

Revision of the Directive on Driving Licences

Eurosmart's Answer to Public Consultation

Eurosmart, the leading European association representing the digital security industry, welcomes the European Commission's approach to give citizens the choice of their driving licence format. This technology-agnostic standpoint aligns with a holistic vision of inclusion without discrimination and empowering citizens with their data. Our organisation is pleased to share its feedback on specific aspects of the proposed Directive on Driving Licences revision.

Maintain high level of service availability for driving licence inspection

Eurosmart very much welcomes the ambition of the text to move towards a driving licence which is mobile in a very short timeframe. This ambition acknowledges the growing place of mobile phones in our daily lives.

Both physical and mobile driving licences are complementary. From a security standpoint, the physical driving licence brings additional physical security features to complement the cybersecurity protections implemented on the digital parts. From the user experience standpoint, even with the obvious growing usage of mobile, some particular cases of equipment unavailabilities (battery ran out, lost or broken) can be complemented by the physical driving licence.

Therefore, Eurosmart calls to amend the proposal accordingly. While Eurosmart strongly supports the ambition to mandatorily issue mobile driving licences set forth in article 3(4), physical driving licence shall also be maintained and still be mandatorily delivered to citizens.

Leveraging the need to maintain a physical driving licence is rather amongst the following:

- (1) Inclusivity-wise, it should be taken into account that a significant number of users are unlikely to adopt a digital driving licence;
- (2) Cross-border recognition of digital driving licences does not happen with countries outside the EU which do not deploy the means to read mDL; in case of mobile lost, theft or broken, a physical document turns very useful;
- (3) For mDL reissuance or portability onto a new device, a physical driving licence will facilitate the transition phase;
- (4) eIDAS envisages using external token hardware to reach level 'high'. Physical DL equipped with a chip can be used as an additional factor leveraging the level assurance for eID provisioning;
- (5) In combination with the EUDI wallet, the physical DL can also serve as an authentication factor.

New physical driving Licence format

Eurosmart very much welcomes the ambition of the proposed text to move forward the deadline for mandatory replacement of existing physical driving licences on the field within Member States by the harmonised EU driving licence from 2033 - as envisioned by the previous directive - to 2030. This will substantially contribute to increase the level of security of driving licence.

Homogeneous and high level of security of all identification documents across Europe

Driving licences, such as national identity cards, residence permits or passports, are identification documents widely used by European citizens to prove their identity in their everyday life. In particular these identification documents can be used for the KYC (Know Your Customer) process, where financial operators should verify the identity of individual before completing any financial operations or bank account opening. This identity verification is instrumental to fight money laundering and terrorism financing.

Over time, the EU legislation has substantially increased the level of security of national identity cards, residence permits and passports while at the same time aligning them. These provisions require that they are all mandatorily equipped with a secure chip containing the holder's identity, portrait and fingerprint. This strategy is twofold. First, making document forgery and counterfeiting harder thanks to the secure chip, which prevents any attempt - secondly avoiding creating a loophole - a category of identification document with a lower level of security - which would instantaneously become the weakest link.

Therefore, Eurosmart calls for mandatorily including into the EU driving licence a secure chip containing at least the identity and portrait of the holder. By doing so, the level of security of the driving licence would be commensurate with the one of national identity cards, residence permits and passports.

Leverage on international standards for the technical specification of chip-based driving licence instead of a non-standard specification

Eurosmart would like to highlight that the content of Annex I-Part B, which defines the specification for the chip introduced as part of the physical driving licence, is neither state of the art any longer nor does the specification enable interoperability between Member State implementations.

The Part B makes use of several references to specific editions of a standard, e.g., ISO/IEC 18013-3:2009, which are outdated and have been replaced with newer editions. The referenced outdated editions are no longer available via the ISO/IEC webstore and, therefore, should be replaced with references to the current editions of these standards. In addition, the evolution of these standards and the state of the art should be reflected in the revised Directive:

- Part B.1 clause 5 (2)(a) requires a security mechanism to access the data in the chip the implementation of Basic Access Protection (BAP) with an MRZ in the interest of interoperability with electronic Machine-Readable Travel Documents (eMRTDs) such as ePassports. From a security point of view, BAP is not state of the art any longer, and ICAO is in the process of deprecating the usage of BAP (called BAC in ICAO's eMRTD specifications) for eMRTDs. For eMRTDs as well as driving licences, PACE is standardised and used instead of BAP / BAC and provides better security as well as usability for officers: a short string instead of the

