Electronic driver's licenses: Driving towards the future

Mario Stoltz, Product Manager, Secure Card Solutions

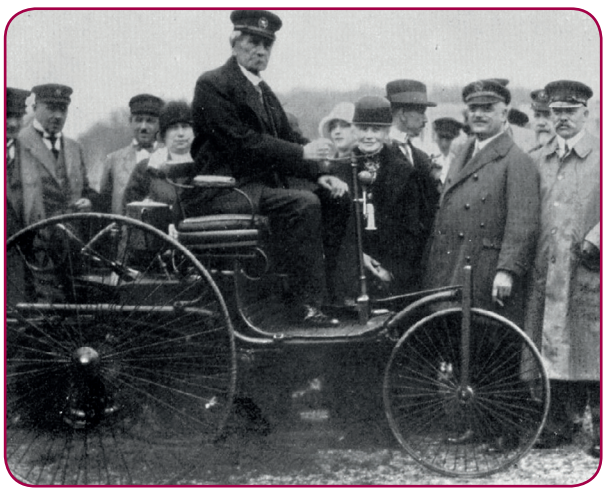
How electronic driver's licenses (eDLs) promise to transform the driving experience

ABSTRACT

Driver's licenses for motor vehicles have been around for more than 125 years. With the expansion of traffic and personal mobility across national borders in the 20th century, the use of driver's licenses has expanded and gained importance beyond the national scope. In some countries, driver's licenses (eDLs) are also used as identity documents or for age verification, inside and sometimes outside the issuing country. The emergence of electronic driver's licenses (eDLs) – documents with an embedded electronic component – offers benefits to everyone involved. For document holders, eDLs can save time and effort by making it possible to interact with the authorities from a home PC or mobile phone, where before they had to line up at a brick-and-mortar office. The issuing authorities can increase their productivity and reduce damages from fraud. Inspecting officers can focus on interacting with the citizen, while letting electronic equipment perform semi-automated background checks. For the future of personal mobility, eDLs offer new use cases that increase convenience and security.

ORIGINS

A driver's license is a document issued by official authorities. It provides evidence that the holder of the license has official permission to operate some kind of motor vehicle – a car, truck, motorcycle, or bus – on a public roadway.



The first driver's license was issued to Karl Benz, the inventor of the modern automobile, in 1888. Because the noise and smell of his motor car led to complaints, Benz requested and received written permission to drive his car on public roads.

The first country to mandate a driver's license and driver testing was Prussia in 1903. In 1910, the German government began requiring that drivers be licensed, and established a system of driver training and tests. Many other countries in Europe became active in similar initiatives around the same time. Also in 1910, the first licensing law for professional chauffeurs of motor vehicles went into effect in New York. Over the course of the 20th century, driver's licenses (DLs) were adopted worldwide. Since 2005, there has been an ISO standard for driver's licenses, ISO 18013. In 2009, this standard was extended with specifications for an electronic driver's license (eDL).

In countries that have no national identification cards, driver's licenses are sometimes used as a form of citizen identification. The United States is the most prominent example, but there are other countries that fall into this category. In many places throughout the world, several types of document – including driver's licenses – are used for private-sector citizen identification.

GROWING TREND

A number of countries have already issued eDLs.

Several of these implementations follow national specifications, while some comply with the ISO 18013 standard. The following is a partial list:

- El Salvador (late 1990s)
- Several states in India (2003, contact chip card)
- Japan (2007, contactless chip card)
- Morocco (since 2007, contactless chip card)
- Mexico (phased rollout began in 2007)
- Indonesia (2009, contactless chip card)
- Queensland, Australia (2010, contact chip card)

A few EU countries have issued eDLs that follow the European Commission's directive EC 383/2012:

- Croatia (May 2013)
- France (September 2013, with a validity period of 15 years)
- Ireland (October 2013)

STANDARDIZATION

Regional agreements about driver's licenses have existed for some time. Especially within the European Union, there have been joint regulations about classes of driving permissions, the physical appearance of, and the data set used on printed driver's licenses.

