Driving Permits

80th Session of WP.1
9 – 13 March 2020

Minimum Security Features & Machine Readable Properties:

Proposed amendments relating to Domestic Driving Permits and International Driving Permits in the 1968 Convention on Road Traffic

Informal Document 15 Rev 1

Introduction

Amalgamated Option adopted at 79th Session:

- A DDP compliant with Annex 6 (of the 1968 Convention) and with minimum security features which are recognised at international level, **or**
- An IDP compliant with Annex 7 (of the 1968 Convention) and with minimum security features recognised at international level.
- Countries wishing to retain a DDP not compliant with Annex 6 for domestic use will have to issue an IDP compliant with Annex 7 to drivers who wish to travel internationally

Minimum Security Features

- Informal Group considered the European Commission Directive 2006/126/EC
- Annex 1 prescribes minimum security features for EU Driving Licence
  - Card material must be polycarbonate
  - The material shall be made secure against forgery using following techniques
    - card bodies shall be UV dull
    - security background pattern designed to be resistant to counterfeit by scanning, printing or copying, using rainbow printing with multicolour security inks and positive and negative guilloche printing. The pattern shall not be composed of the primary colours (CMYK), shall contain complex pattern designs in a minimum of two special colours and shall include micro lettering

Minimum Security Features

- The material used for driving licences shall be made secure against forgery by using following techniques (continued)
  - optical variable elements providing adequate protection against copying and tampering of the photograph
  - laser engraving
  - in the area of the photograph the security design background and photograph should overlap on at least its border (weakening pattern)

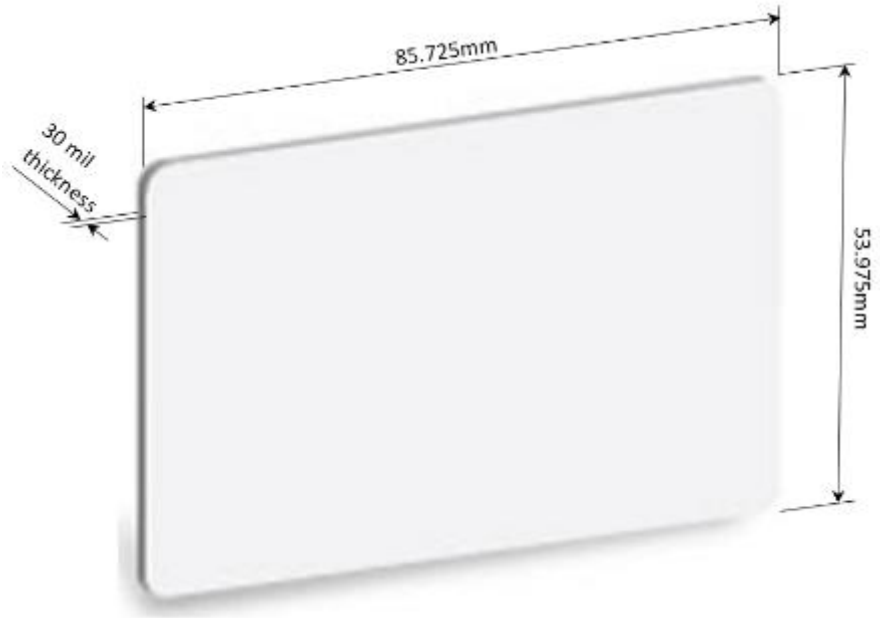
Minimum Security Features

- In addition, the material used for driving licences shall be made secure against forgery by using at least three of the following techniques (additional security features):
  - colour-shifting inks
  - termochromic ink
  - custom holograms
  - variable laser images
  - ultraviolet fluorescent ink, visible and transparent
  - iridescent printing
  - digital watermark in the background
  - infrared or phosphorescent pigments
  - tactile characters, symbols or patterns

Minimum Security Features

- Informal Group considered minimum security features in ISO Standard
- ISO not prescriptive as EC Directive by allowing several options
- Flexibility result in lower compliance cost relative to EC Directive, eg
  - Card material matched to validity period of driving permit, allowing less costly PVC Composite instead of Polycarbonate to be used for cards with validity of 5 years only
  - Various printing options instead of laser engraving only
- Yet, all prescribed security features in EC Directive are also incorporated in ISO Standard and all EU Driving Licences compliant with Directive 2006/126/EC are also compliant with security requirements in ISO Standard