MRZ is sufficient as input which can also be typed in manually if optical recognition should not work or is not supported. Eurosmart recommends to deprecate the BAP protocol for EU driving licences and mandate the implementation of the PACE protocol as specified in ISO/IEC 18013-3:2017/Amd 1:2022 for driving licences. Please note that ISO/IEC 18013-4:2019 specifies test methods for driving licences supporting the PACE protocol.

- Part B.1 clause 5 (2)(b) conditionally requires as security mechanism to access more sensitive data in the chip the implementation of Extended Access Control (EAC), and Part B.2 item 11 references the Technical Guideline TR-03110 for the EAC specification. The 2017 edition of ISO/IEC 18013-3 has adopted the EAC protocol and standardises its interoperable use for driving licences in conformance with BSI TR-03110. In addition, ISO/IEC 18013-4:2019 specifies test methods for Driving Licences supporting the EAC protocol. Eurosmart recommends to replace the reference to the Technical Guideline TR-03110 with reference to ISO/IEC 18013-3:2017 clause 8.6 and Annex D.
- Part B.1 clause 5 (3) refers to the Public Key Infrastructure (PKI) to Annex A of ISO/IEC 18013-3. For interoperability reasons, the PKI including certificate formats and hierarchies as well as revocation mechanisms, need to be specified in detail, while Annex A of ISO/IEC 18013-3:2009 as well as 2017 only describe general mechanisms. ISO/IEC JTC 1/SC 17/WG 10 will most probably revise this Annex A and specify the PKI mechanisms in detail in conformance with the detailed specifications for the PKI for mobile driving licence applications in ISO/IEC 18013-5:2021 Annex B. Please note that a detailed PKI specification seems also to be required for the interoperability of the QR code option introduced in Article 4 of the directive. Eurosmart recommends to add a detailed PKI specification and align with ISO/IEC JTC 1/SC 17/WG 10 to keep this specification and the revised ISO/IEC 18013-3 Annex A in conformance. In addition, an EU certificate policy should be prepared to clarify the governance of the PKI and support cross-recognition, such as the ones already available (visible digital seal on Schengen visa or electronic travel documents).
- The Directive relies on the portrait image as primary means to verify that the person presenting the driving licence is the rightful holder. To support this verification, provisions for the portrait quality should also be added in conformance with ICAO's requirements for the portrait in eMRTDs. Eurosmart recommends to add provisions for the portrait quality in conformance with the relevant provisions in the ICAO Doc 9303 part 3 clause 3.9.1.

In addition, some minor issues apply:

- Annex I- Part A1 item (3) uses the statement "microchip or similar computer device". It is unclear what a similar computer device may be. Therefore Eurosmart recommends to delete "or similar computer device".

Physical driving licence with QR code

In article 4 of the directive, a QR code is introduced as additional machine-readable technology. Eurosmart recommends to specify the barcode symbology (QR, Data Matrix etc.) in the implementing act (as provided for in article 4(7)) based on the requirements for the data. In addition, Eurosmart recommends to use the term 2D barcode instead of QR code in the Directive.

Clarify the link between the mobile driving licence and the EU Digital Identity Wallet

The revision proposal frequently refers to the European Digital Identity Wallet, which has not yet been formally adopted by the European co-legislators, and whose necessary technical specifications for proper implementation are not yet available. Eurosmart would like to invite the Commission to provide more consistent provisions on how the connection between the two texts is envisaged at this stage. To improve legal certainty, Eurosmart urges the Commission to explain how the planning of the two texts, including implemented acts, will be interconnected.

In addition, some provisions of Annex I-Part C are awkward as they seem not to be a requirement for the mobile driving licence itself but rather for the wallet being currently designed within the eIDAS expert group (bullet (6)). Eurosmart suggests to remove this requirement and forward it to the eIDAS expert group.