ISO/IEC 18013 is a relatively new series of international standards for driver's licenses. It covers various aspects of licensing, including security features. In particular, it addresses the use of embedded secure microprocessors, the data sets they use, and the associated protocols for data access. The table below indicates several configuration options for eDLs compliant to the ISO/IEC 18013-2 standard.
The size of the data set and the biometric data in an ISO 18013-compatible driver's license are variable.

Configuration options for ISO/IEC 18013-2 eDLs

eDL chip configuration	Access method	Cryptography	Biometrics in data set	Remarks
Basic	BAP 1	112-Bit DES (2 k 3DES CBC mode), SHA-1	License-holder portrait	Can be made compatible with BAC ePassports for use with the same inspection equipment
	BAP 2	AES-128, SHA-1	May include (each is optional) license-holder portrait, signature, fingerprint(s), iris scan, or other biometric	Any AES cryptography is significantly stronger than DES
	BAP 3	AES-192, SHA-256	Optional biometrics as above	Discouraged due to known attack reducing strength of AES-192 algorithm
	BAP 4	AES-256, SHA-256	Optional biometrics as above	
High-end	EAP	2 k 3DES, RSA1024..3072 or ECC160..512, higher SHA	Optional biometrics as above	Can be made compatible with EAC ePassports for use with the same inspection equipment

The standard is very flexible in this respect – the inclusion of any biometric data is optional and at the discretion of the implementing country. The standard specifies several access methods so as to provide greater flexibility to the implementers. Any access method can be combined with any biometric data stored on the chip.

For the sake of interoperability, it makes sense for neighboring countries to agree on joint access methods and to define compatible data sets and biometrics, especially in areas where there is heavy cross-border traffic. This way, police officers and other officials can inspect the driver's licenses of other countries using the same reader equipment.

The BAP 1 access method from ISO 18013 is compatible with the BAC access protocol used in electronic passports. With an appropriate visual arrangement of the items on the front of the driver's license, existing border-control inspection devices can also inspect a driver's license using the BAP 1 access method*. Furthermore, work is underway to integrate more authentication methods into the ISO 18013 standard, so as to increase interoperability with the existing infrastructure for ePassport and eID inspection.

USE CASES OF A DL/EDL

Driver's licenses are used in a number of different scenarios. Every country is a little different, and this is not an exhaustive list, but the major use cases are summarized in the subsections below.

Enrollment

Before a driver's license can be issued, the identity of the applicant is established, along with their right to be the holder of a (particular class of) driver's license. This is the first step in the document's life cycle.

Applicants typically have to perform specific actions, such as appear at an enrollment office in person, and they usually have to provide a baseline of biographical and biometric data (date of birth, height, weight, coloring). Applicants are also typically asked to show proof of successful driver training, and may be given a written exam, an actual driving test, or both. Showing supporting identity documentation is another part of the process, since a government-issued identity document, such as a birth certificate, may act as a breeder document for the driver's license.

The amount of data collected during enrollment depends more on the business rules of the issuing entity and less on whether the document issued is a DL or an eDL. Applying for an eDL may require one or two extra steps, such as having to generate keys and digital certificates that are to be stored for an eDL, but, in general, these extra steps don't require operator action and, as a result, don't generate significant additional effort.

Issuance

Once the eDL has been produced and personalized (two steps that are beyond the scope of this paper), the finished document needs to be transferred from the issuing authority to the intended holder of the license.

The step that immediately precedes the transfer, called activation, can be used as administrative proof that the handover has occurred, noting the official, the licensee, and the time and location of the handover. This improves the quality of data and organizational accountability. Data analysis can be used to detect abnormalities (like a potentially corrupt officer producing an improbably high number of documents, or documents with statistically notable properties).

