USE CASE 2
DRIVING LICENCES

A Use Case and Issue Brief
Prepared by CIPIT

Strathmore University
Centre for Intellectual Property and Information Technology Law

01

BACKGROUND

Driving licences are connected to freedom of movement. They also enable earning a livelihood for many drivers and those who carry out tasks that sometimes require them to drive. In many low- and middle-income countries where there are high rates of unemployment, the ability to drive a vehicle increases one's employability. For public agencies charged with transport and safety, driving licences are a means of regulating driver behaviour and increasing transport safety. With advancement in road networks, driving licences enable people to drive across borders where they are recognised in more than one country.

Driving licences are target use cases for countries implementing digital identity (DID). Almost all countries already have systems for driving licences. In most, driving licences are legitimate identity documents for day to day transactions. Driving licence databases are being digitalised and linked to the foundational ID.

It should be noted that, unlike some other examples of ID such as national IDs and public healthcare IDs, in developing countries the driving license may not be a document that is widely attainable. A prerequisite for obtaining a driving license is the ability to pass a driving test, and access to a vehicle is not widely available to lower income individuals. Accordingly, this use case disproportionately impacts higher income demographics.

JUSTIFICATIONS FOR THE USE CASE

Rationale for digitisation of driving licences include:

1. Have a register of all drivers

2. Keep records of driver behaviour

3. Add important relevant information to the driving licence e.g. blood group and emergency contacts in case of an accident

4. Increase road safety by rewarding good drivers and punishing bad ones

5. Harmonise driving licences across regions such as East Africa Community

DATA INVOLVED IN THE USE CASE

The data that are collected for digital driving licences may include:

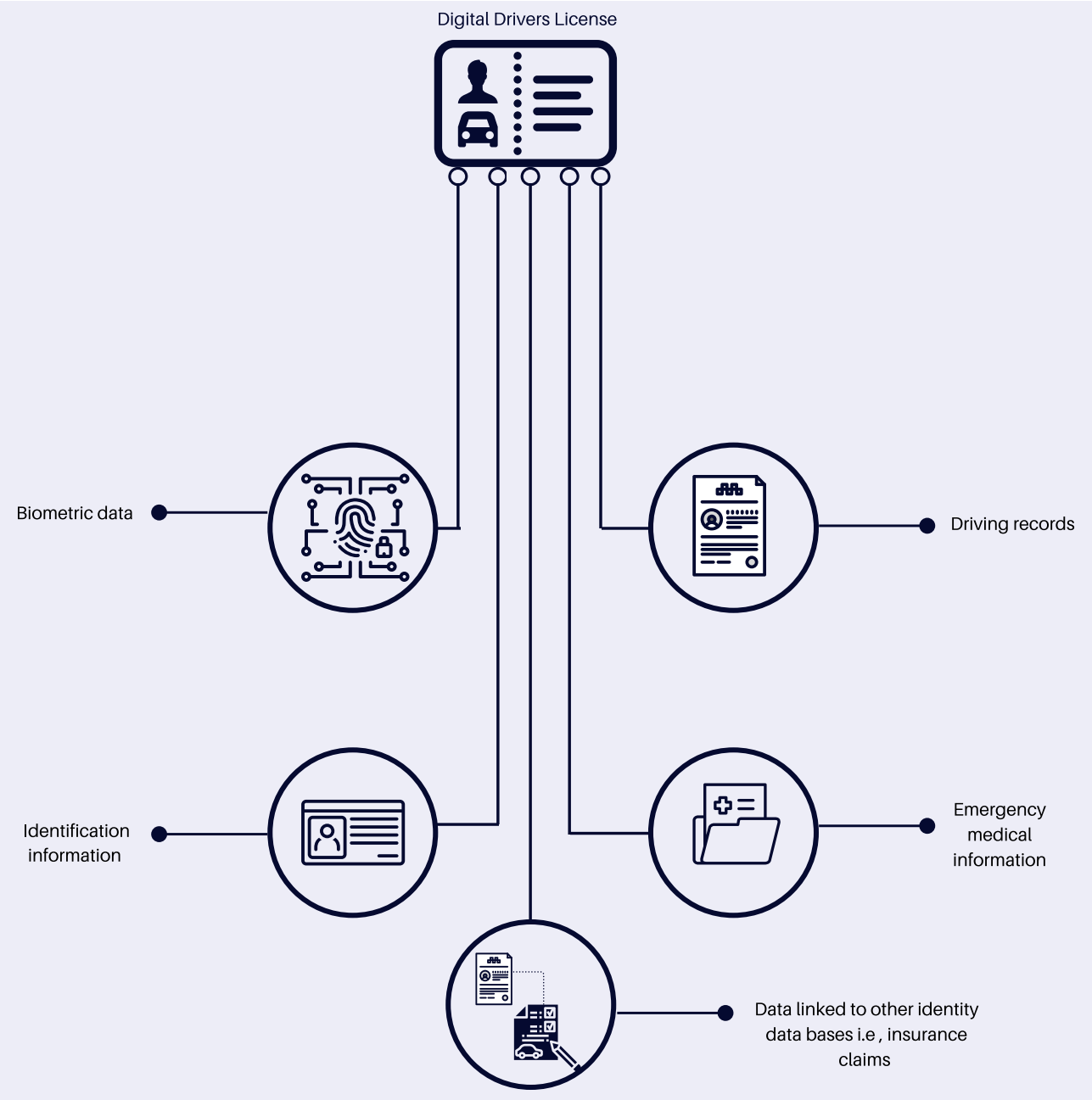
1. Identification information (foundational ID information, also family relations, etc.)

