EUROPEAN
COMMISSION

Brussels, 24.4.2025
COM(2025) 179 final

ANNEX 2

**ANNEX**

**to the**

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on the registration documents for vehicles and vehicle registration data recorded in national vehicle registers and repealing Council Directive 1999/37/EC**

{SEC(2025) 119 final} - {SWD(2025) 96 final} - {SWD(2025) 97 final} -
{SWD(2025) 98 final} - {SWD(2025) 99 final}

## Annex II

## Part II of the registration certificate

1. This part may be implemented in either of two formats: as a paper document or as a smart card. The characteristics of the paper document version are specified in point 2 and those of the smart card version in point 3.

2. Specifications of Part II of the registration certificate in paper format

   (a) The overall dimensions of the registration certificate shall not be greater than an A4 format (210 × 297 mm) or a folder of A4 format.

   (b) The paper used for part II of the registration certificate shall be made secure against forgery by using at least two of the following techniques:

      (i) graphics,

      (ii) watermark,

      (iii) fluorescent fibres, or

      (iv) fluorescent imprints.

      Member States are free to introduce additional security features.

   (c) Part II of the registration certificate may consist of several pages. Member States shall determine the number of pages in accordance with the information contained in the document and its layout.

   (d) The first page of Part II of the registration certificate shall contain

      (i) the name of the Member State issuing Part II of the registration certificate,

      (ii) the distinguishing mark of the Member State issuing Part II of the registration certificate, namely:

      B: Belgium

      BG: Bulgaria

      CZ: Czech Republic

      DK: Denmark

      D: Germany

      EST: Estonia

      GR: Greece

      E: Spain

      F: France

      HR: Croatia

      IRL: Ireland

      I: Italy

      CY: Cyprus

      LV: Latvia

      LT: Lithuania

L: Luxembourg

H: Hungary

M: Malta

NL: Netherlands

A: Austria

PL: Poland

P: Portugal

RO: Romania

SLO: Slovenia

SK: Slovakia

FIN: Finland

S: Sweden

(iii) the name of the competent authority,

(iv) the words ‘Part II of the Registration Certificate’, printed in large type in the language or languages of the Member States issuing the registration certificate; they shall also appear, after a suitable space, in small type, in the other languages of the European Union,

(v) the words ‘European Union’, printed in the language or languages of the Member State issuing Part II of the registration certificate,

(vi) the number of the document.

(e) Part II of the Registration Certificate shall also contain the following data, preceded by the corresponding harmonised Union codes:

(A) registration number,

(B) date of the first registration of the vehicle,

(C.2) owner of the vehicle,

(C.2.1) surname(s) or business name,

(C.2.2) other name(s) or initial(s) (where appropriate),

(C.2.3) address in the Member State of registration, on the date of issue of the document,

(D) vehicle:

(D.1) make,

(D.2) type,

- variant (if available),

- version (if available),

(D.3) commercial description(s),

(E) vehicle identification number,

(J) vehicle category,

(J.1) bodywork,

(K) whole-vehicle vehicle type-approval number (if available).

(f) Part II of the registration certificate may, moreover, contain the following data, preceded by the corresponding harmonised Union codes:

(C) personal data,

(C.3) natural or legal person who may use the vehicle by virtue of a legal right other than that of ownership,

(C.3.1) surname(s) or business name,

(C.3.2) other name(s) or initial(s) (where appropriate),

(C.3.3) address in the Member State of registration, on the date of issue of the document,

(C.5), (C.6) where a change in the personal data given in point (e), code (C.2) and/or code (C.3) does not give rise to the issue of a new Part II of the Registration Certificate, the new personal data corresponding to these points may be included under codes (C.5) or (C.6); they are broken down in accordance with point (e) code (C.2) and code (C.3).

(g) Member States may include additional information in Part II of the registration certificate; in particular, they may add between brackets to the identification codes, as laid down under points (e) and (f), additional national codes.

3. Specifications of Part II of the Registration Certificate in smart card format (Alternative to the specimen in paper format described in point 2)

(a) *Card format and data legible with the eye*

Being a microprocessor card, the chip card shall be designed in accordance with the standards mentioned in point (e).