Roadside inspection

A roadside inspection of a driver's license can have various purposes. As a policing action, roadside inspections are subject to national law. The legal and practical purposes may vary from country to country,

*) See our white paper "Preventing fraud in ePassports and eIDs" for further reference.

but there are some general reasons, valid in most geographies, for performing a roadside inspection:

- To determine whether the driver has a license (with appropriate authorization for the vehicle)
- To read attributes from the driver's license to decide if further investigation is called for (compare residence with location of inspection, check driver age, etc.)
- To identify a driver and check his or her name against a list (e.g. search warrants)

Having to read the printed information on a traditional driver's license prevents the inspecting officer from doing other things, like watching the driver's face, looking inside the vehicle, or asking questions with full concentration.

However when the license is equipped with an electronic component, at least part of the inspection can be performed automatically. If a network connection is available at the inspection site, the examined device can connect to a local or remote host computer and perform automated background checks. Responses can be sent to the inspection officer using an open or covert method (e.g. through vibration or audio feedback to an earphone). If the inspection takes place in a remote location without network access, the inspection device can still perform basic local checks. This is where the electronic component in the license can play up its strengths. Having a secure microprocessor embedded in the document provides secure electronic communication to the reader and secure storage of sufficient data to make offline inspection meaningful.

Automated background checks can include matching against known documents or databases, and against document status (e.g. declared lost or stolen).

If the inspection terminal has a camera, a biometric match between the facial image stored on the card and the driver can also be performed. More sophisticated checks can cover probabilistic and statistical methods (e.g. the probability of a certain individual driving a particular car in a particular location and in a particular direction at a particular time). Such checks can be automated and performed within seconds when using an eDL and inspection equipment with a GPS module and a network connection. Having the ability to perform automated inspections can make officers more productive and more efficient.

Rental-car inspection

When renting a car, drivers typically need to show their license to the rental-car agent. This is the case both for classical car rental as well as for car sharing. The main incentive for a rental-car company to actively check authorization is cost – that is, the cost of liability control and enforcement of insurance policies.

For marketing purposes, many rental-car companies issue loyalty cards to their returning customers. These cards are used as an alternative or additional means of identification (depending on the business rules or legal boundary conditions of the respective geography), and to prove special status as an identity attribute.

The use of eDLs can help rental-car companies simplify their administrative processes by letting them combine the existing use cases of identification, proving authorization (right to drive), and customer status. Third-party information cannot be saved to a government-issued eDL document, so customer status information needs to come from a database. Linking the identity of an eID to a database is simpler and less prone to error than with traditional documents.

Offline loyalty cards may still have a place in some marketing schemes (since they can provide customers with useful information, such as a contact telephone number), but the customer-status attribute can be automatically assigned to the customer after eDL inspection, whether the customer shows the loyalty card or not.

The process of eDL inspection and linking to a rental-car company's database can also be automated, so the transaction can take place at a self-service kiosk or even inside the car itself. Manual inspection of DL/eDL includes an implicit biometric check, since the rental-car agent can match the picture on the card to the person presenting the ID, but this is a process that may not always be carried out in a consistent or credible way. Automated inspection equipment, mounted in a kiosk or inside the car, can be equipped with second-factor authentication, such as a camera or fingerprint reader for biometric authentication, or a secure keypad for PIN/password authentication, and thereby increase the reliability of these checks.

Automated in-vehicle inspection

The steady increase in automotive electronics has brought new levels of computing power and, with it, an opportunity to rethink traditional concepts of ownership and operation. For a long time, individual automobiles have been associated with individual owners, and operation of the vehicle has relied on a physical key. ("Mom, can I have the car keys tonight?")

The one-to-one relationship between car and owner/driver has, in some instances, begun to dissolve. Short-term rentals and car-sharing programs have become popular in a number of places, especially urban areas, and many of these set-ups involve electric vehicles. Authentication and identification technologies can help manage the questions that come with these programs: Who is plugging an electric car into the loading station, and who pays the loading bill? If the car is used as an electricity buffer for the grid overnight, who receives a refund from the utility company, and how is the related data stored?

