

# **INTERNATIONAL STANDARD ISO/IEC 18013**

## **Information technology - Personal identification ISO-compliant driving licence -**

### **A guide for driver licensing authorities**

This document is intended to act as a non-technical guide for national/state/regional driver licensing authorities to the emerging International Driving Licence standard being developed by the International Organisation for Standardisation (ISO) (L'Organisation internationale de normalisation).

It was developed as a result of a request from ISO/IEC JTC1 SC17 Working Group 10 (WG10) to provide a lay person's guide to the emerging standard, a great deal of which includes necessarily technical content.

# Contents Page

<b>1</b>	<b>SECTION 1 - INTRODUCTION – STANDARDS AND SMART CARDS .....</b>	<b>3</b>
1.1	INTRODUCTION.....	3
1.2	STANDARDS .....	3
1.3	SMART CARDS .....	4
<b>2</b>	<b>SECTION 2 – WG10 - PURPOSE AND ROLE.....</b>	<b>7</b>
2.1	WG10 .....	7
<b>3</b>	<b>SECTION 3 – ISO18013 – THE INTERNATIONAL DRIVING LICENCE STANDARD</b>	<b>8</b>
3.1	PART 1 - PHYSICAL CHARACTERISTICS AND BASIC DATA SET .....	8
3.2	PART 2 – MACHINE READABLE TECHNOLOGIES .....	9
3.3	PART 3: ACCESS CONTROL, AUTHENTICATION AND INTEGRITY VALIDATION .....	10
<b>4</b>	<b>ANNEX A.....</b>	<b>12</b>

# 1 Section 1 - Introduction – Standards and Smart Cards

## 1.1 Introduction

- 1.1.1 International Standards Organisation Working Group (WG10) is in the process of developing an international driving licence standard. It is designed in such a way that any individual driving licence authority (national/regional/state) may choose to adopt any, all or (as the standard is entirely voluntary) none of its three constituent parts. Whilst providing a universally recognised standard, it also allows for the inclusion of individual licensing authorities' specific requirements.
- 1.1.2 Part 1 of the standard outlines the physical appearance of the driving licence document and provides an internationally recognized format. Part 2 allows for a number of internationally recognized technologies for electronic storage of information (e.g. chips, bar codes) and outlines a Logical Data Structure (how the information is ordered). Part 3 covers how that data is protected using a range of security mechanisms. Further details of each part are contained in Section 3 of this document.
- 1.1.3 Adoption of any or all of the standard will provide licensing authorities with a means of providing for an internationally recognized driving licence document whether that be purely by visual inspection, with basic details such as name, photograph, vehicle entitlements contained in a universal format, or if they should choose, the addition of electronic media such as a chip to form a smartcard driving licence. As well as harmonizing the way in which this information is stored, it provides licensing authorities with a ready made template, the adoption of which could save development time and provide its IT providers with an off the shelf set of data requirements.

## 1.2 Standards

### What do we mean by standards?

- 1.2.1 Standards make a significant but largely unnoticed contribution to most aspects of our lives. It is often when there is an absence of standards that their importance becomes clear. For example, as purchasers or users of products, we would soon notice if they turned out to be poor quality, did not fit, or were incompatible with equipment we already had, or prove to be unreliable or worse, dangerous. We are usually unaware of the role played by standards in raising levels of quality, safety, reliability, efficiency and interchangeability - as well as in providing such benefits at an economical cost. The organization responsible for many thousands of the standards which benefit society worldwide is the International Standards Organisation.
- 1.2.2 In 1946, delegates from 25 countries met in London and decided to create a new international organisation, of which the object would be "to facilitate the international coordination and unification of industrial standards". The new organization, ISO, officially began operations on 23 February 1947.

### The role of the ISO

- 1.2.3 ISO standards contribute to making the development, manufacturing and supply of products and services more efficient, safer and cleaner. They make trade and interaction between countries easier and fairer. They provide governments with a technical base for health, safety and environmental legislation. They aid in transferring technology to developing countries. ISO

standards also serve to safeguard consumers, and users in general, of products and services - as well as to make their lives simpler.

- 1.2.4 While the ISO defines itself as a non-governmental organisation (NGO), its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most NGOs. In practice, the ISO acts as a consortium with strong links to governments. There are 158 members, each of which represents one country.