Printed on the front and back of the card shall be at least the data specified in point 2, points (d) and (e); these data shall be legible with the eye (minimum character height: 6 points) and printed on as follows. (Examples of possible layouts are presented in Figure 2 at the end of this section)

(i) Basic Imprint

*Front*

(1) To the right of the chip location:

in the language(s) of the Member State issuing the Registration Certificate

— the words ‘European Union’,

— the name of the Member State issuing the Registration Certificate,

— the words ‘Part II of the Registration Certificate’ printed in large type,

— another (e.g. previous national) designation of the equivalent document (optional),

— the name of the competent authority (alternatively, also in the form of a personalisation imprint as per point (ii)),

— the unambiguous consecutive number of the document as used within the Member State (alternatively, also in the form of a personalisation imprint as per point (ii)).

(2) Above the chip location:

The distinguishing mark of the Member State issuing the Registration Certificate, white in a blue rectangle and surrounded by 12 yellow stars:

B Belgium

BG: Bulgaria

CZ: Czech Republic

DK: Denmark

D: Germany

EST: Estonia

GR: Greece

E: Spain

F: France

HR: Croatia

IRL: Ireland

I: Italy

CY: Cyprus

LV: Latvia

LT: Lithuania

L: Luxembourg

H: Hungary

M: Malta

NL: Netherlands

A: Austria

PL: Poland

P: Portugal

RO: Romania

SLO: Slovenia

SK: Slovakia

FIN: Finland

S: Sweden

(3) Member States might consider adding, at the lower edge in small type and in their national language(s), the note: 'This document should be kept in a safe place outside the vehicle.'

(4) The basic colour of the card is red (Pantone 194); alternatively, a red-to-white transition is possible.

(5) A symbol representing a wheel (see proposed lay-out) shall be printed within the printing area in the bottom left corner of the card front.

(6) In other respects, the provisions of point (m) shall apply.

(ii) Personalisation imprint

The personalisation imprint shall contain the following information:

*Back*

The back shall bear at least the remaining data specified in point 2, point (e).

According to point 2, point (g), individual national codes may be added to the preceding harmonised Union codes.

In detail, these vehicle data are:

(C.2) owner of the vehicle,

(C.2.1) surname(s) or business name,

(C.2.2) other name(s) or initial(s) (where appropriate),

(C.2.3) address in the Member State of registration, on the date of issue of the document,

(D.1) make,

(D.2) type (variant/version, where appropriate),

(D.3) commercial description(s),

(E) vehicle identification number,

(J) vehicle category,

(J.1) bodywork,

(K) Vehicle-type vehicle type-approval number (if available).

Optionally, additional data from point 2, point (f) (with the harmonised codes) and point 2, point (g) may be added on the back of the card.

*Front*

(1) the name of the competent authority – see also point (i),

(2) the name of the authority issuing the Registration Certificate (optional),

(3) the unambiguous consecutive number of the document as used within the Member State – see also point (i),

(4) the following data from point 2, point (e),

(5) according to point 2, point (g), individual national codes may be added to the preceding harmonised Union codes:

(A) registration number (official licence number),

(B) date of first registration of the vehicle.

*Back*

(iii) Physical security features of the smart card

The threats to the physical security of documents are:

(1) Production of false cards: creating a new object which bears great resemblance to the document, either by making it from scratch or by copying an original document.

(2) Material alteration: changing a property of an original document, e.g. modifying some of the data printed on the document.

As a basis, the techniques indicated with an asterisk are to be preferred as they enable the law enforcement officers to check the validity of the card without any special means.

The material used for Part II of the registration certificate shall be and secure against forgery by using at least three of the following techniques:

— microprinting,

— guilloche printing*,

— iridescent printing,

— laser engraving,

— ultraviolet fluorescent ink,

— inks with viewing angle — dependent colour*,

— inks with temperature — dependent colour*,

— custom holograms*,

— variable laser images,

— optical variable images.

Member States are free to introduce additional security features.

(b) *Data storage and protection*

Preceded by the harmonised common codes (where appropriate, in connection with the individual codes of the Member States according topoint 2, point (g)), the following data shall or may be additionally stored on the card surface bearing the legible information as per point (a):

(i) Data as per point 2, points (d) and (e).