As automotive computing power increases, it's conceivable that by, say, 2020, an automobile could interact with a driver in a number of ways:

- The engine only starts if a valid eDL is presented. The driver's identity is logged in the car's black box. This could be an optional process that is sponsored by auto-insurance companies, offering lower rates to drivers who are identified by the car (as opposed to "unidentified" drivers).
- The car's features are scaled according to driver privileges. For example, drivers under a certain age or with a driver's license that is less than two years old might only be able to access reduced engine power or have a speed limit enforced by the car's systems. These drivers might also be blocked from having the volume of the entertainment system above a certain level while driving. More experienced drivers, on the other hand, would be able to access the vehicle's full performance and features. Such mechanisms could be enforced by an issuing state to reduce the number of traffic accidents, or sponsored by auto insurers.
- Payment information might be loaded into the car by swiping a valid means of contactless payment (e.g. contactless credit card, or NFC-based payment scheme on a mobile phone). This could be an optional feature promoted by the operators of road tolls, as a way to offer lower rates to drivers whose cars support automated billing of toll fees. Versions of these auto-payment schemes are in place today. For example, the congestion charge in London requires drivers to accept automated billing. At present, this kind of automated billing is only enabled over the Internet, in kiosks, or in shops. It would add a level of convenience if drivers could authorize payments directly, when entering the car, without prior registration.
- Payment schemes could also be used for parking fees or traffic fines. Rebates could be offered to drivers who accept automated billing. The benefit to operators would be simplified administrative processes compared to present-day invoicing.

Driver's licenses tend to have fairly long lifetimes. Designs tend to stay in place for several years. For example, a new design of a national driver's license, released in 2015, would likely be used for new cards until at least through 2018.

Most national driver's licenses are valid for ten years, and even more in some countries. That means the 2015 design could still be around in 2028. It's difficult to forecast what, exactly, personal mobility

will look like in the future, but it's clear that today's authentication methods and file systems need to be designed with future use-cases in mind. Doing so makes the document more useful to consumers, and helps safeguard the infrastructure investment.

Private-sector use

In some geographies and in some circumstances, DLs (and consequently, eDLs) are used as means of identification. This is particularly the case where there is no or no widespread ID card or other form of government-issued identification document that is both portable and easy to inspect.

Unless such secondary use as an ID document is explicitly intended by the issuing entity, it has to be taken into account that the DL or eDL is not created as an identity document. Its purpose is not to prove citizenship, age, or residence. A DL or eDL proves that an individual with the referenced identity parameters has the right to drive a motor vehicle under the legislation of the issuing authority. It is a proof of attribute and not a proof of identity. Normally, a driver's license is not a root document for identity, but identity data contained in it is derived from a separate breeder document.

The role a DL or eDL plays depends on legal boundary conditions and choices made by the implementing state:

- In places like the United States and the United Kingdom, where the state does not issue a separate national ID document, an eDL can also be a de-facto eID document. Besides serving its main purpose as a driver's license, the eDL can also become an official document with online authentication capability and support for other applications. The security and credibility of an eDL solution for such purposes can typically match that of a national eID card.
- For implementing states that also issue a national eID document, there is a need to clearly define use cases for both documents. In principle, both documents can be issued to equal standards of security and quality, and with equally current data. However, this requires close alignment of issuing agencies (e.g. ministry of home affairs and ministry of transport). In practice, existing national law will set the framework for how each of these documents can be used.

It's important to keep in mind that a DL or eDL may not, depending on national conditions, deliver as high a level of data quality as a national ID card or passport. In many countries, it is possible to use an ID card as a breeder document for the issuance of a driver's license right up to breeder document's date of expiration. As a result, the identity information on the DL document may be as old as the validity period of the underlying national ID document (often 10 years) plus the life of the DL document.

