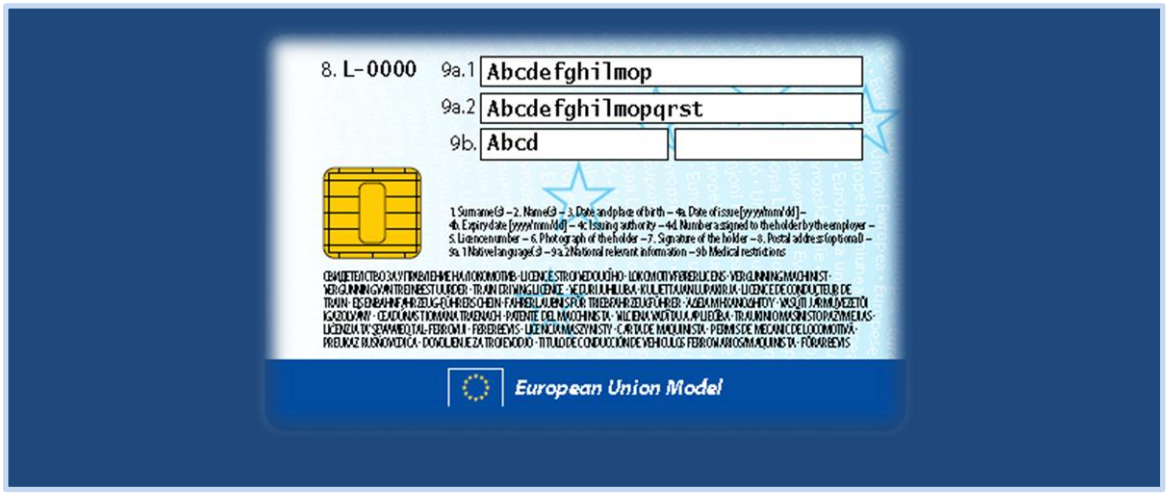
Report on the use of smartcards

Report on the possibility to use smartcards combining train driving licences and complementary certificates



Document Information

Date:	Fri, 2012 Dec 14
Release Number:	1
Version:	0.3
Reference:	ERA/REP/13-2012/INT

Table of Contents

Executive Summary

Introduction

Article 16b.1(e) of the Regulation (EC) No 881/2004[1] and Article 34 of the Directive 2007/59/EC[2] require the European Railway Agency (ERA) to investigate the possibility to use smartcards for train drivers' licensing/certification, combining driving licence (TDL) and complementary certificate (CC). This report contains the results of the activity undertaken by ERA to comply with this obligation.

The present report does not extend beyond the scope of investigating the possibility to use smartcards, but it is providing a generic overall architecture and feasible technical features. The full design of the system requires primarily the endorsement and commitment of the whole railway sector, and an adequate complex of human and budgetary resources to develop a thorough, comprehensive project.

For the scope of investigating the possibility to use smartcards, this report presents the result of a survey on the use of smartcards in the railway sector (NSAs, RUs, IMs) and in other industries across Europe, a sketch of technical and operational features for the system and a cost-benefit analysis, based on an ERA-commissioned study that was carried out by the consultancy firm, PricewaterhouseCoopers (PwC).

The report also tries to identify roles and responsibilities of actors in the current and in a future smartcard system-based situation and contains a SWOT analysis, based on the PwC study results as well as on available information on the railway sector. The European Commission and the whole railway sector are expected to benefit from the result of this report, increasing their awareness on the use of smartcards for the combined used of TDL and CC.

Generalities on smartcards

A (contact or contactless) smartcard is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligent system with internal memory or a memory chip alone.

Smartcards are used in a variety of applications (credit/debit cards and other types of automated payment, identity cards, healthcare, scholar or professional qualification, secured access to buildings/areas, transport ticketing, super markets, etc.)

The Railway sector, in addition to the specific application of identifying the train driver and retrieving data on professional qualification, may use smartcards for other application such as starting a train or recording driving time.

