction specific restriction code description	Text describing the jurisdiction-specific restriction code(s) that curtail driving privileges.	DL	V50ANS

2.12.3.3 Additional data elements

Jurisdictions wishing to encode data elements in their PDF417 bar codes other than those described in the above lists of mandatory and optional data elements should coordinate with CCMTA on the format and Data Element ID to use for that data. This will prevent the introduction of conflicts and variances across the jurisdictions.

CDLA APPENDIX 3: DRIVER LICENCE SECURITY DEVICES SPECIFICATION (normative)

Physical Security

3.1 Scope

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

3.2 Introduction

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

This appendix draws heavily upon ISO IEC CD 18013-1, Appendix 5. This approach recognizes that a feature or technique that may be necessary to protect one Issuer's cards may be superfluous or of minor importance to another Issuer using different production systems and vice versa. A targeted approach that allows issuing authorities flexibility to choose from different card technologies (pure plastic cards or combined structures incorporating other materials in the core of the card-body) and a combination of security features and/or techniques most appropriate to their particular needs is therefore preferred to a "one size fits all" philosophy. However, to help ensure that a balanced set of security features and/or techniques is chosen, it is first necessary for each issuing authority to conduct a risk assessment and select optional features and/or techniques that are appropriate to the particular issuing environment and to meeting any specific security concerns. All this must serve the objective of facilitating the task of card verification as much as possible under all practical circumstances.

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

3.3 Definitions

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

Biographical data (biodata): The personalized details of the holder of the card.
Card core: The opaque or translucent inner layers of a laminated card upon which the security design is usually printed.

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

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

CMYK colours: The “process” colours, cyan, magenta, yellow and black used in combination in commercial colour printing, normally in the form of half-tone images, and by digital printing devices to approximately represent the visible colour spectrum and enable the printing of ‘colour pictures’.

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

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

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

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

- *Level 1*: synonymous with "first line inspection"
- *Level 2*: synonymous with "second line inspection"
- *Level 3*: synonymous with "third line inspection"

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

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

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

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

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

Security feature: A feature of a document that is linked to a specific method of verification and thus helps insure the document's integrity and/or authenticity as a properly issued document that has not been tampered with. Security features may be distinguished in different kinds of categories such as:

- for human or machine verification,
- for first line, second line, or third line inspection,
- substance features, structure features, or data features according to ICAO doc. 9303.

Security elements applied during production of a document may contribute more than one feature and therefore also cover more than one category of each kind.

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

3.4 Basic Principles

3.4.1 Card Production

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

3.4.2 Accountability and auditing

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

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

3.4.3 Graphics design

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

3.4.4 Security overtime

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

3.4.5 Covert features

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

3.4.6 Common security element

All compliant DL/ID documents must include the common security element prescribed by CCMTA in Zone 4 of the card (see Appendix 4, paragraph 6.5). Although the common security element contains advanced security features, it should not be considered as helping fulfill the requirements of this appendix. The common security element, while being highly resistant to counterfeit, will be the primary focus of fraudsters. Its primary goal is to establish an easily recognizable common security element, similar to the concept introduced for major credit cards, to aid in the recognition of DL/ID documents. Additional security features are needed to fully protect the card from counterfeit and alteration.

3.5 Risk Assessment

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

3.6 General Requirements

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

- Do not conflict with each other and should be planned for maximum effectiveness.
- Do not interfere with the operation of machine-readable technology(ies) on the document.
- Are layered in order to benefit from the combined protection of multiple features and leverage the card production process.

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

3.7 Use of the *DL/ID Security Device Index*

Appendix 5 contains the *DL/ID Security Device Index*. This index is to be used as a guideline for security feature selection. The index is an inclusive list of security devices that includes a general description of the device and a guideline for determining what threats each device protects against at levels 1 and 2. The *DL/ID Security Device Index* will assist issuing jurisdictions to make educated decisions about the security design of their DL/ID document system.

The properties of the security devices identified in Appendix 5 should be considered generally and as a beginning of discussion. Security device vendors may offer new approaches to established security devices that provide protection above and beyond those listed in Appendix 5. Security devices may be combined and implemented in a manner that offers protection against more threats than when the devices are considered individually. The *DL/ID Security Device Index* indicates coverage against various threat types at different levels of inspection (level 1 and level 2). The levels of inspection and threat types are as follows:

3.7.1.1 Level 1: first line inspection

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

3.7.1.2 Level 2: second line inspection

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

3.7.1.3 Type 1: Counterfeit / simulation

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

3.7.1.4 Type 2: Alteration

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

3.7.1.5 Type 3: Photo / signature substitution

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

3.7.1.6 Type 4: Counterfeit from cannibalized cards

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

3.7.2 Minimum requirements

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

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

CDLA APPENDIX 4: CARD DESIGN SPECIFICATION

(Normative)

4.1 Introduction

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

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

4.2 Scope

Appendix 6 defines the specifications of the card layout, together with informative examples for ease of understanding.

4.3 Dimensions and character set

The dimensions of the DL/ID shall be in conformance with ISO/IEC7810 ID-1.
All mandatory human readable data elements shall be printed in ANS characters, i.e. the extended Latin character set, including characters such as ß, ä, ã, ç, è, é, ö, and ü.

