United Nations ECE/TRANS/WP.1/2020/8

Economic and Social Council

Distr.: General
13 July 2020

Original: English

Economic Commission for Europe

Inland Transport Committee

Global Forum for Road Traffic Safety

Eighty-first session
Geneva, 21-25 September 2020
Item 3 (b) of the provisional agenda
Convention on Road Traffic (1968):
Driving Permits

Appendix C Examples of the difficulty of selecting options from the ISO Standards for inclusion in the 1968 Convention

Submitted by the Experts of Belgium, Brazil, Canada, France, Luxembourg, Russian Federation, United Kingdom of, Great Britain and Northern Ireland, Fédération Internationale de l'Automobile and International Organization for Standardization

This document contains Appendix C of ECE/TRANS/WP.1/2018/1/Rev.3. That is, examples of the difficulty of selecting options from the ISO Standards for inclusion in the 1968 Convention (provided by ISO).

GE.20-09309(E)
2009309

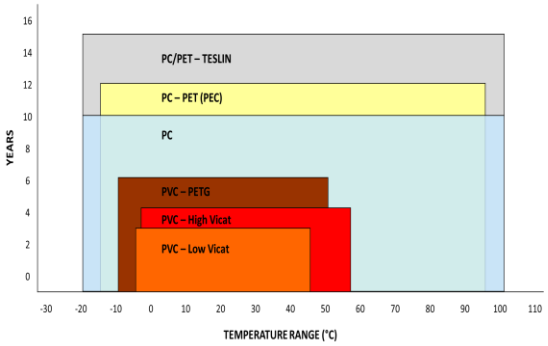
Appendix C

I. Card body material

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

2. The following materials are typically used:

- PVC: up to 3-year card service life;
- PVC Composite: up to 6-year card service life;
- Polycarbonate (PC): 10-year card service life;
- PEC: up to 12-year card service life;
- PC/PET-Teslin: up to 15-year card service life (if cared for well).



3. The European Commission opted for a polycarbonate card body to match their desired 10-year service life. But, there are many Contracting Parties to the 1968 Convention that issue a driving licence valid for only 3 years or 5 years. To prescribe a single card body material for them will result in unnecessary additional costs as the less costly PVC or PVC Composite card body material would have been appropriate for a 3-year or 5-year validity period respectively.

II. Printing (personalisation)

4. The following printing technologies are included as options in the ISO standard:

- Electro-photographic printing;
- Thermal transfer printing;
- Ink-jet printing;
- Photographic process;
- Laser engraving.

5. The printing technology must be appropriate for the card body material and aspects such as whether lamination is applied before or after personalisation. Upon selecting a polycarbonate card, the European Commission had to select a printing option appropriate for the card body material and did not have many options but to opt for laser engraving. Laser engraving has many security benefits but cannot personalise a digitised colour photograph of the card holder unless a second printing technology is combined with laser engraving. Not only is laser engraving one of the costliest printing options, but many Contracting Parties to the 1968 Convention require that a digital colour image of the holder be on the card.

III. Minimum Security Features

6. To effectively combat the possible attacks on a driving licence card, the ISO standard identifies 3 types of card fraud together with the threats relating to each type, and lists the available options to counter each of the threats for the issuing authority to select its desired combination of features:

- Counterfeiting – producing a simulation of the genuine document, including reproduction by scanning or copying and re-origination.
- Falsification – altering the holder's details on a genuine document, including modification of existing valid documents and reuse of valid or invalid documents.
- Misuse of a genuine document – theft of original blank documents, or posing as the rightful holder (particularly with a poor-quality photo image of the holder on the card) by an imposter that resembles the actual holder of the driving licence.
- The following counter measures and number of options for each are listed in the ISO standard:
- Card-body design – 10 features, of which one is compulsory and another one from the remaining 9 options must be selected. Amongst the 9 options are the following: Fixed printed and/or dynamic data on different layers, Tamper evident card body, Look through element (transparent) such as window element, Pre-printed serial number on card blanks and Embedded thread or fibre.
- Security design resistant to reproduction – 8 features, of which three are compulsory and another one from the remaining 5 options must be selected. Amongst the 5 options are the following: Micro printed text, Duplex security pattern, Rainbow printing, Deliberate error into the design or microprint and Use of non-standard type fonts.
- Security inks/ pigments – 10 features, of which one is compulsory and another two from the remaining 9 options must be selected. Amongst the 9 options are the following: Optical effect pigments (other than UV or IR pigments), IR-fluorescent ink, IR-drop out inks, Non-optical effect pigments and UV fluorescent ink in personalised data.
- Protecting personalised data – 12 features, of which three are compulsory and another one from the remaining 9 options must be selected. Amongst the 9 options are the following: Visible security element overlapping the portrait, Embedded data in the portrait image, Redundant personalized data, Optical Variable Element, Areas of different surface reflection, Personalised tactile elements, Lenticular patterns (such as variable laser element CLI/MLI) and Random pattern resulting in unique codes.