2. Emergency medical information, e.g., blood group and emergency contacts

3. Driving record for access by traffic enforcement officers

4. Biometric data for verification

5. Data linking to other identity databases, e.g., criminal records or insurance claims



RISKS INVOLVED IN THE USE CASE

The risks associated for digital driving licences include:

1. Susceptibility of the DID system to fraud (corrupt system for issuance of merit and demerit points)

2. Risk of inaccurate information, e.g., on blood group

3. Asymmetry in information where driving licence holders are not aware of how their data is accessed and used

4. Use of the data by government for purposes that are not consistent with human rights norms

02

ANALYSIS

Many low- and middle-income countries are digitising driving licence records, signalling a strong preference for use of DID for this function. Driving licences are important in low- and middle-income countries, for example, as tools of trade for millions who work in public transportation.

Public safety is often put forward as a justification for the push for digitisation. While there is public buy-in for improvement of road safety, driving licenses contribute only one part of road safety.

Another justification for digitisation of driving licences is that, in many sub-Saharan African countries, public transport is a market function delivered by private entities. Accordingly, although they are subjected to regulation, public transport services are chaotic in many African cities. Many countries are betting on digitisation of the road transport sector as a means to resolve or lessen the chaos.

In addition, governments assert that the benefits of smart driving licences include reduction of avenues for corruption, as most processes such as application and processing are done online, eliminating middlemen. Countries are also counting on the improved efficiency to reduce the time it takes to deliver the service.

Notwithstanding these claimed benefits, a reward and punishment mechanism through DID for drivers should be subjected to wide public discussion in order for potential human rights pitfalls to be identified and safeguarded. Such discussions are not happening or are superficially conducted, even though many countries are implementing DID systems for driving licences.

In Africa, regional blocks are implementing smart driving licences to facilitate movement of people within their areas. Ghana was the first country in West African Community to implement smart driving licences in 2017.

Digitisation of driving licences is happening alongside smart motor vehicle ownership stickers, smart licence plates, smart insurance stickers, and so on. This results in a centralised register of assets and compliance that include drivers, motor vehicle owners and service providers in the industry such as insurance companies. It is not clear how this data will be used, and the circumstances under which other government agencies such as law enforcement can access this data.

