EUROSMART
The Voice of the Digital Security Industry

Eurosmart position paper on the EU Driving Licences Directive

December 2025

Introduction

Eurosmart strongly welcomes the EU Driving Licences Directive, which will enable the migration of driving licences to mobile driving licences.

The migration from physical driving licences to mobile driving licences is a change of paradigm, which requires Member States to carefully understand and assess the workflow currently in place for physical driving licences to adapt it to the digital world.

In addition, this directive only provides high level objectives and leaves implementation up to Member States. This may lead to a fragmented implementation and diverse level of security of the management of mobile driving licences across EU, which could create a loophole. In turn, that loophole could be exploited by fraudsters to unlawfully obtain mobile driving licences and forge individual's identity or create identity.

Therefore, to ensure the successful deployment of mobile driving licences across the EU and to achieve a harmonized and secure implementation, Eurosmart recommends that the European Commission develop a clear guidance to support the implementation of the directive.

The guidance should particularly address:

- the smooth and successful migration to mobile driving licences across the EU;
- a harmonized and secure implementation framework for mobile driving licences within the EU.

In this position paper, Eurosmart provides recommendations to support (1) the successful migration to mobile driving licences across the EU, and (2) a harmonized and secure implementation of mobile driving licences within the EU.

This position follows the previous Eurosmart's white paper of the 31st of May 2023, entitled Revision of the Directive on Driving Licences – Eurosmart's Answer to Public Consultation.

1. Ensure a successful migration to mobile driving licences across the EU

1.1. Identify the workflows within the EU Member States for managing and using physical driving licences

As a first step before introducing mobile driving licences, it is important to have a clear overview of the lifecycle of a physical driving licence and its use, as well as the use cases and applicable legal requirements within the EU Member States.

This step is key to well identify and understand the governance, use cases and constraints ruling physical driving licences in the EU. Moreover, it will help create a common understanding amongst Member States on the lifecycle of physical driving licence.

More precisely the processes and policies for the following operations should be identified and described in the case of physical driving licence:

- issuance, revocation, replacement;
- inspection by law enforcement authorities;
- use for the provision of a service by a relying party (private sector) and whether it is allowed;
- suspension and seizing;
- loss or stolen driving license.

In addition, the governance of a physical driving licence within EU Member States should be described. The authorities in charge of issuance, managing authentic sources, revoking, suspending and seizing the physical driving licence within the EU should be identified.

One of the key deliverables of that step is to clearly identify the (1) lifecycle of the physical driving licence and (2) the authorities and their responsibilities.

1.2. Update the workflows to adapt them to the mobile driving licences

Based on the clear mapping and description of the workflows in place within the EU Member States for managing and using physical driving licences, the impact of digital format should be assessed and the workflows should be updated accordingly.

In particular the following aspects should be duly considered to adapt these workflows:

- unlike physical driving licence, it is possible to have simultaneously several copies of a mobile driving licence;
- unlike physical driving licence, it is possible to invalidate remotely a mobile driving licence;
- new use cases should be addressed such as (1) the change or loss of the device holding the mobile driving licence, or (2) the backup of mobile driving licence;
- the new paradigms such as the risks of massive data collection and non-authorized data processing should be considered, which implies the implementation of data protection mechanisms for instance data minimization and selective disclosure;
- storage in a wallet of the mobile driving licence together with digital versions of other related documents (e.g. vehicle registration card, insurance certificate, etc.) issued by other entities. This will require these entities to be able to manage digital versions of these documents in that wallet but also to identity and authenticate the holder prior to issuance. For instance, this is already the case in France and Germany where the mobile driving licence and vehicle registration certificate can be stored in a wallet on a mobile phone;
- dissociation between the validity period of the digital credential (e.g. a few days, weeks or a year) and the right to drive. This makes the workflow of mobile driving licence more complicated than the physical driving licence.

In that regard, the findings and the final reports from the Large Scale Pilots (LSP) piloting the EUDI Wallet for the use cases of mobile driving licences should be carefully considered:

- POTENTIAL (https://www.digital-identity-wallet.eu/);

This migration will substantially impact the entities holding the authentic sources (database of driving licence holder), as they will have to be connected to a central system to allow the issuance of mobile driving licence. This may be challenging especially in Member States were the entities holding these authentic sources are decentralized (e.g. Germany), while in those where the management is centralized (e.g. Austria, Poland) it would be much easier.

2. Ensure a harmonized and secure implementation of mobile driving licences within the EU

2.1. Management of mobile driving licences within the EUDI Wallet

First, the shape a mobile driving licence will take within the EUDI Wallet framework is not defined in the directive and should be clarified. Eurosmart recommends that mobile driving licences be handled as “electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source” as defined in Article 3(46) of the eIDAS Regulation. This is appropriate, as mobile driving licences are to be issued only by States themselves.