Business model of the mobile driving licence

From a cost perspective for the user and for inclusivity, physical and mobile driving licences should be treated equally. Eurosmart supports the principle of ensuring that Road Safety authorities can charge for their services. This is important to ensure that the authorities have the necessary resources to maintain and update the system and guarantee the safety and security of all citizens.

Security of the mobile driving licence

Eurosmart strongly believes that bringing the same level of trust across driving licence formats requires careful attention to security standards. It is essential to ensure proper articulation with the specifications of the EU Digital Identity Wallet.

Private sector access to mobile driving licence

Eurosmart acknowledges that relying parties from the private sector will benefit from verifying these mobile driving licences, not only law enforcement actors. Eurosmart requests clarification on how this will be implemented in the text, including ground rules and common services for access by the private sector, such as setting up a trusted list of issuing authorities, access to validity checks, and potential conditions to get authorised.

The specification of the mobile driving licence contains substantial ambiguities which could impede successful deployment and interoperability

The way the specification of the mobile driving licence leverage ISO/IEC 18013-5 is unclear

Eurosmart very much welcomes the proposal to rely on the ISO/IEC 18013-5 standard for mobile driving licence (Annex I-Part C bullet (2)), which has successfully been deployed in the United States. However, the content of the whole Annex I-Part C brings substantial confusion regarding the specification of the mobile driving licence. It is not clear whether the requirements describe features present in ISO/IEC 18013-5 or if they supplement or modify ISO/IEC 18013-5 standard. In its current

shape, the content of Annex I Part C is very likely to lead to (1) incompatible implementations of mobile driving licence across Europe, and (2) implementations of mobile driving licence which are not in line with ISO/IEC 18013-5, because of the confusion it brings. In order to remove any confusion, Eurosmart has the following recommendations.

1. **Reference to ISO/IEC 18013-5 should be complemented with reference to the upcoming ISO/IEC 23220-4 for optional features (e.g. mdoc reader authentication)**
2. **Establish clear links between the requirements enacted in Part C and the ISO/IEC 18013-5 standard.**

Part C should clearly indicate which features of ISO/IEC 18013-5 should be supported. According to the content of Part C, this list shall contain the following:

- server retrieval (§9.2 of ISO/IEC 18013-5);
- mandatory mdoc reader authentication (ISO/IEC 18013-5, section 9.1.4 and upcoming ISO/IEC 23220-4, section 7.1.20);

In addition, **to remove ambiguities, the wording used in ISO/IEC 18013-5 should be reused. Using other wording introduces substantial confusion.** In particular, Eurosmart recommends to:

- replace the wording “verifiable data” by “mdoc pursuant to ISO/IEC 18013-5”;
- clarify that the information listed in Part D shall be nested within a mdoc pursuant to ISO/IEC 18013-5;
- Replace the wording “pointer” and “single-use token” by “token to retrieve data from a server pursuant to ISO/IEC 18013-5”;

Pursuant to bullet (5) 4th paragraph and Part D, information specific to the European mobile driving licence is introduced. **In order to fit within the ISO/IEC 18013-5 framework, the following clarifications should be brought regarding this information:**

- The information listed in Part D shall be included within a mdoc pursuant to ISO/IEC 18013-5 using a dedicated Namespace pursuant to ISO/IEC 18013-5.
- The value assigned for this Namespace shall be indicated;

Also, in order to support the implementation of this provision, a technical document detailing the encoding and structure of this information will be needed. Eurosmart would be more than happy to contribute to the preparation of this technical document.

Some wording used throughout Part C (e.g. “single-use” in single-use token) seems to suggest technical implementation going beyond the technical standards. Such wording should be avoided.

3. **The scope of the mobile driving licence is unclear**

The content of Annex I Part C is unclear whether mobile driving licence should support (1) “server retrieval” or (2) “device retrieval”, or both. In addition, it is unclear whether for server retrieval the WebAPI and / or the OIDC solution standardised in ISO/IEC 18013-5 is selected. One of the two modes of implementation, server retrieval or device retrieval, is sufficient to allow inspection of driving rights: the device in charge of the inspection shall support both modes to accommodate any kind of mobile driving licence, a bit in the same manner as for electronic travel documents. Eurosmart believes that in accordance with ISO/IEC 18013-5, only “device retrieval” should be mandatory, while “server retrieval” should remain optional. Each Member State should be free to implement the “server retrieval” mode in the mobile driving licence it delivers but should not be forced to support it if it deems this mode is not suitable. In particular, some Member States may be reluctant to opt for “server