4.4 Functions

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

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

4.5 Common recognition

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

- The common security element, as prescribed by CCMTA, shall be included in Zone IV of the card. The common security element shall only go on driver licences and non-driver identification cards issued by the department [of motor vehicles]. Non-driver identification card defined as: “A card issued to a person whose identity is verified in the same manner as required for the issuance of a driver licence by a licensing authority for identification purposes only”. This definition does not include any other identification provided by the department [of motor vehicles], such as provincial/territorial employee identification, senior citizen cards, etc.

- Distinctly different colours should be used for the background Zone I of the driver licence and non-driver identification cards. The Zone I background colour should be predominantly a high security colour chosen to make copying or duplication of the document difficult. The background

of Zone I may utilize any type of design. The use of the following colours for background of Zone I is recommended, but not required:

- For driver licence documents, it is recommended that the background colour of Zone I be predominantly a 30% tint of Pantone reference 198 as specified in ISO/IEC CD18013-1 for ISO Compliant Driver Licences.

- For non-driver identification cards, it is recommended that the background colour be predominantly a 30% tint of Pantone reference 368.

- The reproduction of the portrait of the holder of the licence is depicted on the left side on the portrait side of the card as shown by the position of Zone III in figure 4.2 and 4.3.

4.6 Layout

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

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

Portrait side

- Data Element Set of text, digitally printed reproduction of portrait and signature.
- Zones I, II and III.

Non-portrait side

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

4.7 Contents of the zones

4.7.1 General

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

4.7.2 Zone I

4.7.2.1 Document type indicator

For driver licences, the words “DRIVING LICENSE/LICENCE (ISO-compatible)” or “DRIVER LICENSE/LICENCE” (not ISO-compatible) in English must be included as text or, alternatively, the words “DRIVING LICENSE” or “DRIVER LICENSE” may be incorporated in the background graphic design of Zone I. The words may also be in French (“PERMIS de CONDUIRE”). NOTE: The term “driving licence” is used for compatibility with the ISO draft standard. If a version is to be used other than “licence” or

"licence", the jurisdiction must apply for an exception. You may also use a bilingual version of both French and the ISO compliant English. Other types of driving licences may be indicated in the same manner, such as commercial driving licences and instruction/learning permits.

For non-driving identification cards, the words "IDENTIFICATION CARD" must be included as text or, alternatively, the words "IDENTIFICATION CARD" may be incorporated in the background graphic design of Zone I. The words may also be in French ("CARTE D'IDENTITÉ").

4.7.2.2 Issuing jurisdiction information

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

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

- Canadian jurisdictions shall use: CAN

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

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

4.7.3 Zone II

Zone II contains the following data elements:

- Family name (or concatenated Name)
- Given name(s) (or concatenated Name)
- Suffix (optional)
- Date of birth
- Date of issue
- Date of expiry
- Customer number
- Document discriminator
- Signature (unless in Zone III)
- Cardholder/Organization address
- Vehicle classifications (if codes are used, they should be explained in Zone IV; overflow information may be placed in Zone IV) (optional)
- Vehicle restrictions and endorsements (if codes are used, they should be explained in Zone IV; overflow information may be placed in Zone IV) (optional)
- Cardholder sex
- Cardholder height (optional)
- Cardholder weight (optional)
- Cardholder eye colour (optional)
- Audit information (optional)
- Issuing jurisdiction
- Cardholder signature (may be in Zone III instead)
- Cardholder hair colour (optional)
- Cardholder place of birth (optional)
- Date of expiry per vehicle classification / category (optional - may be in Zone IV instead) (optional)

- Date of issue per vehicle classification / category (optional - may be in Zone IV instead) (optional)
- Date of first issue per vehicle classification / category (optional - may be in Zone IV instead) Other data fields for national or jurisdictional purposes in human readable format (optional). (optional)

4.7.4 Zone III

Zone III contains the following:

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

4.7.5 Zone IV

Zone IV contains the following:

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

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

4.7.6 Zone V

The PDF417 2-dimensional bar code must be included in Zone V. Other optional machine-readable technologies may co-exist with the PDF417 2-dimensional bar code in Zone V. This specification contains requirements for PDF417 2-dimensional bar codes, 3-track magnetic stripes, and optional memory cards. No other machine-readable technologies, including IC chips, are supported in this specification. Issuing jurisdictions wishing to implement non-proprietary technologies, such as integrated circuit cards (also known as “smart cards”), are asked to work with CCMTA prior to implementation, so that future iterations of this specification will properly include these technologies to ensure future interoperability with other jurisdictions.

The positions of the zones for the optional jurisdiction-specific human readable fields and optional machine-readable technologies are presented in figures 4.4 and 4.5 of the appendix. The position and size of Zones IV and V may be adjusted in accordance with the machine-readable technologies incorporated on the card.

4.7.7 Reproduction of images

4.7.7.1 Portrait

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

Pose. The portrait shall depict the face of the rightful holder of the card in a full-face frontal pose with both eyes visible; i.e. captured perpendicular to an imaginary plane formed parallel to the front surface of the face. The portrait may only show the holder with headgear, if the holder is a member of a religion requiring the wearing thereof and provided that the headgear does not render the portrait inadequate for

the identification of the holder. Jurisdictions that incorporate facial recognition biometric technology may wish to ensure eyeglasses are removed as well, to aid in consistent identification of the cardholder.