Switching to an electronic driver's license can help ensure that identity data is more up to date, since the enrollment and issuance processes are likely to reference a qualified official database for verification. This means that the quality of identity information on an eDL will be as good or nearly as good as it is on a passport or national ID card. Also, it is relatively easy in an eDL scheme to support document verification by offering tools or a website that can be used by the private sector.

RELATED DOCUMENTS

In most geographies, motor vehicles must be registered with public authorities before operating on public roads, and a technical inspection may be part of the registration process.

The vehicle registration (VR) is typically a paper document issued to the vehicle owner. Similar to a DL, a VR is an attribute document. The related identity or breeder document is the chassis number permanently fixed to the vehicle. Databases for the issuing agency form a supporting structure to verify and validate registration and type approval processes.

VRs can be equipped with an embedded secure microprocessor that adds security and makes the document easier to issue and use. Various countries are considering or have already started to issue electronic VRs that are permanently attached to the vehicle (for example, in the form of windscreen or window stickers). Because VRs are so closely related to DLs, and are often issued by the same organization, it often makes sense to migrate both documents to electronic format at the same time.

Besides VR documents, there are other opportunities for synergy with eDL programs. This includes electronically readable license plates for automobiles. In many countries, license plates are read optically, by cameras, at a range of several to many meters.

The license number is used for road tolls, to enforce speed limits, to provide inner-city access, and more. Whenever a car is stopped by the police, the license number is usually checked against a database of stolen vehicles and search warrants. However, a license plate is easily forged. Criminals are known to copy license plates of other, unsuspicious vehicles and use these to move within the country or to smuggle stolen vehicles across borders. Integrating electronic tags into license plates is a step that some countries are starting to consider. Using secure elements to add a layer of security can make it much more difficult to forge license plates. The information on the tag matches information in the VR document and can contain certain data that is very difficult to fake. Issuing agencies that already have eIDs in place can link the license-plate data to the back-office system.

By making the eDL part of a broader scheme that includes vehicle registrations and license plates, the issuing agency can create multiple opportunities for administrative simplification and can leverage the investment and migration effort to serve more than one purpose.

SECURITY CONSIDERATIONS

There are more than a billion automobiles on the road today (including cars, cargo vehicles, and buses), and nearly as many licensed drivers.

Many aspects of motorized road traffic offer attractive business cases to criminals and crime syndicates, and this has given rise to well-established black markets for fraudulent and forged documents. Examples of illegal activities include:

- "Helping" motorists that have lost their driver's license due to traffic violations
- "Legalizing" stolen vehicles by producing fake registration papers
- Providing illegal migrants with fake driver's licenses that serve as identity papers

These criminal businesses continue to thrive because traditional documents are relatively easy to counterfeit. The possibilities that electronic documents offer for automated inspection and online authentication give governments a way to considerably reduce or even eliminate document fraud and forgery.

ADMINISTRATIVE SAVINGS

Transitioning to eDLs can simplify enrollment and issuance. Application forms can be shorter to fill out or even eliminated, and online services can save time and effort because applicants don't have to visit an office or wait in line to apply in person.

For the issuing authority, the benefits include increased quality of data capture and better administrative processes. When an eDL is introduced as a standalone electronic document, the administrative processes differ only slightly from those used with a paper document. Using eDL data as the source for other electronic documents can prevent errors in typing and copying, reduce the amount of duplicated work, and increase employee productivity.

IMPLEMENTATION COSTS

If the driver's license is already a plastic card, adding a chip is not a major cost driver. Integrating a secure microprocessor and antenna to an existing card typically increases cost by about 30%. The exact figure depends on the specific features of the existing driver's license.

From an administrative standpoint, all that's needed to support eDLs is an extension of the agency's existing computerized databases and management systems. Specialized consulting companies can help manage this process and scale the system extensions correctly.