#### ISO/IEC Joint Technical Committee 1

- 1.2.5 To deal with the consequences of substantial overlap in areas of standardisation and work related to information technology, ISO and IEC formed a Joint Technical Committee known as the ISO/IEC JTC1. It was the first such committee, and to date remains the only one. Its official mandate is to develop, maintain, promote and facilitate IT standards required by global markets meeting business and user requirements concerning across a whole range of areas.
- 1.2.6 WG10 - or ISO/IEC JTC1 SC17 WG10 to give it its full name – sits within the ISO structure as follows: ISO/IEC Joint Technical Committee 1/SC17 - Cards and Personal Identification/Working Group 10 - Motor vehicle driver licence and related documents

Please see **Annex A** for full details of the JTC1 structure, its committees and working groups.

#### Format

- 1.2.7 ISO standards are numbered, and have a format that contains "*ISO [IEC] [ASTM] [IS] nnnnn [ : yyyy] Title*" where "*nnnnn*" is the standard number, "*yyyy*" is the year published, and "*Title*" describes the subject. "IEC" will only be included if the standard results from the work of JTC1 (the "Joint Technical Committee"; see below). "ASTM" is included for standards developed in cooperation with ASTM International. The date and "IS" will always be left off an incomplete or unpublished standard, and may (under certain circumstances) be left off the title of the published work.

### **1.3 Smart Cards**

#### Definition

- 1.3.1 A smart card, chip card, or Integrated Circuit Card (ICC), can be defined as a credit card-sized card with embedded integrated circuits which can process information. There are two broad categories of ICCs. Memory cards contain only non-dynamic memory storage (information can only be read and cannot be changed) components, and perhaps some specific security logic. Microprocessor cards contain dynamic memory and microprocessor components (information can be updated).

#### History

- 1.3.2 Smart cards were invented in the late 60s in Germany, with the patent approved in 1982. The first mass use of the cards was for payment in French pay phones in 1983. Ten years later, microchips were inserted into French debit cards where users were required to authenticate themselves using a PIN. Smart-card-based electronic purse systems (in which value is stored on the card chip, not in an externally recorded account, so that machines accepting the card need no network connectivity) were tried throughout Europe from the mid-1990s.
- 1.3.3 The major boom in smart card use came in the 1990s, with the introduction of the smart-card-based SIM used in mobile phone equipment in Europe. With the proliferation of mobile phones, smart cards have become very common.
- 1.3.4 The international payment brands MasterCard, Visa, and Europay agreed in 1993 to work together to develop the specifications for the use of smart cards in payment cards used as either

a debit or a credit card. The first version of the EMV system was released in 1994 with further enhancements of the system in 1998, 2000 and 2004. With the exception of the United States there has been significant progress in the deployment of EMV-compliant point of sale equipment and the issuance of debit and or credit cards adhering the EMV specifications.

- 1.3.5 Smart cards with contactless interfaces are becoming increasingly popular for payment and ticketing applications such as mass transport systems. Visa and MasterCard have agreed to an easy-to-implement version currently being deployed (2004-2006) in the USA. Across the globe, contactless fare collection systems are being implemented to drive efficiencies in public transit. The various standards emerging are local in focus and are not compatible, though the MIFARE card from Philips has a considerable market share in the US and Europe.
- 1.3.6 Smart cards are also being introduced in personal identification and entitlement schemes at regional, national, and international levels. Citizen cards, driving licences, and patient card schemes are becoming more prevalent, and contactless smart cards are being integrated into International Civil Aviation Organisation (ICAO) biometric passports to enhance security for international travel in line with international obligations.

#### Contact Smart Card

- 1.3.7 Contact cards are the most apparent smartcards as they have a gold contact “chip” visible on the front of the card. When inserted into a reader, the chip makes contact with electrical connectors that can read information from the chip and write information back.
- 1.3.8 The cards do not contain a power source; energy is supplied by the card reader. Contact smart card readers are used as a communications medium between the smart card and a host, e.g. a computer, a point of sale terminal, or a mobile telephone.

#### Contactless Smart Cards

- 1.3.9 A second type is the contactless smart card, in which the chip communicates with the card reader through Radio Frequency Identification (RFID) induction technology. These cards require only close proximity to an antenna to complete a transaction. They are often used when transactions must be processed quickly or hands-free, such as on mass transport systems, where smart cards can be used without even removing them from a wallet.
- 1.3.10 The standard for contactless smart card communications is ISO/IEC 14443. It defines two types of contactless cards ("A" and "B"), allows for communications at distances up to 10 cm. ISO 15693 allows communications at distances up to 50 cm.

#### Dual interface

- 1.3.11 There are dual-interface cards that implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, that uses a chip in contact and contactless (ISO 14443B).
- 1.3.12 Like smart cards with contacts, contactless cards do not have a battery. Instead, they use a built-in inductor to capture the radio frequency transmitted by the card reader and use it to power the card's electronics.