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

Orientation*.* The crown (top of the hair) shall be nearest the top edge of Zone III as defined in figure 4.2 and 4.3; i.e. the crown to chin orientation covering the longest dimension defined for Zone III.

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

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

Background*.* A uniform light blue colour or white background shall be used to provide a contrast to the face and hair. Preference is for uniform light blue colour, Pantone 277 (though the Pantone colour is not a requirement).

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

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

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

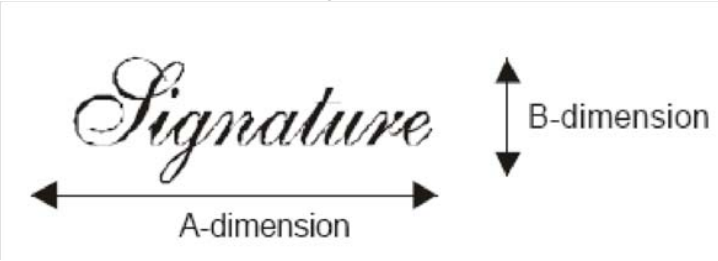
Printing resolution*.* The digitally printed reproduction shall yield an accurate recognizable representation of the rightful holder of the licence. The quality of a digitally reproduced portrait shall be visually comparable to an acceptable photograph. To achieve this comparable quality in a digital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

4.7.7.2 Signature

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

Orientation*.* The digitally printed reproduction of the signature shall be displayed in either Zone II or Zone III with its A-dimension parallel to the Top Reference Edge of the horizontal format cards identified in figure 4.2. In the case of vertical format cards, the A-dimension will be perpendicular to the Top Reference Edge. (See figure 4.2.1 for an example of the horizontal format and figure 4.3.1 for an example of the vertical format.).

Figure 4.1



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

Scaling. In the event the signature displayed is scaled-up or scaled-down, the aspect ratio (A-dimension to B-dimension) of the original signature shall be maintained. In the case of a scaled-down image, the image shall not be reduced to a size where it is no longer a discernible representation of the original. The resulting signature must be a smooth representation of the original signature without such distortions such as stair stepping, stretching and/or squishing being apparent to the human eye.

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

Colour. The digital reproduction of the signature shall be printed in definite contrast to the background colour of the licence. Either a light signature on a dark background or a dark signature on a light background. The ink of the signature must be printed entirely in the same shade of colour, not varying shades (i.e. grey scale printing).

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

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

4.8 Security

Aspects such as a specific background pattern, rainbow printing, holograms and special inks relate to the minimum security requirements of the card and should not be confused with common recognition of the DL/ID. The security requirements are addressed in Appendix 3.

Figure 4.2: Portrait side of Horizontal DL/ID (not to scale)

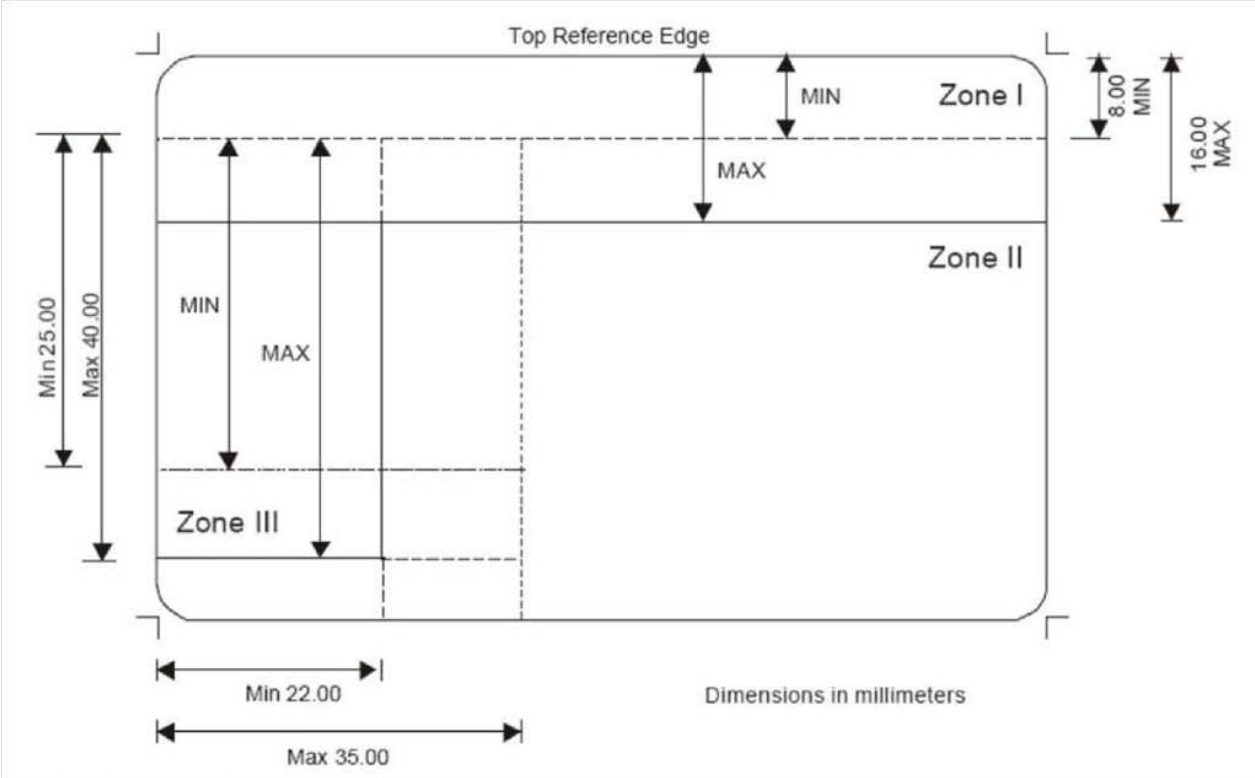
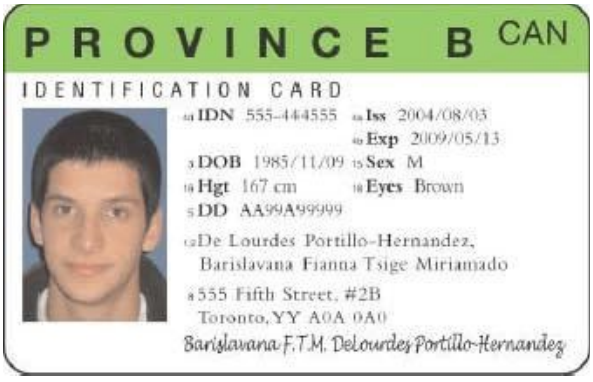
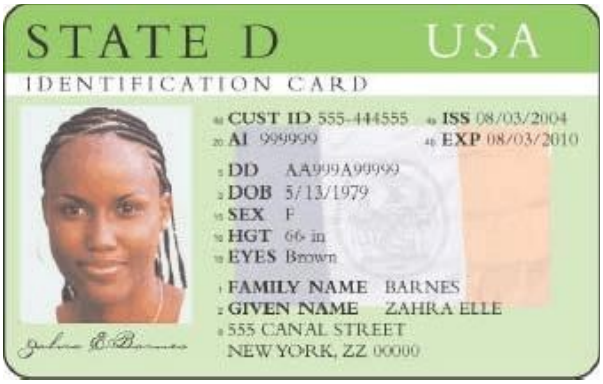