In countries such as Kenya and Ghana, not enough effort has been put on creating public awareness on the rationale and benefits of the systems. Instead, public agencies make it mandatory to acquire one form of DID in order to get the other, or put undue burdens on those seeking to obtain or renew a DID. In Kenya for example, drivers have been given a deadline within which to present themselves for biometric enrolment of the smart driving licences. There is no explanation on why biometrics are being collected, or how those without proper biometrics will be provided for.

In practice, driving licences are produced to law enforcement officers who have wide ranging powers. Without rules on how they can access data on the smart licences, there is cause for concern that licence holders may be subjected to arbitrary procedures. Furthermore, the reality of corruption is that it manifests in a variety of ways, and the existence of a DID system for driving licences does not reduce overall corruption where there is a lack of rule of law.

GOOD ID PRINCIPLES IN THE USE CASE

1. Separation of the foundational data from the functional driving licence, and limited access to the functional data.

2. Use of alternative methods for authentication, other than biometrics.

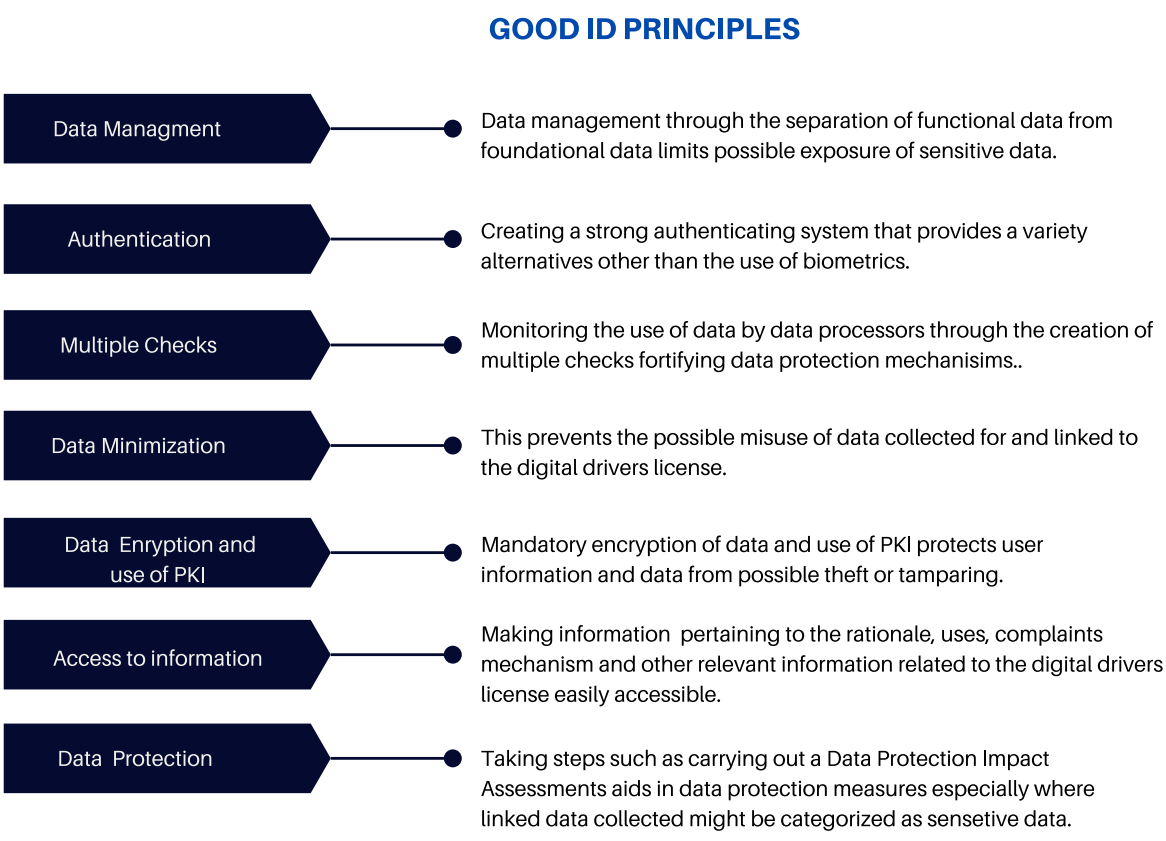
3. Multiple strong checks on the use of data by data processors.