retrieval” because of its shortcomings: privacy issues when disclosing information, complexity in the back-end system of the issuing authorities, and above all the lack of resilience in case of cyber-attacks, as the verification relies on the availability of the network and the back-end system of the issuing authorities. Therefore, Eurosmart recommends clarifying that “device retrieval” shall be mandatorily supported by the mobile driving licence, while “server retrieval” is optional. In addition, to enhance interoperability and minimise the implementation effort, Eurosmart recommends to retain only the WebAPI server retrieval option (ISO/IEC 18013-5).

Neither the proposal of directive, nor the Annex I-Part C defines the context of use of the mobile driving licence, namely whether it should be used for an offline transaction (involving a physical interaction between the holder and the reader) or an online transaction, where the holder remotely presents its information. While ISO/IEC 18013-5 is fully relevant for the case of mobile driving licence used in the context of an offline transaction, it is relevant but not sufficient for an online transaction. In that case, supplemental technical mechanisms are needed, which are not defined in ISO/IEC 18013-5 but provided in the upcoming ISO/IEC 18013-7 which relies on the upcoming ISO/IEC 23220-4. Therefore, Eurosmart recommends clarifying the context of use of the mobile driving licence and whether it shall support offline transaction and/or online transaction. In addition, if online transaction is required, compliance to ISO/IEC 18013-7 shall also be required, alongside ISO/IEC 18013-5.

Other technical concerns

Eurosmart has some other concerns regarding the specification of the mobile driving licence described in Annex I-Part C:

- bullet (3) describes the conditions under which the holder is considered the authorised user of the mobile driving licence. For that purpose, electronic identification achieved using any electronic identification means compliant with regulation 910/2014 should be accepted. Eurosmart very much welcomes this proposal, however, the required Level of Assurance shall be clarified. As a driving rights inspection under law enforcement authorities is at stake, the highest level of Assurance (LoA “high”) shall be mandated to avoid impersonation and identity theft: pursuant to regulation 910/2014, a LoA “high” “[...] prevent[s] misuse or alteration of the identity” (article 8(2)c). For this very reason, Eurosmart recommends to require using any electronic identification means compliant with regulation 910/2014 with an authentication of Level of Assurance “high”;
- bullet (3) states that the primary means for identification shall be electronic identification. However, mobile driving licence pursuant to ISO/IEC 18013-5 could also be directly used for identification as it contains the identification data, and the portrait allowing to bind the identification data to the holder in the course of a physical transaction. Some Member States may be willing to rely on this simple approach, and the text should not prohibit it. Eurosmart recommends not to discard this mode of identification, which is very convenient, especially in the course of a physical inspection. Therefore, Eurosmart recommends to reword “The primary means for identification shall be electronic identification” as follows: “electronic identification shall be accepted as a mean for identification”;
- bullet (3) considers the usage of electronic identification means pursuant to eIDAS regulation. These seem more suitable for online transaction, where the holder remotely presents its information, than offline transaction (involving a physical interaction between the holder and the reader), where the portrait could be exploited. This provision brings substantial confusion regarding the context of use of the mobile driving licence: online and/or offline (see former comment). Eurosmart calls for clarifications;