Dimensions



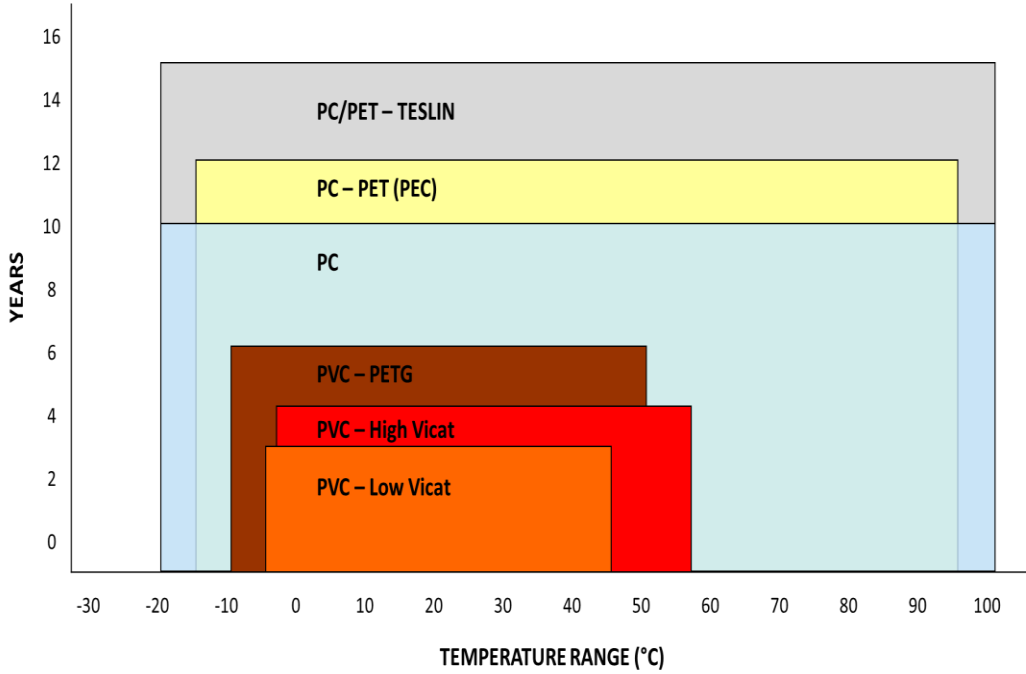
- The nominal dimensions of the card must be in conformance with ISO/IEC 7810 ID-1 (also in EC directives):
  - 85.60 × 53.98 millimetre (mm);
  - 30 mil thickness; and
  - rounded corners with a radius of 2.88–3.48 mm.
- Proposed reference to ISO/IEC 18013 incorporates requirements of ISO/IEC 7810

Card Material Options

An important consideration when selecting card body materials is durability of the material since this will determine the minimum guaranteed card life.

The following materials are typically used:

- PVC: up to 3 years
- PVC Composite: up to 6 y
- Polycarbonate (PC): 10 y
- PEC: up to 12 years
- PC/PET-Teslin: up to 15y (if cared for well)



Card Material Durability

Minimum Security Features

- ISO Standard classifies attacks as follow:
  - Counterfeiting:
    - Reproducing by scanning or copying
    - Re-origination
  - Falsification:
    - Modification of existing valid documents
    - Reuse of valid or invalid documents
  - Misuse of a genuine document:
    - Theft of original blank documents

Minimum Security Features

ISO Standard classifies security features to counter attacks:

- Card-body design
  - 10 features, of which one is compulsory and another one from the remaining 9 options must be selected.
- Security design resistant to reproduction
  - 8 features, of which three are compulsory and another one from the remaining 5 options must be selected.
- Security inks / pigments
  - 10 features, of which one is compulsory and another two from the remaining 9 options must be selected.
- Protecting personalised data
  - 12 features, of which three are compulsory and another one from the remaining 9 options must be selected.