Figure 4.2.1: Horizontal DL/ID - Informative examples (not to scale) - intended to show what could be done within this specification.





**NOTE: The background colours in Zone I of the sample cards (which are specified as Pantone reference 198 and 368) may not appear as the true shade due to variations between individual monitors and printers on which they are viewed or printed. It is for this reason the Pantone reference numbers are used to specify the colours to be used on the actual cards.

Figure 4.3: Portrait side of Vertical DL/ID (not to scale)

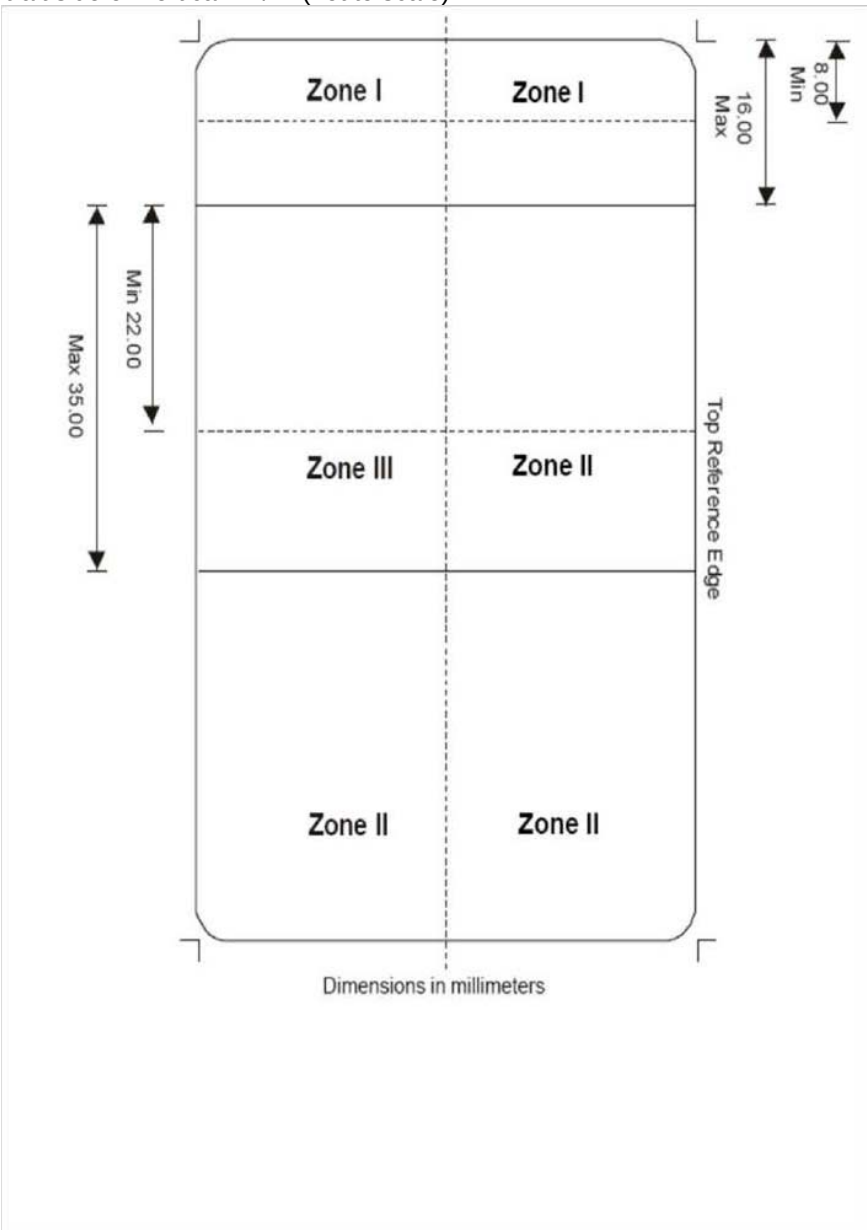