All data specified in point 2, points (d) and (e) shall be mandatorily stored on the card.

(ii) Other data as per point point 2, point (f).

Moreover, the Member States are free to store more data as perpoint 2, point (f), to the necessary extent.

(iii) Other data as per point point 2, point (g).

Optionally, further vehicle-related data of general interest may be stored on the card.

The data from the points (i) and (ii) are stored in two corresponding files with transparent structure (see ISO/IEC 7816-4). The Member States may specify the storage of data from point (iii) according their requirements.

There are no read restrictions on these files.

Write access to these files shall be restricted to the national competent authorities (and their authorised Agencies) in the Member State issuing the smart card.

Write access is permitted only after an asymmetric authentication with session key exchange for protecting the session between the vehicle registration card and a Security Module (e.g. a Security Module Card) of the national competent authorities (or their authorised Agencies). Thereby Card Verifiable certificates according to ISO/IEC 7816-8 are exchanged before the authentication process. The Card Verifiable certificates contain the corresponding public keys to be retrieved and to be used in the following authentication process. These certificates are signed by the national competent authorities and contain an authorisation object (certificate holder authorisation) according to ISO/IEC 7816-9 in order to encode role specific authorisation to the card. This role authorisation is related to the national competent authority (e.g. to update a data field).

The corresponding public keys of the national competent authority are stored as trust anchor (root public key) in the card.

The specification of the files and commands needed for the authentication process and the writing process is under responsibility of the Member States. The security assurance has to be approved by Common Criteria Evaluation according to EAL4+. The augmentations are as follows: 1. AVA MSU.3 Analysis and testing for insecure states; 2. AVA VLA.4 Highly resistant.

(iv) Verification data for authenticity of registration data

The issuing authority calculates its electronic signature about the complete data of a file containing the data of the points (i) and (ii) and stores it in a related file. These signatures allow the authenticity of the stored data to be verified. The cards shall store the following data:

(1) electronic signature of registration data related to point (i),

(2) electronic signature of registration data related to point (ii).

For verification of these electronic signatures the card shall store:

(1) certificates of the issuing authority calculating the signatures about the data of points (i) and (ii).

Electronic signatures and the certificates shall be readable without restriction. Write access to electronic signatures and certificates shall be restricted to the national competent authorities.

(c) *Interface*

External contacts should be used for interfacing. A combination of external contacts with a transponder is optional.

(d) *Storage capacity of the card*

The card shall have sufficient capacity to store the data mentioned inpoint (b).

(e) *Standards*

The chip card and reading devices used shall comply with the following standards:

| | |
|---|---|
| ISO 7810 | Standards for identification cards (plastic cards): Physical characteristics |
| ISO 7816-1 and -2 | Physical characteristics of chip cards, dimensions and location of contacts |
| ISO 7816-3 | Electrical characteristics of contacts, transmission protocols |
| ISO 7816-4 | Communication contents, chip card data structure, safety architecture, access mechanisms |
| ISO 7816-5 | Structure of application identifiers, selection and execution of application identifiers, registration procedure for application identifiers (numbering system) |
| ISO 7816-6 | Inter-industry data elements for interchange |
| ISO 7816-8 | Integrated circuit(s) cards with contacts – Security related inter-industry commands |
| ISO 7816-9 | Integrated circuit(s) cards with contacts – Enhanced inter-industry commands |

(f) *Technical characteristics and transmission protocols*

The format shall be ID-1 (normal size, see ISO/IEC 7810).

The card shall support transmission protocol T = 1 in compliance with ISO/IEC 7816-3. Additionally other transmission protocols may be supported, e.g. T=0, USB or contactless protocols.

For bit transmission the 'direct convention' shall be applied (see ISO/IEC 7816-3).

(i) Supply voltage, programming voltage

The card shall work with Vcc = 3V (+/0.3V) or with Vcc = 5V (+/0.5V). The card shall not require a programming voltage at pin C6.

(ii) Answer to reset

The Information Field Size Card byte shall be presented at the ATR in character TA3. This value shall be at least '80h' (=128 bytes).