4. Where there is a significant lack of respect for the rule of law, data collected for and linked to a digital driver licence system should be strictly minimized.

5. Mandatory encryption of data, and mandatory use of PKI.

6. Publication of information pertaining to the rationale, uses, complaints mechanism and other relevant information related to digital driving licences.

7. Carrying out of a data protection impact assessment for the use case.



03

CONCLUSION

Obtaining a driving licence is typically mandatory only to obtain the right to drive a vehicle, and therefore the lack of a driving licence is unlikely to result in the denial of other services. A digital system for driving licences has substantial potential benefits in terms of tracking motor vehicle-related data, but there is considerable risk that such data or related/linked data may be misused. Where it is contemplated to introduce a digital driver licence system, a thorough impact assessment should be carried out to ascertain potential conflicts with people's rights and to put in place the necessary safeguards.

ADDENDUM: KENYA AS A CASE STUDY.

DIGITAL ID & DRIVING LICENSES: USE CASES OF KENYA'S NTSA DIGITAL LICENSE

The increase in the number of motor vehicles on Kenyan roads led to a high demand for road transport related licences such as driving, public service vehicle (PSV), tourist service vehicles (TSV), and freight transport vehicles licences, as well as for motor vehicle registration. The high demand increased avenues for corruption and fraudulent licences. The licences were issued by several agencies including the Kenya Revenue Authority (KRA) Road Transport Department and Transport Licensing Board. A 2006 report by the Kenya Anti-Corruption Commission (now Ethics and Anti-Corruption Commission) found that the processes for service delivery in the road transport sector created opportunities for corruption, denying those without adequate 'facilitation' fees to access these services.

To reform the sector, an integrated transport policy was passed in 2009. In 2014, a dedicated agency, National Transport and Transport Authority (NTSA) took over most of the regulatory functions. Part of these functions include licensing driving schools, testing drivers and issuing driving licences.

DIGITAL DRIVING LICENCES

One of NTSA's first tasks in relation to driving licences was easing the process of renewal. Driving licence records were digitalised and renewal of driving licences was among the first services offered through the government service portal e-citizen. NTSA also developed the transport integrated management system (TIMS) through which all other services are offered. TIMS is linked to the national ID as well as tax database.

NTSA has been mooting the idea of digital driving licences since 2016. In January 2020, NTSA announced that all drivers would have to acquire new driving licences before July. The new licence is a smart card bearing details such as the driver's name, blood group, emergency contacts and KRA pin. Reports indicate that the licences will contain 'other' biometric data which are yet to be confirmed. They also contain the driver's KRA pin.

INAPPROPRIATE OR RISKY USE CASES

1. Employers may access driving record.

2. NTSA plans to share drivers' details with insurers. Offenders might have their premiums increased. Without appropriate oversight, this leaves room for abuse by insurance companies.

3. NTSA has a centralized database. Vulnerabilities in such a system could lead to injustices such as:

- *Misidentification: One of the ways the government is planning to use it is to identify terror and crime suspects. However, digital identity is not always accurate, and a search may bring up many false positive results. This can result in wrongful arrests and/or convictions.*

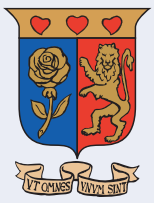
- *Data breaches*

- *Surveillance. The NTSA database was implemented alongside a rapid proliferation of roadside surveillance cameras. The vast amounts of data gathered by such cameras, especially in conjunction with digitized and biometric-based ID, could be used in ways that intrude upon the right of privacy.*

POSITIVE USE CASES

Digital registration of car ownership used to identify fraudulent registrations.

Digital scanners used to authenticate licenses.



Ole Sangale Rd, Madaraka Estate.
PO Box 59857 00200, Nairobi, Kenya | Tel +254 (0)703 034 612
Email: cipit@strathmore.edu | Website: https://cipit.strathmore.edu