Figure 4.3.1: Vertical DL/ID - Informative examples (not to scale) - intended to show what could be done within this specification

**NOTE: The background colours in Zone I of the sample cards (which are specified as Pantone reference 198 and 368) may not appear as the true shade due to variations between individual monitors and printers on which they are viewed or printed. It is for this reason the Pantone reference numbers are used to specify the colours to be used on the actual cards.

Figure 4.4: Non-portrait side of Horizontal and Vertical DL/ID

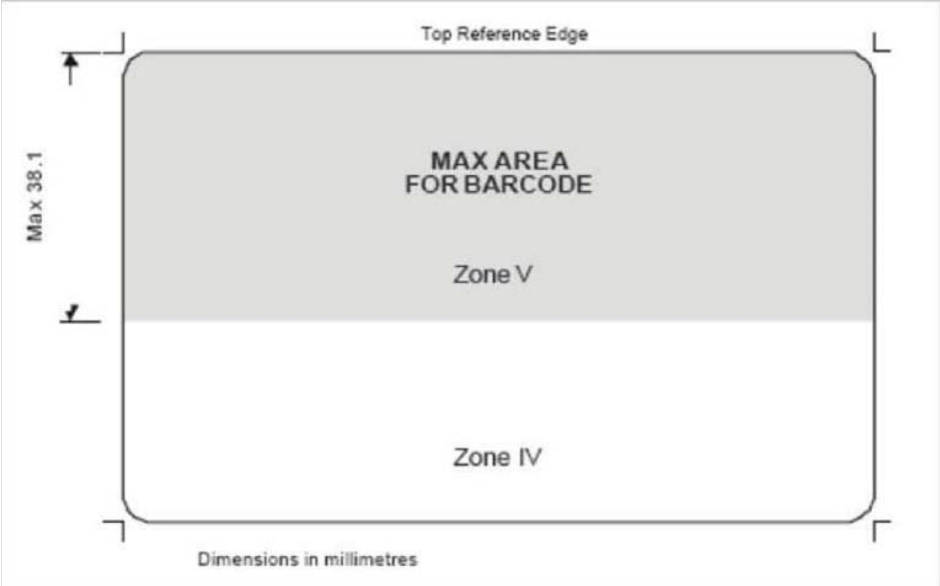
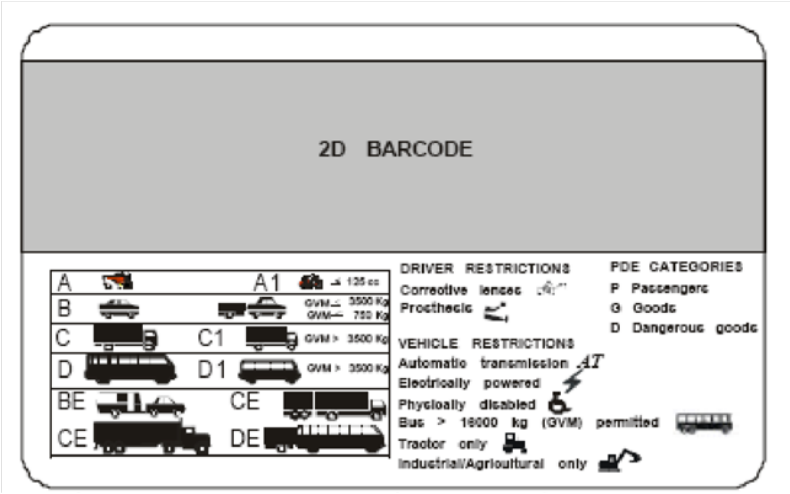
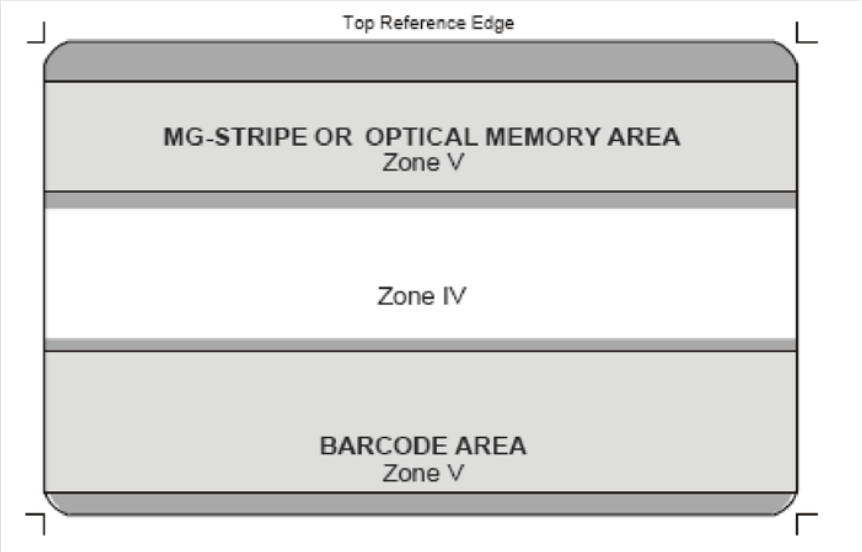