ISO Minimum Security Features

- Card body security options to choose from:
  - UV-A dull substrate material
  - Fixed printed and/or dynamic data on different layers
  - Tamper evident card body
  - Taggant substances for genuine authentication
  - Look through element (transparent) such as window element
  - Look through element comprising grey levels
  - Card core inclusions
  - Pre-printed serial number on card blanks
  - Embossed surface pattern
  - Embedded thread or fibre

ISO Minimum Security Features

- Design security options to choose from:
  - No CMYK colours and at least 2 special colours
  - Guilloche design
  - Micro printed text
  - Anti-scan pattern
  - Duplex security pattern
  - Rainbow printing
  - Deliberate error into the design or microprint
  - Use of non-standard type-fonts

ISO Minimum Security Features

Security ink/Pigment options to choose from:

- Security background printing
  - UV fluorescent ink in security background printing
  - Optical effect pigments (other than UV or IR pigments)
  - IR-fluorescent ink
  - IR-drop out inks
  - Non-optical effect pigments
- Personalised data
  - Optical effect pigments (other than UV or IR pigments)
  - IR fluorescent ink
  - IR drop-out inks
  - Non-optical effect pigments
  - UV fluorescent ink in personalized data

ISO Minimum Security Features

- Printing security options to choose from:
  - Electro-photographic printing
  - Thermal transfer printing
  - Ink-jet printing
  - Photographic process
  - Laser engraving

ISO Minimum Security Features

- Personalisation security options to choose from:
  - Printing dynamic data elements using digital imaging technologies
  - Sub-surface personalisation technique, or laminate, overlay or coating for surface printed data and portrait
  - Visible security element overlapping the portrait
  - Security background overlapping the portrait image area
  - Embedded data in the portrait image
  - Redundant personalized data
  - Optical Variable Element
  - Areas of different surface reflection
  - Personalized tactile elements
  - Lenticular patterns (such as variable laser element CLI/MLI)
  - Random pattern resulting in unique codes
  - Magnetic/Optical media "finger printing"

Examples of Security Features

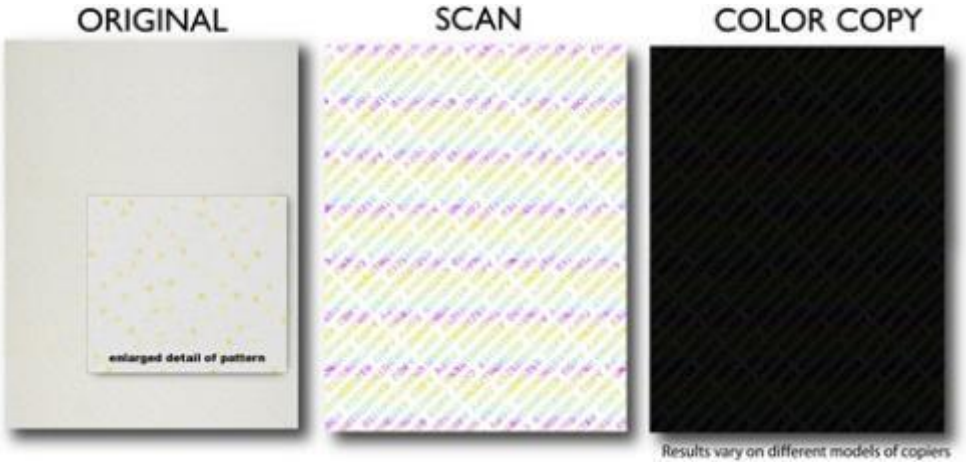
- UV-A Dull Substrate Material
  - UV Dull materials possess a controlled response to UV light and exhibit a particular fluorescence that can easily be distinguished in colour from the blue-hued fluorescence seen when more commonly available material is used to produce a document.

- No CMYK Colours and at least 2 Special Colours
  - CMYK refers to the four inks used in some colour printing: cyan, magenta, yellow, and key (black). Special colours are any custom (non-standard) colours that are difficult to reproduce/ copy.
  - The static security features on the document body must not feature CMYK colours and must also contain at least two special colours.

Examples of Security Features

- Guilloche Design

- Anti-Scan Pattern
  - image is constructed of fine lines at varying angular displacement and embedded in the security background design



Examples of Security Features

- UV Fluorescent Ink in Security Background Printing

- Printing Dynamic Data Elements Using Digital Imaging Technologies
  - Marking private/ dynamic data that is specific to a given document onto the document surface. Examples of private/ dynamic data includes the licence number, portrait image, signature, name, surname, date of birth, and other human readable data elements.