Survey on the use of smartcards

The report includes the result of a survey on the use of smartcards in the railway domain and in other sectors, as public administration, civil aviation, public transport ticketing and constructions. There is very little use of smartcards in the railway domain, and the very sporadic initiatives are mainly based on company needs. In other investigated sectors, the use of smartcards is mainly oriented to e-identity documents (at State level); access to restricted

[1] Regulation (EC) No 881/2004 of the European Parliament and of the Council of 29 April 2004 establishing a European railway agency (Agency Regulation) (OJ L 164, 21.6.2004, p. 1).

[2] Directive 2007/59/EC of the European Parliament and of the Council of 23 October 2007 on the certification of train drivers operating locomotives and trains on the railway system in the Community, O.J. L 315, 3.12.2007, p.51

areas and ticketing. For instance, smart-ticketing is perceived to be a lot more reliable, convenient, faster and easier to use than conventional ticketing, which delivers a better overall product allowing users to travel with more liberty.

Technical and operational features

The report contains an outline of technical features for the smartcards, both generic and specific for the train drivers licensing and certification. The assumption is that such smartcard should incorporate data which pertain to the train driving licence and those which pertain to the complementary certificate, in order to detect and eliminate duplications of data and optimise the use of memory.

The operational features aim at identifying the roles and the smartcards' supply flow and manage the necessary interfaces.

SWOT Analysis

The use of smartcards is very widespread outside the railway sector in Europe, with different purposes and a variety of suppliers. The report aims at identifying the strengths, weaknesses, opportunities and threats associated with the implementation of a whole smartcard system for the licensing/certification of train drivers. The result of the SWOT is summarised in the table:

HELPFUL	**STRENGTHS** Harmonised approach and processes throughout Europe Centralised design at EU level (shared decisions and costs) Flexibility (new functionalities can be added beside the pure use for TDL/CC) Specific for RUs/IMs: ensure compliance with requirements Specific for NSAs: improved controls (assist on inspections) Ease of use and information management	**WEAKNESSES** Technology may not be sufficient to manage the whole system No reference standard for building the system Complexity of relations (mainly for source of information and roles in managing data) Lack of harmonisation in display of data Update of information (needs a procedure) The approach of a European system is not sufficient for taking into account RU's specific change request in due time. Production costs Cost of technological components Cost-effectiveness of the system Protection of personal data and security of transactions Resources needed for adding functionalities
	OPPORTUNITIES Adoption of common standards/procedures Development of a centralised system, optimising design, interfaces, database, purchases and costs Automated access to databases/registers Immediate authentication Develop a reference standard	**THREATS** Absence of a reference standard Smartcards can be hacked/affected by viruses Possibilities that cards are lost/stolen (unavailability/misuse/need of procedures) Non familiarity with technologies Persistent lack of harmonisation in display of data In case the smartcard includes function to start a train, a defective cards or mal-functioning card-readers may prevent it to run
		HARMFUL

Cost-benefit analysis

The Agency's report on the possibility for introducing a smartcard system for train drivers licences and certificates includes a cost-benefit analysis in accordance with the provision in Directive 2007/59/EC (Article 34). This follows also from established Agency practice where in principle all of its recommendations should undergo an impact assessment. The cost-benefit analysis is carried out following the Commission Impact Assessment Guidelines. Two alternative scenarios (with a smartcard system – either with basic or more enhanced applications) are compared to a reference scenario (without a smartcard system).

The cost-benefit analysis demonstrates that a smartcard system in this area would entail significant costs particularly (fixed) set-up costs compared to the reference scenario without a smartcard. Furthermore, the operational costs are also likely to be much higher with a smartcard system. A smartcard limited to allow for the data storage of train drivers' licences and certificates (alternative 1) is likely to lead to substantial costs compared to the benefits. On the other hand moving to an enhanced smartcard system with additional applications may only lead to limited further cost increases (notably the case of a smartcard system with a digital tachograph). These additional applications are likely to bring additional benefits which may even outweigh the costs incurred. However, there is limited quantified information available about the benefits (in contrast to costs where orders of magnitude estimates are available). A further difficulty is that small countries face disproportionate costs of smartcard system compared to larger countries due to the presence of economies of scale in this area. Overall, our view is that further analysis is required to weigh the costs and benefits of the smartcard system, particularly with respect to decision making principles of each RU (based on its internal processes) and the complexity of design in case additional applications and features that may be integrated in the smartcard (a multi-application smartcard).