Figure 6.4.1: Informative Example



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

Figure 4.5: Non-portrait side of Horizontal and Vertical DL/ID - magnetic stripe and bar code



CDLA APPENDIX 5: DL/ID SECURITY DEVICE INDEX SPECIFICATION (informative)

5.1 Introduction

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

5.2 Threat Levels

Level 1 - A Level 1 security device supports first line inspection.
Level 2 - A Level 2 security device supports second line inspection.

5.3 Threat Types

Type 1 - Counterfeit/Simulation
Type 2 - Alteration
Type 3 - Photo Substitution
Type 4 - Cannibalization
(*Refer to Appendix 3, section 3.7 for definitions of these terms)*

5.4 Printing

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
a. Deliberate Errors/known flaws A feature is purposely made with an intentional mistake known only to the manufacturer or inspection officials.						X			
b. Duplex Patterns A design made up of an interlocking pattern of small irregular shapes, printed in two colours and requiring very close register printing in order to preserve the integrity of the image.		X	X		X	X	X		
c. Fine line background (Guilloche pattern) A pattern of continuously fine lines constructed by using two or more lines in overlapping bands that repeat a lacy, web-like curve.		X	X	X	X	X	X	X	X

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
d. Fine line foreground A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve.		X	X	X	X	X	X	X	X
e. Front to back (see through) register A design printed on both sides of a card that forms an interlocking image when held to a light source.		X							
f. Ghost Image Half tone reproduction of the original image that is typically printed in the same area as, and behind, personal data.			X	X	X	X			X
g. Layered printing (on lamination) Printing separate elements of the secure design on different layers of the laminated card body materials so that no single layer contains all of the security features and the entire products is only apparent after lamination.		X	X		X				
h. Micro optical imaging Text, line art, gray scale images and multi - reflectivity images are engineered into optical WORM media at high resolution (over 12,000 dpi). Difficult to simulate the printing resolution.		X	X			X	X	X	
i. Microprinting / nanoprinting Miniature lettering which is discernible under magnification. Incorporated into fine line backgrounds or placed to appear as bold lines. Continues to decrease in size as technology improves. Difficult to duplicate.						X			X

j. Moiré pattern (anti-scan/VOID pattern) A new pattern formed by the super positioning of two patterns whose periodicities are not identical. Security designs can be developed so that a scanner or copier will only display part of the pattern and/or word VOID or COPY appears instead of the pattern.						X	X	X	X
PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
k. Non standard type fonts Special type that is not available on the commercial market and is reserved for security card use only.		X	X			X	X		
l. Rainbow printing Must demonstrate a controlled exacting colour shift subtly in a linear continuous fashion. Accurately designed patterns cannot be easily copied or duplicated via scanning. It is applied using non-commercial method of printing. It is often used with a fine line or medallion pattern in the background of a card.		X							
m. Security code High-resolution colour printing systems print a security code within the body of the colour printed photo image. The code can be printed in a non-proportional font that can embed characters on the edge or bottom of the printed picture.						X		X	

5.5 Inks

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4

a. Chemically Reactive Contains a security agent that is sensitive to chemicals, i.e., polar and non-polar solvents and bleach, commonly used to alter documents. The chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.			X				X		
b. Infrared fluorescent Forms a visible image when illuminated with light in the infrared / red visible part of the spectrum.						X	X		
c. Infrared drop-out Forms a visible image when illuminated with light in the visible part of the spectrum, but cannot be detected in the infrared region.						X	X		
PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
d. Metallic, pearlescent, and iridescent Inks that fluctuate in brilliance depending on the angle of illumination of the viewing. Difficult to mimic the luster and hard to copy or scan.		X	X	X					
e. Metameric The use of a pair of ink colours that differ in spectral composition but match one another under certain lighting conditions. Under incandescent light that may appear the same, but under coloured light they appear as different colours.						X			
f. Phosphorescent Contains a pigment that glows when exposed to a light source of appropriate wavelength. The reactive glow decays after the light source is removed.						X	X		

g. Tagged Contains taggants or compounds that are not naturally occurring and that can be detected using special equipment that reacts to electromagnetic energy identifying the grouping or type.					X			
h. Thermochromatic Ink that exhibits a sharp, reversible colour change when exposed to heat, i.e. finger rubbing or hot air.	X				X	X		
i. Ultraviolet fluorescence Invisible inks that emit visible colour under exposure to ultraviolet light. Colours can be formulated that are not commercially available, making resistance to counterfeiting higher.					X	X	X	X