Examples of Security Features

- Laminate, Overlay or Coating for Surface Printed Data and Portrait

- Security Background Overlapping The Portrait Image Area

Examples of Security Features

- Pre-Printed Serial Number on Blanks

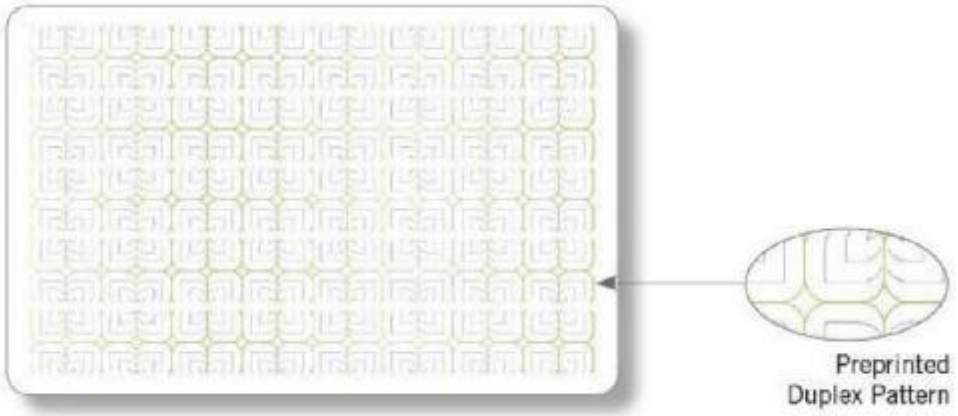
- Embossed Surface Pattern

Examples of Security Features

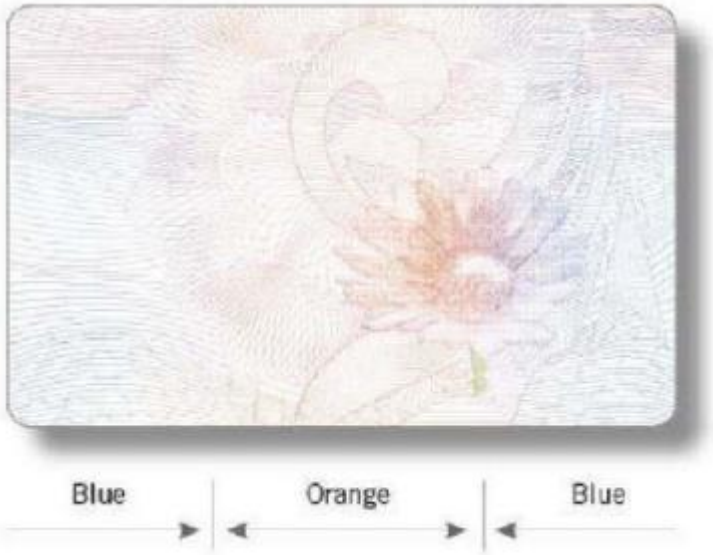
- Micro Printed Text

Examples of Security Features

- Duplex Security Pattern



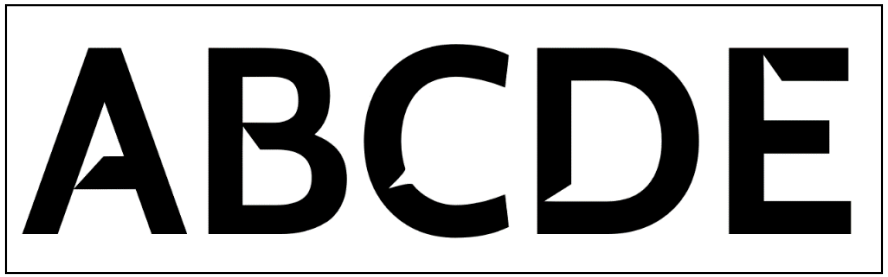
- Rainbow Printing



Examples of Security Features

- Deliberate Error Into the Design or Microprint

- Use of Non-Standard Type-Fonts



Examples of Security Features

- UV Fluorescent Ink in Personalised Data

- Optically Variable Element

Examples of Security Features

- Redundant Personalised Data

Portrait side

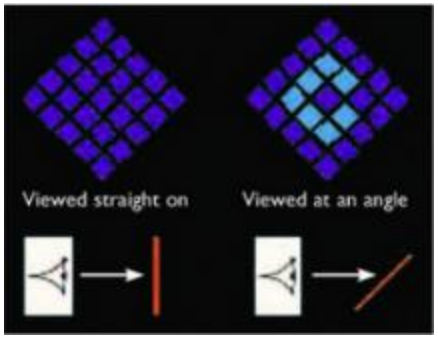
Non-portrait side

Examples of Security Features

- Taggant Substances for Genuine Authentication