#### ID Cards and PKI

- 1.3.13 A quickly growing application is in digital identification cards. In this application, the cards are used for authentication of identity. The most common example is in conjunction with a Public Key Infrastructure (PKI). PKI is a collection of technologies, processes, and organisational policies that support the use of public key cryptography (see below) and in particular the means to verify the authenticity of public keys. Digital certificates provide a link between a particular individual or system and their public key, and this certificate is signed by a certificate authority,

so that anyone who trusts that authority will also trust that the corresponding key pair is genuine.

1.3.14 Public Key Cryptography involves mathematical algorithms for encryption and decryption of information by separate but mathematically related keys in a key pair. Encryption carried out by one key of the pair must be decrypted by the other key. Knowledge of one of the keys in the pair does not give any clues or easy path to knowing the value of the other key in the pair. One member of the key pair is designated a Public Key (hence the name Public Key Cryptography), and indeed made public, with the other member of the key pair declared the Private Key and kept secret.

1.3.15 This removes the weakness of traditional single private key methods where that key has to be transmitted between several parties, and instead allows operations useful to the business to be carried out:

- Confidentiality
- Authentication
- Integrity
- Non-Repudiation

1.3.16 For an ID card, the chip will store an encrypted digital certificate issued from the PKI along with any other relevant or needed information about the cardholder. When combined with biometrics, smart ID Cards can provide two-or three-factor authentication.

## 2 Section 2 – WG10 - Purpose and Role

### 2.1 WG10

- 2.1.1 The work towards an international standard for the driving licence is undertaken within the International Organization for Standardization's (ISO) Joint Technical Committee for Information Technology (JTC1), Subcommittee for Identification Cards and Related Devices (SC17) (see Section 1).
- 2.1.2 WG10 - or to give it its full name - ISO/IEC JTC1/SC17 WG10 ISO Standardization in the field of Driver Licences – first met in Luxembourg in 1999 where representatives from 9 countries took part. It is made up of a mixture of government (driver licensing authorities/police) and industry (card manufacturers/PKI specialists etc.) representatives. It meets around 3 times a year and is usually attended by around 20-30 people. The most recent meeting in Edinburgh was attended by representatives from France, Germany, Greece, South Africa, Switzerland, USA and UK.
- 2.1.3 WG10 was initially formed to develop an International Standard for a driver licence identification card including a basic functional "model" set of data elements, for the most part, as specified in the 968 Vienna Convention. It was envisaged that the annexes to the standard would describe a variety of card technologies from which driver licensing/motor vehicle authorities could select an appropriate approach that best met its electronic data storage requirements (if any). It was not intended to mandate the use of any specific methodology or technology in the production or issuance of a driving licence document.
- 2.1.4 The initial goal was to learn and understand the needs of national and regional motor vehicle authorities as well as the international motor vehicle community, which UN/ECE represents to reduce the risk of driver licence fraud and abuse and help maintain road safety.

#### Current status of ISO18013

- 2.1.5 The standard seeks to establish guidelines in the format and content of motor vehicle driver licences (DLs) to support the requirements of national or regional motor vehicle authorities and international conventions. It creates a common basis for international use and recognition of DLs without impeding individual national and regional authorities in taking care of their specific requirements. An ISO DL is a document issued by a government agency, granting an individual permission to drive a motor vehicle within that agency's jurisdiction or region with the goal of ensuring the safety of individuals and property.
- 2.1.6 DLs and related documents are defined within the standard, in a broad framework of categories as documents for separate uses or function including passenger vehicles, commercial transport vehicles, and other related traffic safety applications (e.g. transport driver recorder card) and other card functions at the discretion of individual national/regional motor vehicle authorities. They can be enhanced by the adoption of machine-readable technologies.
- 2.1.7 The standard does not propose a global system standard for DLs outside the actual document.
- 2.1.8 The standard is in 3 parts. Part 1 of the standard was published in August 2005; Part 2 is at FDIS (Final Draft International Standard) stage; and Part 3 is at Committee Draft Ballot stage. Further details of the component parts of the Standards are contained in Section 3.

# 3 Section 3 – ISO18013 – The International Driving Licence Standard

## 3.1 Part 1 - Physical characteristics and basic data set

3.1.1 Part 1 establishes the design format and data content of an ISO-compliant driving licence (IDL) with regard to the human-readable (visual) features and the inclusion of machine-readable technologies on the card. It creates a common basis for international use and mutual recognition of the licence without restricting individual domestic or regional driver licensing authorities from incorporating their specific requirements.