5.6 Substrate Inclusion

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
a. Core inclusion The manufacture of card stock with different layers. A coloured core material may be placed inside to create a coloured edge along the card.		X							
b. Embedded thread, fiber or planchette Small, often fluorescent particles or platelets incorporated into a card material at the time of manufacture that can be seen later under certain lighting conditions. The embedded elements may have magnetic or other machine-readable properties that may be used to enhance the levels of security provided.						X	X		
c. Opacity mark Similar to a watermark, it is a plastic that contains a unique translucent mark.		X							

d. Security bonding The card periphery incorporates a security bonding material that bonds all of the layers together. Tamper evidence is seen if access is attempted to obtain the internal structures of the card.					X	X		X
e. Ultraviolet features Card bodies are made UV dull or possess a controlled response to UV light so they exhibit fluorescence that can be distinguished in colour from the “blue” used in commonly available fluorescent materials.					X	X		

5.7 Optically Variable Devices (OVD)

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
a.1 Metalized DOVID (Diffractive Image) Opaque metalized DOVID (diffractive optically variable image device). OVD authentication effects cannot be photocopied or digitally recreated. OVDs are holographically mastered or digitally mastered using computer-guided lasers or electron beams.		X	X	X					

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4
a.1.1 De-Metalized OVD (Diffractive Image) A combination of metal and transparency on the same foil or laminate. High resolution OVD has selective demetallization, either transparent or opaque, as defined above.		X	X	X					

a.2 Transparent DOVID Transparent DOVID (diffractive optically variable image device). When incorporated into a driver licence design, feature will not interfere with photo or data information. Transparent OVD authentication effects cannot be photocopied or digitally recreated. OVDs are holographically mastered or digitally mastered using computer-guided lasers or electron beams.	X	X	X					
b. Film - Colour Shifting OVD Semi-transparent, multilayer light interference film creates noticeable, reflecting colour shifts, i.e. clear to blue, magenta to blue, yellow to orange, etc. When incorporated into a driver licence design, feature will minimally interfere with photo or data information. OVD colour shifting effect cannot be photocopied or digitally recreated.	X	X	X					
c. Ink - Colour Shifting OVD Printed opaque, multilayer light interference ink pigment creates noticeable, reflecting colour shifts, i.e., gold to green, green to blue, etc. similar to what is seen on many global identification documents including driver licences, banknotes, passports, and visas. The colour shifting and authentication effect cannot be replicated or digitally recreated. Tightly controlled and only available for the most secure document applications.	X	X						
d. Liquid Crystal - Colour Shifting OVD Semi-transparent, liquid crystal light interference layers create noticeable, reflecting colour shifts, i.e., orange to green. When incorporated into a driver licence design, feature will minimally interfere with photo or data information. OVD colour shifting effect cannot be photocopied or digitally recreated.	X	X	X					

PHYSICAL SECURITY FEATURE		LEVEL 1				LEVEL 2			
	Threat Type	1	2	3	4	1	2	3	4

e. Personalized OVD OVD that is personalized for each card based upon biographical data, portrait, or signature of the cardholder.	X	X	X	X	X	X	X	X
f. Virtual Image OVD Transparent or semi-transparent virtual image appears to float above or sink below the surface of the document, as the viewing angle changes. When incorporated into a driver licence design, feature will not interfere with photo or data information. OVD virtual image effect cannot be photocopied or digitally recreated.	X	X	X					

5.8 Additional Features

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
a. Biometric feature (template) A biometric template of the customer's physical characteristics.					X	X	X	X
b. Covert Device - Readable and Storage Technology Unique individual Near IR or IR invisible data mark, 2dimensional encrypted bar code, capable of storing independent information or details.					X	X	X	X
c. Covert variable pixel manipulation Covert dot matrix images that are converted to visible text with a special reader or lens.					X	X	X	X
d. Digital Seal A method of securing and validating data by electronic means using digital signature technology. The issuing authority "signs" the information contained in the MRT.					X	X		X
e. Embedded Image An image or information that is embedded or encoded within a primary visual image.					X	X	X	X
f. Laminates (security) Transparent layers or films with an integrated security feature(s) are applied to the card with an adhesive or fused by heat. Available in a number of forms, security laminates are designed to be tamper evident and carry other security features to the card.	X	X	X	X				
g. Laser encoded optical image Image and text files are placed to an optical WORM media as a visible diffraction pattern image that is eye-readable under a variety of lighting conditions.	X	X	X					

h. Laser engraving The information cannot be mechanically or chemically removed without surface damage to the card. Can be used for photos, characters, bar codes, OCR, etc.	X	X	X			X		

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
i. Laser perforation Holes are made with the laser beam of images or objects. The image is visible when held up to the light source. It has a tactile feel with conical holes that are larger at the entrance than exit.	X	X	X	X				
j. Machine readable technology (MRT) Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc. Verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other information.					X	X	X	X
k. Magnetic media fingerprinting Tracks unique, random patterns of magnetic media formed as a by-product manufacture of card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.					X	X		X
l. Optical media fingerprinting Tracks unique, random patterns of optic media (e.g., fibers) on card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.					X	X	X	X

m. Optical watermark Fine line images that are engineered into optical WORM media with a very high resolution (12,000 dpi). The watermark is overwritten with a laser-encoded optical image, locking together a preformatted document security feature with a laser encoded personalization security feature.	X	X			X	X		X
n. Overlay An ultra-thin film or protective coating that may be applied to the surfaced of a card in place of a security laminate and which may contain optically variable features.	X	X	X	X				