(iii) Protocol parameter selection

The support of protocol parameter selection (PPS) according to ISO/IEC 7816-3 is mandatory. It is used for selecting T=1, if T=0 is additionally present in the card, and to negotiate the Fi/Di parameters for achieving higher transmission rates.

(iv) Transmission protocol T=1

The support of chaining is mandatory.

The following simplifications are allowed:

(1) NAD Byte: not used (NAD should be set to '00'),

(2) S-Block ABORT: not used,

(3) S-Block VPP state error: not used.

The information field size device (IFSD) shall be indicated from the IFD immediately after ATR, i.e. the IFD shall transmit the S-block IFS request after ATR and the card shall send back S-block IFS. The recommended value for IFSD is 254 bytes.

(g) *Temperature range*

The registration certificate in smart card format shall properly function under all climatic conditions usually prevailing in the territories of the Union and at least in the temperature range specified in ISO 7810. The cards shall be capable of operating correctly in the humidity range 10 % to 90%.

(h) *Physical lifetime*

If used in accordance with the environmental and electricity-related specifications, the card must function properly for a period of ten years. The material of the card must be chosen in such a way that this lifetime is ensured.

(i) *Electrical characteristics*

During operation, the cards shall conform to the provisions of Regulation (EU) 2019/2144 related to electromagnetic compatibility, and shall be protected against electrostatic discharges.

(j) *File structure*

Table 4 lists the mandatory elementary files (EF) of the application DF (see ISO/IEC 7816-4) DF.Registration. All these files have a transparent structure. The access requirements are described in point (b). The file sizes are specified by the Member States according their requirements.

Table 4

| Filename | File Identifier | Description |
|---|---|---|
| EF.Registration_A | ‘D001’ | Registration data according to the point 2, points (d) and (e) |
| EF.Signature_A | ‘E001’ | Electronic Signature about complete data content of EF.Registration_A |
| EF.C.IA_A.DS | ‘C001’ | X.509v3 Certificate of the issuing authority calculating the signatures for EF.Signature_A |
| EF.Registration_B | ‘D011’ | Registration data accordingpoint 2, point (f) |
| EF.Signature_B | ‘E011’ | Electronic Signature about complete data content of EF.Registration_B |
| EF.C.IA_B.DS | ‘C011’ | X.509v3 Certificate of the issuing authority calculating the signatures for EF.Signature_B |

(k) *Data structure*

The stored certificates are in the X.509v3 format according ISO/IEC 9594-8.

The electronic signatures are stored transparent.

The registration data is stored as BER-TLV data objects (see ISO/IEC 7816-4) in the corresponding elementary files. The value fields are coded as ASCII character as defined by ISO/IEC 8824-1, the values ‘C0’-‘FF’ are defined by ISO/IEC 8859-1 (Latin1 character set) or ISO/IEC 8859-7 (Greek character set) or ISO/IEC 8859-5 (Cyrillic character set). The format of dates is YYYYMMDD.

Table 1 lists the Tags identifying the data objects corresponding to the registration data of point 2, points (d) and (e) together with additional data from point (a). Unless otherwise stated, the data objects listed in Table 5 are mandatory. Optional data objects may be omitted. The column of the Tag indicates the level of nesting.

Table 1

| **Tag** | | | | **Description** |
|---|---|---|---|---|
| ‘78’ | | | | Compatible tag allocation authority, nesting object ‘4F’ (see ISO/IEC 7816-4 and ISO/IEC 7816-6) |
| | ‘4F’ | | | Application identifier (see ISO/IEC 7816-4) |
| ‘73’ | | | | Inter-industry template (see ISO/IEC 7816-4 and ISO/IEC 7816-6) corresponding to mandatory data of the registration certificate Part 2, nesting all following objects |
| | ‘80’ | | | Version of tag definition |
| | ‘9F33’ | | | Name of the Member State issuing the registration certificate |

| **Tag** | | | | **Description** |
|---|---|---|---|---|
| | | | | Part 2 |
| | ‘9F34’ | | | Another (e.g. previous national) designation of the equivalent document (optional) |
| | ‘9F35’ | | | Name of the competent authority |
| | ‘9F36’ | | | Name of the authority issuing the registration certificate (optional) |
| | ‘9F37’ | | | Character set used:‘00’: ISO/IEC 8859-1 (Latin1 character set)‘01’: ISO/IEC 8859-5 (Cyrillic character set)‘02’: ISO/IEC 8859-7 (Greek character set) |
| | ‘9F38’ | | | Unambiguous consecutive number of the document as used within the Member |