3.1.2 The ID-1 sized IDL (which is based largely on the EU driving licence format – 91/439/EEC) allows one document to serve a dual purpose; a domestic driving permit and an international driving permit (IDP). Thus the IDL replaces the need for two separate documents.

3.1.3 Alternatively, those countries that choose to maintain their individual domestic design (or conclude they cannot meet the ISO standard due to their domestic requirements) can continue to do so, but they could still issue a second card (with or without machine-readable technologies) to replace the current IDP paper document only.

3.1.4 Part 1 also specifies an explanatory booklet with sleeve insert pocket that may optionally accompany an IDL to facilitate its worldwide interpretation when used instead of an IDP.

3.1.5 The IDL comprises the following:

- minimum common mandatory data element set,
- common layout for ease of recognition,
- minimum set of security requirements.

3.1.6 Part 1 of the standard allows domestic or regional driver licensing authorities to exercise their own discretion in respect of the following aspects of the IDL in order to meet their specific requirements:

- including supplementary optional data elements (in addition to the minimum common mandatory data element set);
- incorporating machine-readable technologies includes magnetic stripe, integrated circuit with contacts, contactless integrated circuit (smart cards) or optical memory technology, and 1 or 2 dimensional bar codes;
- incorporating current and future technologies (including biometrics, cryptography/PKI and data compression);
- adding physical document security elements (in addition to the mandatory elements).

3.1.7 This new IDL design provides a document that:

- is more secure from counterfeiting and alteration than the IDP document;
- allows authorities to verify the authenticity of the document;
- integrates the personal data into a secure ID-1 size medium;
- allows more reliable identification of the licence holder;

- allows for machine-readable technologies;
- facilitates information exchange and mutual recognition among driver licensing authorities;

### 3.2 Part 2 – Machine Readable Technologies

- 3.2.1 Part 2 describes the technologies that may be used for the standard, including the logical data structure (how information is organized) and data mapping for each technology. It prescribes requirements for the implementation of machine-readable technology on an ISO compliant driving licence (IDL).
- 3.2.2 One of the functions of an IDL is to facilitate international interchange. Storing IDL data in machine-readable form supports this function by speeding up data input and eliminating transcription errors. Consequently, the automation and productivity of traffic law enforcement and other traffic safety processes can be achieved or improved where it already in existence.
- 3.2.3 This part of the standard allows issuing authorities to customise machine-readable data for domestic use. Apart from international interchange, the use of an IDL as a domestic driving permit thus provides for domestic standardisation and creates a domestic infrastructure capable of processing IDLs issued by other issuing authorities.
- 3.2.4 The purpose of storing IDL data on machine-readable media on the IDL is to:
- Assist in authenticity and integrity validation;
  - Facilitate electronic data exchange;
  - Increase productivity (of data and IDL use).
- 3.2.5 Part 2 thus specifies the following:
- The logical data structure;
  - Mandatory and optional machine-readable data;
  - Encoding rules for the machine-readable technologies currently supported.
- 3.2.6 To prevent unauthorised access to the data contained on a contactless integrated circuit (e.g. by eavesdropping), provision is made to protect the privacy of the licence holder via basic access protection (requiring a human-readable and/or machine readable key/password on the IDL to access the data on the contactless integrated circuit (via protected-channel communication)). The implementation details of this function however are defined in Part 3 of ISO/IEC 18013. Provision is made for issuing authorities to validate the authenticity and integrity of the mandatory and optional data. In addition, the option of protecting access to optional data (beyond basic access protection) is provided for.
- 3.2.7 The key elements of Part 2 are the ordering of the Logical Data Structure (LDS) and the optional provision for machine readable technologies.
- 3.2.8 The LDS has been defined in such a way as to cater for the vast majority of individual licence authorities' requirements. Only one of these – Data Group 1 – is mandatory to meet the requirements of the international standard. The others - there are currently 11 DGs (this part is still a draft) - are voluntary. The Data Groups are ordered as follows:

**Data Group 1:** Mandatory data (this includes: Family name; Given name; Date of birth; Date of Issue; Date of Expiry; Issuing Country; Issuing Authority; Licence number; Categories of vehicles, restrictions)

- Data Group 2:** Optional licence holder information
- Data Group 3:** Optional issuing authority details
- Data Group 4:** Optional Portrait images
- Data Group 5:** Optional signature / mark image
- Data Group 6:** Optional facial biometric template
- Data Group 7:** Optional finger template
- Data Group 8:** Optional iris biometric template
- Data Group 9:** Optional other biometric template
- Data Group 10:** Reserved for future use
- Data Group 11:** Optional Domestic Use