The inspection systems used to authenticate eDLs can be tailored to specific requirements. There are specialized inspection devices that target law-enforcement agencies. In many cases, though, all the technology required to inspect an eDL with a contactless interface is already included in smartphones equipped with an NFC interface. The smartphone's camera can be used for an optical check of security features, and for capture of the machine-readable zone to derive access parameters. The smartphone's CPU is typically powerful enough to compute the necessary inspection checks, and the phone's network link provides interoperability to services and databases, either locally (e.g. police car via WLAN) or remotely (e.g. central server via GPRS). The smartphone has to be equipped with a dedicated

application and must store access keys securely. In addition, the back-office systems need to provide a secure access server to process system queries relating to inspection. However, even with the cost of developing these features, using smartphones as the basis of the inspection system can minimize the start-up investment.

Once an eDL system is in place, the issuing authority can use the system for online driver authentication. The system can also be extended to provide online services to license holders. Today, actively providing online services is often outside the scope for many of the public authorities issuing driver's licenses. However, today's young people are heavy users of online services, and there is likely to be greater demand for online services in future.

Building meaningful online services around an electronic document such as an eDL can be a great opportunity, since a well-designed online presence can offer more direct and more effective ways to interact with citizens. On the other hand, poorly designed and poorly supported online services can be problematic. They can quickly cause user frustration and make the administration look inept in the public eye. Services that don't live up to public expectation can also prompt the press to focus negative attention on the responsible agency, and that can cause further problems.

SUMMARY

eDLs present a significant opportunity for issuing authorities to provide meaningful services to motorists. At the same time, these new licenses can simplify administration, provide higher-quality data and services, and can make organizations more efficient. Compared to traditional licenses, eDLs are easier to inspect. Inspecting officers can focus on their interaction with the citizen, letting the inspection terminal handle the task of authenticating the document. This makes document inspection faster and easier for everyone.

eDLs also support new eServices, such as at-home online services, which save citizens from waiting in long lines at authority offices, filling in paper-based forms, and waiting for response letters. Automated services that can be accessed from the car or the roadways are also possible. These can be national projects, but can also be supported on regional and even municipal levels.

The new ISO/IEC 18013 standard for eDLs provides a framework for interoperability beyond national borders. Document designs typically need to be updated every few years, and this presents a good opportunity to transition to electronic-enabled formats. The added investment of issuing an eDocument over a traditional document is easily offset by the many benefits that these new designs have to offer.

ABOUT NXP

Based on trusted security, a complete product portfolio and the best contactless performance, NXP is the leader in the overall ID market as well as in key market segments such as transport ticketing, eGovernment, access, infrastructure, RFID/ authentication, payments, and NFC. NXP provides the entire ID market with end-to-end solutions, enabling customers to create trusted solutions for a smarter life.

Sample eDL IC configurations

Card configuration	Chip memory (data set)	Chip access method	Biometric data	Crypto-graphy	Use case	Benefit
Basic	16 kB	BAP1	License-holder portrait (10 kB)	112 bit 3DES	Driver authentication (face recognition)	Automated inspection, forgery protection
Mid-range	24 kB	BAP4	License-holder portrait (15 kB), two fingerprint minutiae (2 kB)	AES-256	Driver authentication (face recognition), match-on-card of fingerprint minutiae	Automated inspection with higher recognition rate, forgery protection
High-end	64 kB	EAP	License-holder portrait (15 kB), two fingerprint images (30 kB)	ECC 244	Driver authentication (face recognition), match-on-card of fingerprint image online authentication function	Automated inspection with higher recognition rate*, forgery protection, citizen online services, meets security requirements for high-end national eID schemes

*) An EAP fingerprint reader is less expensive than one based on BAP4 because there's no need for minutiae extraction in the reader device

Date of release: June 2014
Document order number: 9397 750 17570
Printed in the Netherlands