Why is this clarification required?

This clarification is needed so that the relying party accepting a mobile driving licence knows the applicable legal framework, and thus who bears the risk in case the information it contains is wrong. This is key for the relying party to ensure legal certainty, and ultimately to guarantee a large acceptance and use of the mobile driving licence. Classifying mobile driving licence as "electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source" as defined in Article 3(46) of the eIDAS Regulation would provide a protective legal framework for relying parties as it would ensure that the issuer is liable for the trustworthiness of the data within the mobile driving licence. Failing to clarify the applicable legal framework would hamper the acceptance, use of and trust in mobile driving licences by relying parties and thus its uptake.

In addition, there are several ways to manage the credential representing the mobile driving licence:

- **the credential is long-lasting.** In that case the validity status of the credential should be made available to third parties by the issuing authorities (e.g. through CRLs) to allow detection of revoked credentials (e.g. loss of mobile phone, wallet is compromised, mobile driving licence is revoked, etc).
- **the credential is short lived**. In that case, it is not needed to make available any validity status of the credential to third parties. In that approach, each credential representing the mobile driving licence is delivered with a short lifetime and replaced very often.

For both of these approaches, the validity period of the credential is likely not to be aligned with the validity period of the mobile driving licence – representing the right to drive, or they may be revoked before the end of their validity period to be reissued. Therefore it should be clarified whether the issuance of a new credential should be interpreted (1) as the issuance of a new mobile driving licence and thus covered by Article 10 or (2) as a replacement of a mobile driving licence, and thus not covered by Article 10.

Why is this clarification required?

This clarification is needed so that all authorities (issuing and controlling) within the EU as well as relying parties have the same understanding of the validity period of the mobile driving licences. It is instrumental to ensure trust in mobile driving licences. Failing to do so would substantially hamper the acceptance, use of and trust in mobile driving licences and thus its uptake.

Furthermore, for both of these approaches, clarifications and harmonized policies are required. In particular a policy for the management of (1) the mobile driving licence representing the right to drive AND (2) the credential representing the mobile driving licence is needed, covering (not limitative):

- **Procedures and controls for issuance, revocation and renewal** of credential and mobile driving licence encompassing the following aspects:
    - Identity verification of the holder prior to issuance, revocation or revocation of credential and mobile driving licence:
        - should a new identity verification of the holder be triggered?
        - how should it be carried out?
            - physically (face-to-face)?
            - remotely?
            - using the EUDI Wallet and the PID it contains?
            - in the case where attributes not present in the PID are required (e.g. portrait), how to proceed to ensure a consistent security level?
        - with which level of assurance?

        - which conformity assessment (if so) for the identification verification?
    - Binding with the new EUDI Wallet prior to issuance, revocation or revocation:
        - which requirements?
- **Technical security controls** (HSM, etc.);
- **Facility, management, and operational controls** (physical security, IT security, staff, etc.);
- **Lifecyle and lifetime of credential**.

Why are these clarifications required?

These clarifications are needed to establish trust in the mobile driving licence. It is instrumental to ensure trust in mobile driving licences. Failing to do so would substantially hinder the acceptance, use of and trust in mobile driving licences and hence its uptake.

2.2. Case of renewal of change of mobile device

The case of renewal or change of the holder's mobile device should be duly considered. A harmonized policy should be defined to address the situation where the holder of a valid mobile driving licence – representing its right to drive – renews or changes his mobile device (and thus EUDI Wallet) while its mobile driving licence remains valid. This case is highly likely to happen considering the typical validity of the mobile driving licence, the frequency of device renewal (~3/4 years) and the risk of theft.

It may also be useful that such policy includes rules for fraud detection related to mobile phone renewal or change, for example:

- which monitoring to circumvent fraud attempt exploiting mobile phone renewal or changes?
- which actions (tightened screening, etc)?

Why are these clarifications required?

These clarifications are needed to establish trust in the mobile driving licence. It is crucial to ensure trust in mobile driving licences. Failing to do so would substantially hamper the acceptance, use of and trust in mobile driving licences and thus its uptake.

Conclusion

Eurosmart recommends the European Commission to draft a guidance to support a harmonized and secure implementation of the new directive, and in particular of the mobile driving licences.

The preparation of this guidance should be carried out with the national authorities issuing driving licences but should also closely involve digital secure identity industry (e.g. provider of Wallet, etc). Therefore, **Eurosmart recommends the European Commission to establish a dedicated expert group on digital identity, encompassing national issuing authorities and digital secure identity experts to draft this guidance. Eurosmart stands ready to support this effort.**

In order to avoid any risks of fragmentation, Eurosmart also recommends having this guidance available as soon as possible, as several Member States are already working on deploying mobile driving licence, as it is an important use case of the EUDI Wallet (e.g. France).

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 @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 471 34 59 64 | mail Contact@eurosmart.com