3.2.9 This provides a modular approach where specific modules can be selected for inclusion.

3.2.10 The standard allows for the following (optional) machine readable technologies:

- magnetic stripe**
- contactless Smart Card**
- contact Smart Card**
- two-dimensional bar code**
- optical memory**

3.2.11 The above technologies have been considered as suitable for inclusion in the standard as they are ones which are already in use across the world or are likely to be considered for adoption in the future. For example, several EU Member States are considering the inclusion of a chip in the driving licence as the 3<sup>rd</sup> EU Directive allows this, subject to agreement on standards. Similarly, the REAL ID Act includes a yet to be defined "common machine-readable technology".

### **3.3 Part 3: Access control, authentication and integrity validation**

- 3.3.1 Part 3 describes the electronic security features that may be incorporated under the standard, including mechanisms for controlling access to data, verifying the origin of an IDL, and confirming data integrity.
- 3.3.2 This Part of the standard prescribes requirements for the implementation of mechanisms to control access to data recorded in the machine-readable technology on an ISO compliant driving licence (IDL), verifying the origin of an IDL, and confirming data integrity.
- 3.3.3 One of the functions of an IDL is to facilitate international interchange. Whilst storing data in machine-readable form on the IDL supports this function by speeding up data input and eliminating transcription errors, certain machine-readable technologies are vulnerable to being read unknowingly to the card holder and other means of unauthorised access by unintended persons other than driving licence or law enforcement authorities. Part 3 provides mechanisms for protecting these.
- 3.3.4 Controlling access to IDL data stored in machine-readable form protects the data on the card from being read remotely by electronic means unknowingly to the card holder.
- 3.3.5 Identifying falsified driving licences, or an alteration to the human readable data on authentic driving licences present a major problem for driving licence and law enforcement authorities, both domestically and in the context of international interchange. Verifying the authenticity of an IDL and confirming the integrity of the data recorded on an IDL provide driving licence or law enforcement authorities a means to identify an authentic IDL from a falsified or altered one in the interest of traffic law enforcement and other traffic safety processes.

This Part of ISO/IEC 18013:

- Is based on the machine-readable data content specified in Part 2.
- Specifies mechanisms and rules available to issuing authorities for:
  - (a) Access control (i.e. limiting access to the machine readable data recorded on the IDL).
  - (b) Document authentication (i.e. confirming that the document was issued by the claimed issuing authority).
  - (c) Data integrity validation (i.e. confirming that the data was not changed since issuing).

Suggests a number of options for the implementation of the mechanisms specified, such as cryptography as well as informative examples of key management.

## 4 Annex A

### ISO/IEC Joint Technical Committee 1

4.1.1 There are 18 sub-committees each of which have a number of Working Groups. WG10 the design and development of IT systems and tools

- the performance and quality of IT products and systems
- the security of IT systems and information
- the portability of application programs
- the interoperability of IT products and systems
- the unified tools and environments
- the harmonized IT vocabulary, and
- the user-friendly and ergonomically designed user interfaces.

4.1.2 There are currently 18 sub-committees:

SC 02 - Coded Character Sets

SC 06 - Telecommunications and Information Exchange Between Systems

SC 07 - Software and System Engineering

SC 17 - Cards and Personal Identification

SC 22 - Programming Languages, their Environments and Systems Software Interfaces

SC 23 - Removable Digital Storage Media Utilizing Optical and/or Magnetic Recording \* Technology for Digital

SC 24 - Computer Graphics and Image Processing

SC 25 - Interconnection of Information Technology Equipment

SC 27 - IT Security Techniques

SC 28 - Office Equipment

SC 29 - Coding of Audio, Picture, and Multimedia and Hypermedia Information

SC 31 - Automatic Identification and Data Capture Techniques

SC 32 - Data Management and Interchange

SC 34 - Document Description and Processing Languages

SC 35 - User Interfaces

SC 36 - Information Technology for Learning, Education, and Training

SC 37 – Biometrics

4.1.3 Each of the sub-committees has a number of related Working Groups. In SC17, these currently are:

WG 1 - Physical characteristics and test methods for ID-cards

WG 3 - Identification cards - Machine readable travel documents

WG 4 - Integrated circuit card with contacts

WG 5 - Registration Management Group (RMG)

WG 8 - Integrated circuit cards without contacts

WG 9 - Optical memory cards and devices

WG 10 - Motor vehicle driver licence and related documents

WG 11 - Application of biometrics to cards and personal identification