7. In summary, the proposed ISO card security standard allows for the selection of security features that match the card service life, security threats and budget of each issuing authority. At the same time, it also establishes sufficient security to allow one issuing authority to trust the integrity of a card issued by another issuing authority. The European Commission has selected a number of these security features based on the selection of a polycarbonate card body material and laser engraving printing, which have been prescribed to its members.

8. However, due to the vast differences in validity period of the domestic driving permits among the Contracting Parties and consequently the most economical card body material to match the required card service life, this approach is not feasible to be adopted in the proposed amendments of the 1968 Convention.

IV. Machine Readable Technologies

9. It is not envisaged to include machine readable technologies on a card as a mandatory requirement for a DDP or IDP in the proposed amendment of Annex 6 and Annex 7, but to allow Contracting Parties who wish to include such technologies the option to do so. There are many benefits to include the ISO specified machine readable technologies on a DDP, the

most significant of which is that the digital signature included with the stored data in respect of all the specified technologies allows “off line” authentication of the document and verification of the integrity of the stored data without the need to connect to the originating database.

10. However, to enable international interoperability of such machine-readable technologies for contracting parties to be able to benefit from such electronic security features and an “off-line” authentication of a DDP issued by another contracting party, the data content of these technologies must conform to a standardised structure. Similarly, the method of securing the data by digital signature and the means of validating the integrity of the stored data must be standardised. In the absence thereof, only the issuing authority that issued the DDP will be able to interpret the content of the machine-readable technologies on a card.

11. The ISO standards take into account that the data storage capacity of the various machine-readable technologies are not the same, and specify a data structure suitable to the limitations of each technology, without sacrificing the minimum security requirements relating to each. The following machine-readable technologies are specified:

- 2-Dimensional barcode – printed on the back of the card during personalisation without any additional cost relative to a card without any machine-readable technology.
- Contact chip – chip (integrated circuit) protruding from the card surface to allow contact between the reader and the chip, adding to the cost of the card. The data storage capacity of a chip is scalable but has a cost implication – the larger the storage capacity the costlier the chip becomes. However, it does allow for storage of biometric credentials such as the digital portrait image and finger print of the card holder.
- Proximity chip – chip (integrated circuit) is encapsulated within the card body, inclusive of an antenna to allow reading of the chip. A proximity chip is generally costlier than a contact chip, but presents a more durable card as the surface of the card is not broken and removing a chip from a card and placing it in another card is not possible without delaminating the card (and probably damaging the antennae). The data storage capacity is scalable similar to the contact chip and also has a similar cost implication.

12. The European Commission has selected a specific data structure, matching content and security features for a chip (contact or proximity) from ISO/IEC 18013, and prescribed that for its members in a Regulation to be complied with if included on its driving licence by any EU member state.

13. However, this approach is not feasible to be adopted in the proposed amendments of the 1968 Convention because it rules out the cost-effective use of a 2-dimensional barcode and imposes a minimum data storage capacity (and corresponding cost) of the chip. Again, the ISO standards allow the issuing authority to select the machine-readable technology appropriate to its driving licence, if any. Furthermore, it does not require a minimum storage capacity of a chip included on a driving licence – certain optional data groups relating to data specified as optional in the 1968 Convention and biometric credentials are simply not stored if the chip storage capacity is insufficient to accommodate such aspects.