  - Taggant substances are secret tracer materials inserted inside the document, which can only be detected in a laboratory with specific equipment.
- Look Through Element
  - A transparent window is created inside the document, which renders it impossible to copy.

Examples of Security Features

- Optical Effect Pigments

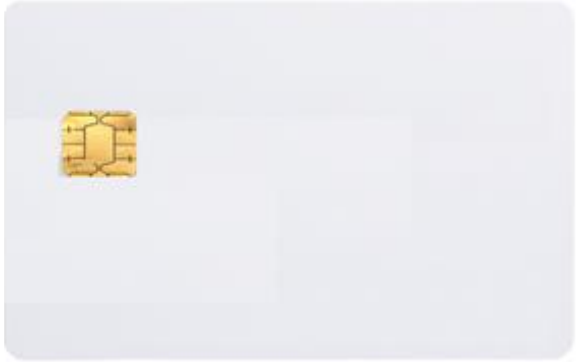


- IR-Fluorescent
  - IR fluorescent pigments do not follow Stokes Law, instead they are excited by IR energy, and either emit in the visible region or in the IR region but at a shorter wavelength
- IR Drop Out
  - These inks are the exact opposite of IR-fluorescent inks.

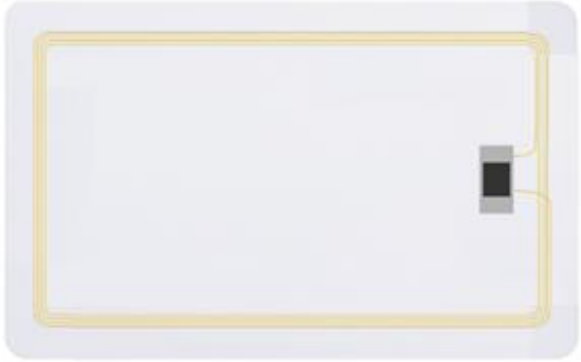
Machine Readable Technologies

- DDP and IDP may contain data & photograph of driver stored:
  - In a printed 2D Barcode of type PDF-417
  - Electronically in an Integrated Circuit of either:
    - Contact Integrated Circuit (C-ICC) – contact chip
    - Proximity Integrated Circuit (P-ICC) – contactless chip