- bullet (5) “Member States shall not consider data valid when it has been retrieved more than 7 days before the time of verification [...]” (last paragraph): this provision sets a maximum time frame of 7 days for refreshing the data of the mobile driving licence. It may be very challenging, especially where several instances of data have to be refreshed and not a single one. Several instances of data are needed to protect privacy of the user (to avoid linking several transactions to the same person) in the case where the mobile driving licence is also allowed to be used for a transaction with the private sector. Usually, in that case a minimum of a dozen of instances is needed. Therefore, depending on whether the mobile driving licence is allowed to be used by the private sector and the targeted level of privacy (the higher, the more instances are needed) - both defined by the issuing Member State - the threshold of 7 days may be more or less challenging. Eurosmart recommends lowering down this threshold to 15 days, and to leave it up to Member States to further restrict this time frame depending on (1) whether or not they allow the private sector to use the mobile driving licence and (2) the targeted level of privacy;
- bullet (5) introduces the option to retrieve data that is not available in the national system by other secure means. While there is nothing wrong with this option in general, the example to retrieve the portrait image from an ePassport seems questionable. The portrait image stored in the ePassport could be rather old, not conform to state-of-the-art quality requirements any longer etc. Therefore Eurosmart recommends to delete this example. In addition, Eurosmart recommends to (1) specify clear provisions for these alternative secure means in an implementing act, in conformance with the provisions for the EUDI Wallet and (2) provide examples in this implementing act, but not in the Directive;
- bullet (6): the meaning of « invalid » for person identification data is unclear and would deserve much more clarity. It may result either from the expiration of person identification data or its revocation. Does it mean that even revoked person identification data should be accepted? Eurosmart strongly recommends to remove the wording “invalid” and restrict it to “expired” only, as revoked person identification data should not be accepted;
- bullet (8): depending on the holder's situation, Member States may decide to impose a face-to-face interaction before the renewal, replacement or exchange of a driving licence. Therefore the provision of this bullet should not impose remote procedures but only allow them at Member States' discretion: “shall” should be replaced by a “may”;
- In Part D, it should be clarified that the country code listed are the codes for the UN distinguishing sign-, in addition ISO 3166-1 country codes are required for the mobile driving licence in accordance with ISO/IEC 18013-5;

Better structure the content of Part C

Annex I-Part C should clearly separate provisions relating to the specification of the mobile driving licence, from those covering policy aspects, i.e., the governance and the management of the mobile driving licence and its infrastructure. These aspects should be clearly identified and gathered. It applies to the following items:

- bullet (3);
- bullet (4);
- bullet (5):

“Competent authorities of the Member States shall be authorised to retrieve the data contained in the mobile driving licences in order to be able to ascertain the driving rights of the holder of the driving licence (verification)”

“Competent authorities of the Member States shall be authorised to access national systems of other Member States. Member States shall ensure that once the data of the licence holder is verified the transmitted data is not retained.”

“Member States shall not consider data valid when it has been retrieved more than 7 days before the time of verification or when the number of the driving licence is included in the revocation list managed by the Member State which issued the mobile driving licence. A revocation list shall contain information on all driving licences that no longer entitle holders to exercise the right to drive.”

- bullet (6);
- bullet (7);
- bullet (8);

In order to support the implementation of this policy, a technical document will be needed. Eurosmart would be more than happy to contribute to the preparation of this technical document.

Leverage as much as possible existing international standards and avoid non-standard implementation

Eurosmart recommends leveraging as much as possible on existing international standards for the implementation of this directive. Standards are available for all the technical features which are foreseen, and those should be considered and referenced as much as possible.

In particular, Eurosmart would like to avoid the reiteration of the situation of regulation 383/2012, where the technical specification was formed out of a set of various references to diverse standards, but the technical specification in itself was non-standard.

The support of international standards allows for international interoperability of EU Driving Licences and readers, i.e.

- for EU Driving Licences to be used also outside the EU and;
- for Driving Licence Readers in the EU to successfully inspect foreign Driving Licences based on these international standards.

Table 1. Recommended international standards:

Annex I - Part B1	ISO/IEC 18013-2	For chip-based driving licences
Annex I - Part B2	ISO/IEC 18013-3	For chip-based driving licences
Annex I - Part B3/§3	ISO/IEC 18013-4	For functional testing of chip-based driving licences
Annex I - Part C	ISO/IEC 18013-5 AND ISO/IEC 23220-4 (upcoming)	For offline transaction for mobile driving licences
Annex I - Part C	ISO/IEC 18013-5 AND ISO/IEC 18013-7 (upcoming)	For online transaction for mobile driving licences
Annex I - Part C	ISO/IEC 18013-6 (upcoming)	For functional testing of mobile driving licences This standard is crucial to ensure interoperability of mobile driving licences across the EU.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.



EUROSMART
The Voice of the Digital Security Industry



www.eurosmart.com



[@Eurosmart_EU](https://twitter.com/Eurosmart_EU)



[@Eurosmart](https://www.linkedin.com/company/eurosmart)

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com