| Tag | | | | Description |
|---|---|---|---|---|
| | | | | State |
| | ‘81’ | | | Registration number |
| | ‘82’ | | | Date of first registration |
| | ‘A3’ | | | Vehicle, nesting objects ‘87’, ‘88’ and ‘89’ |
| | | ‘87’ | | Vehicle make |
| | | ‘88’ | | Vehicle type |
| | | ‘89’ | | Vehicle commercial descriptions |
| | ‘8A’ | | | Vehicle identification number |
| | ‘8F’ | | | Type approval number |

Table 3 lists the Tags identifying the data objects corresponding to the registration data of point 2, point (f). The data objects listed in Table 6 are optional.

Table 3

| Tag | | | | Description |
|---|---|---|---|---|
| ‘78’ | | | | Compatible tag allocation authority, nesting object ‘4F’ (see ISO/IEC 7816-4 and ISO/IEC |

| Tag | | | | Description |
|---|---|---|---|---|
| | | | | 7816-6) |
| | ‘4F’ | | | Application identifier (see ISO/IEC 7816-4) |
| ‘74’ | | | | Inter-industry template (see ISO/IEC 7816-4 and ISO/IEC 7816-6) corresponding to optional data of the registration certificate Part 1,point 2, point (f), nesting all following objects |
| | ‘80’ | | | Version of tag definition |
| | ‘A1’ | | | Personal data nesting objects ‘A7’, ‘A8’ and ‘A9’ |
| | | ‘A7’ | | Vehicle owner nesting objects ‘83’, ‘84’ and ‘85’ |
| | | | ‘83’ | Surname or business name |
| | | | ‘84’ | Other names |

| **Tag** | | | | **Description** |
|---|---|---|---|---|
| | | | | or initials (optional) |
| | | | ‘85’ | Address in the Member State |
| | | ‘A8’ | | Second vehicle owner nesting objects ‘83’, ‘84’ and ‘85’ |
| | | | ... | |
| | | ‘A9’ | | Person who may use the vehicle by virtue of legal right other than ownership nesting objects ‘83’, ‘84’, and ‘85’ |
| | | | ... | |
| | ‘98’ | | | Vehicle category |

Structure and format of the data according to point 2, point (g) are specified by the Member States.

(l) *Reading the registration data*

(i) Application Selection

The Application ‘Vehicle Registration’ shall be selectable by a SELECT DF (by name, see ISO/IEC 7816-4) with its Application identifier (AID). The AID value is requested from a laboratory selected by the European Commission.

(ii) Reading data from files

The files corresponding to point 2, points (d), (e) and (f), shall be selectable by SELECT (see ISO/IEC 7816-4) with the command parameters P1 set to ‘02’, P2 set to ‘04’ and the command data field

containing the file identifier (see point (j), Table 4 ). The returned FCP template contains the file size which can be useful for reading these files.

These files shall be readable with READ BINARY (see ISO/IEC 7816-4) with an absent command data field and Le set to the length of the expected data, using a short Le.

(iii) Verification of data authenticity

To verify the authenticity of the stored registration data, the corresponding electronic signature may be verified. This means that besides the registration data also the corresponding electronic signature may be read from the registration card.

The public key for signature verification can be retrieved by reading the corresponding issuing authority certificate from the registration card. Certificates contain the public key and the identity of the corresponding authority. The signature verification may be performed by another system than the registration card.

The Member States are free in retrieving the public keys and certificates for verifying the issuing authority certificate.

(m) *Special provisions*

Irrespective of the other provisions herein, the Member States, after notifying the European Commission, may add colours, marks or symbols. In addition, for certain data of point (b)(iii), the Member States may allow XML format and may allow access via TCP/IP. Member States may, with the agreement of the European Commission, add other applications for which no harmonised rules or documents exist yet at EU level (e.g. roadworthiness certificate), on the vehicle registration card to realise additional vehicle related services.