2D Barcode

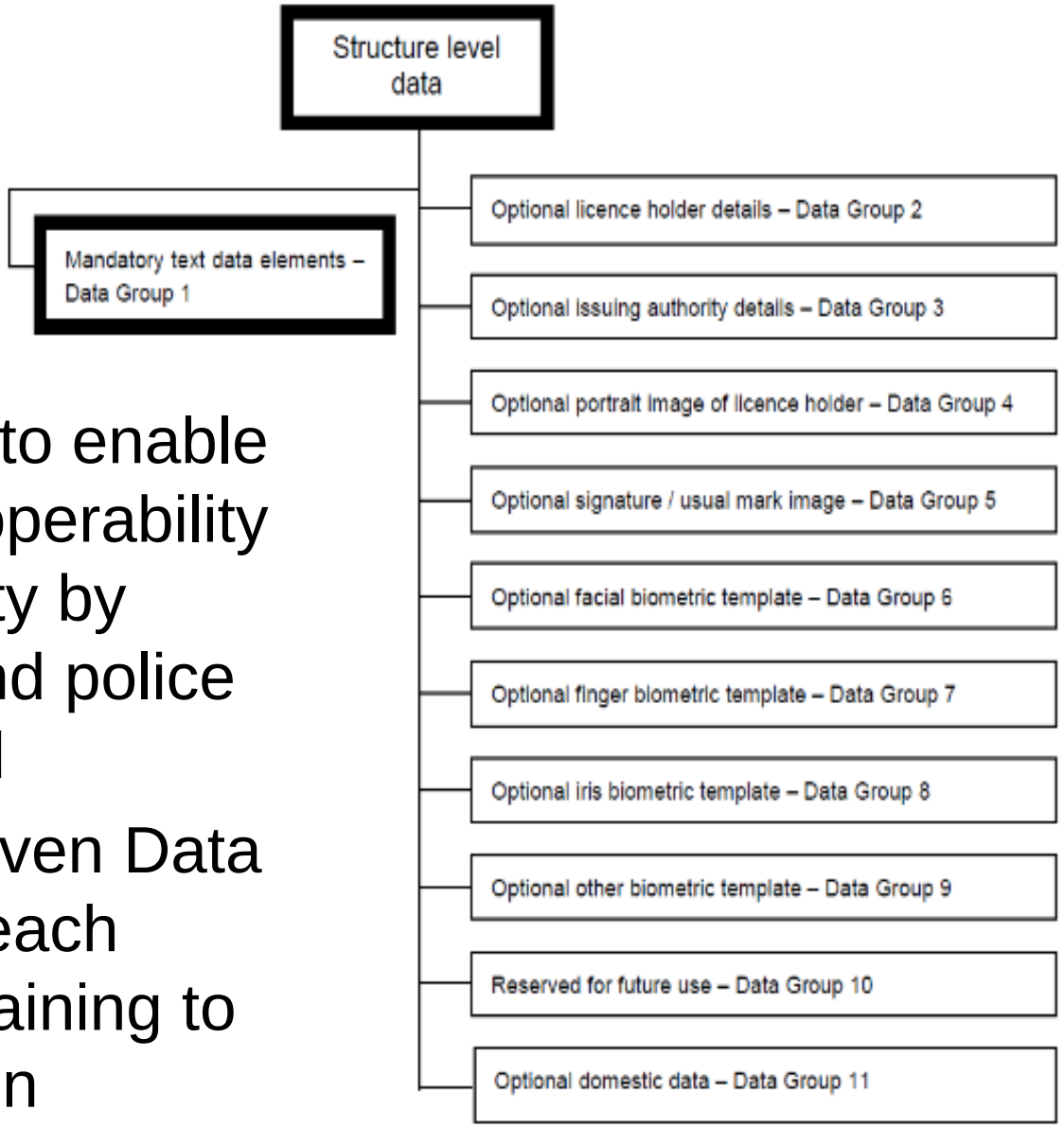


C-ICC (with surface contacts)



P-ICC (embedded within card layers)

Machine Readable Data



- Data is structured to enable international interoperability – ensure readability by domestic police and police in countries visited
- Organised into eleven Data Groups, of which each contains data pertaining to a particular function

Recording of Data

Technology with Limited Storage Capacity

- High efficiency (compact) coding of data
- Data take up less storage space (kilobytes)
- Typical media includes:
  - 2D Barcodes
  - P-ICCs and C-ICCs with limited storage capacity

Technology with Larger Storage Capacity

- Data take up larger memory capacity (megabytes)
- Allows random data access for more flexible reading
- Typical media includes:
  - C-ICCs (based on ISO/IEC 7816)
  - P-ICCs (based on ISO/IEC 14443)

Interoperablility

- In both cases only achieved by following one common & comprehensive standard

Data Integrity & Protection

- **2D Barcode – Digital Signature**
  - Incorporated in data recorded in 2D Barcode to enable validating correctness & authenticity of data
- **ICC - Access Control, Authentication, Integrity Validation**
  - Digital signature (to confirm data has not been changed)
  - No data access without optical visibility of printed information too
  - Release of specific data only upon presentation of authorisation (using cryptographic techniques)
  - Cryptographically securing data exchange
- **Only useful if both issuer and reader follow the same standard**

Conclusion

- Minimum security features & machine readable properties for DDP:
  - In conformance with ISO Standards
  - EC Regulation (EU) No 383/2012 of 4 May 2012 also refers to the ISO Standards
- Minimum security features, machine readable properties & format of IDP:
  - Card with layout corresponding to DDP, but for inscription “International Driving Permit”
  - Promote ease of interpretation by police & service providers as standalone document in the absence of DDP
  - In conformance with ISO Standards, similar to DDP
- Future direction
  - Incorporate provision for Mobile Driving Permit/Licence