PHYSICAL SECURITY FEATURE	LEVEL 1				LEVEL 2			
Threat Type	1	2	3	4	1	2	3	4
o. Overlapping data Variable data, such as digitized signature, seals or text can be placed over another field such as a photo image. Both fields must be altered if a substitution is to take place making it more difficult.		X	X	X	X	X	X	X
p. Redundant data Display of data in more than one location on the card. A visual inspection may determine if all of the fields match. Usually, the data is displayed in a variety of colours and fonts to further deter alteration.		X						
q. Retroreflective device Optical constructions that reflect light such that covert logos become visible over the entire document when viewed using a focused light source or retroreflective viewer. Level 1 capability is based on a distinctive tactile quality.	X	X	X	X	X	X	X	X

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

CDLA APPENDIX 6: CARD DURABILITY TEST METHODS SPECIFICATION (normative)

Introduction (informative)

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

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

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

6.1 Scope

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

6.2 Conformance

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

6.3 Normative references

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

- ANSI NCITS 322, *For information technology-Card durability test methods: 1998*
- ISO 10373-1, *Identification cards - Test methods - General characteristics tests*

6.4 Terms and definitions

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

6.4.1 card service life

Period of time between card issuance and expiration date .

6.5 Test methods and sample size

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

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

ANSI NCITS 322 recommended sample size (informative)

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

		axis A, face down	4
		axis B, face up	4
		axis B, face down	4
5.7	Impact Resistance	NA	25
Clause	Test description	Card orientation NA = not applicable	Typical sample size # cards
5.8	Elevated Temperature & Humidity Exposure	NA	6
5.9	Surface Abrasion	NA	6
5.10	Bar Code Abrasion	NA	6
5.11	Magnetic Stripe Abrasion	NA	6
5.12	Image Abrasion	NA	6
5.13	Temperature & Humidity Induces Dye Migration	NA	6
5.14	Plasticizer Induced Dye Migration	NA	6 sets of 5
5.15	Ultraviolet (UV) Light Exposure Stability	test both sides of card	6
5.16	Daylight Exposure Image Stability - Xenon Arc	test both sides of card	6
5.17	Laundry Test	NA	6
5.18	Embossed Character Retention - Pressure	NA	6
2.19	Embossed Character Retention - Heat	NA	6
5.20	Corner Impact Test	NA	6
5.21	Wet Abrasion & Impact	NA	6-16

5.22	IC Card with Contacts Micromodule Adhesion	NA	6
5.9	Dynamic torsional stress (torsion)	NA	6
6.1	Card Structure Integrity Test Sequence	NA	6-16

6.6 Test report

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

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

ANNEX "A"

SECURITY REQUIREMENT CHECK LIST (SRCL)

RECEIVED
FEB 2 8 2018

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-18-RFI1
Security Classification / Classification de sécurité
Protected A

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Canadian Armed Forces
2. Branch or Directorate / Direction générale ou Direction: Director General Defence Security (DGDS)

3. a) Subcontract Number / Numéro du contrat de sous-traitance:
3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant:

4. Brief Description of Work / Brève description du travail:
DGDS requires to improve the efficiency of identification management related activities so is seeking solutions that could automate the management of identification across the enterprise and produce identification.

5. a) Will the supplier require access to Controlled Goods? / Le fournisseur aura-t-il accès à des marchandises contrôlées? — No / Non: ✓ — Yes / Oui:

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? / Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? — No / Non: ✓ — Yes / Oui:

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? / Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) / (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) — No / Non: — Yes / Oui: ✓

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. / Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. — No / Non: ✓ — Yes / Oui:

6. c) Is this a commercial courier or delivery requirement with no overnight storage? / S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? — No / Non: ✓ — Yes / Oui:

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ✓	NATO / OTAN	Foreign / Étranger
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ✓ Not releasable / À ne pas diffuser Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :	All NATO countries / Tous les pays de l'OTAN Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :	No release restrictions / Aucune restriction relative à la diffusion Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	PROTECTED A / PROTÉGÉ A
PROTECTED B / PROTÉGÉ B	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	PROTECTED B / PROTÉGÉ B
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET
TOP SECRET / TRÈS SECRET		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
Protected A

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-18-RFI1

Security Classification / Classification de sécurité
Protected A

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No / Non ✓ — Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No / Non ✓ — Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

✓	RELIABILITY STATUS COTE DE FIABILITÉ	CONFIDENTIAL CONFIDENTIEL	SECRET SECRET	TOP SECRET TRÈS SECRET
	TOP SECRET– SIGINT TRÈS SECRET – SIGINT	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET
	SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No / Non — Yes / Oui ✓
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? ON GROUND PREMISES MAY
If Yes, will unscreened personnel be escorted? UNSCREENED PERSONNEL — No / Non — Yes / Oui ✓
Dans l'affirmative, le personnel en question sera-t-il escorté? ONLY ACCESS PUBLIC/RECEPTION ZONES

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No / Non ✓ — Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No / Non ✓ — Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No / Non ✓ — Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No / Non ✓ — Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No / Non ✓ — Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-18-RF11

Security Classification / Classification de sécurité
Protected A

PART C - (continued) / PARTIE C - (suite)

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC				
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens															
Production															
IT Media / Support TI															
IT Link / Lien électronique															

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

No ✓ Non — Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

No ✓ Non — Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).