Conclusions and recommendations

The current scenery shows that there are varied and complex relationships between actors involved in the licensing/certification system. However this report provides only a snapshot of the situation: whenever a decision to introduce a smartcard system would be taken, a thorough investigation of the involved actors will have to be carried out, especially as far as the centralization, decentralisation and delegation of tasks in the licensing and certification processes are concerned. Further actors may have to be considered as a result of the necessarily detailed analysis of the reference scenario, preliminarily to the system design.

Then, a European smartcard system should be designed very carefully to ensure that all roles and responsibilities are fulfilled, ensuring that the licensing activity is carried out in a safe, secure, respecting all privacy issues and cost-effective manner.

We can conclude that the introduction of a smartcard system involves remarkable challenges in regard to data storage concerning infrastructure and rolling stock competence due to missing harmonised specifications. The low number of cards needed by the market in addition reduces the cost-effectiveness in particular when taking into account a relatively limited benefit (facilitated supervision). Additional functions of the smartcard could increase the benefit but would assume major costs and time demanding preparatory work on other regulatory fields (e.g.: equipment of rolling stock and description of infrastructure).

The current work on improving interoperability of licence and certificate registers may show that the prompt availability and updated plus accurate information from the authentic source is already sufficient for the need of the railway sector. Costs of designing, implementing and maintaining a smartcard system could then be avoided.

On this background, the following recommendations should be taken into consideration:

- Further steps on the implementation of a smartcard system for train driver licences should be delayed until the processes mentioned above will provide for more supportive circumstances.
- Appropriate solutions to use smartcards combining train driving licences and complementary certificates should be related to the solution that will be found for the interoperability of the train driving licences registers (NLRs) and complementary certificate registers (CCRs).
- In addition, projects developed at EU level, as the IMI (Internal Market Information System), as platform for the exchange of information and the forthcoming European Professional Card (the latter currently under discussions in the European Parliament and Council).

ERA, in co-operation with the NSAs and the representative organisations, has recently started to investigate the systems described at the last bullet point, in order to propose the European railway sector with a cost-effective and accurate solution.

1 Introduction and general explanations

The purpose of this report is to provide the European railway sector (mainly Railway Undertakings, Infrastructure Managers and National Safety Authorities) and the European Commission as with, the result after exploring the possibility to introduce a smartcard system for retrieving the information on train driving licence and complementary certificates of train drivers, as required by Article 16b.1(e) of the Regulation (EC) No 881/2004 and Article 34 of Directive 2007/59/EC[3] (see Chapter 2 for more details on the legal basis). The train driver licensing/certification system is currently regulated through separate documents as described in Regulation (EU) 36/2010[4].

The present report does not go beyond the scope of investigating the possibility to use smartcards. As far as the technical and operational features, this report provides:

- **a generic overall architecture**, because a detailed analysis of all the possible functions and interfaces would require the involvement and expertise of many more domains,
- **the basic technical features** of the smartcards and the comparison of possible solutions, and
- the **generic operational model to ensure the flow of information and role of actors involved**.

The report could not analyse all possible situations (centralisation or decentralisation in the issuing of documents) and allocation of responsibilities for managing source of data (Human resource departments / training centres / depots / others).

First of all, in order to develop the full design of a smartcard system the endorsement and commitment of the whole railway sector would be necessary, together with an adequate complex of human and budgetary resources to develop a thorough, comprehensive project.

1.1 Report preparation

In order to establish the baseline[5] for the present report, ERA commissioned a study, awarded to PricewaterhouseCoopers (PwC, hereinafter) on responding to the Invitation to Tender ERA/2010/SAF/OP/03, launched in December 2010. This study, completed in February 2012 and now available on the ERA website, provides the Agency with understanding on:

[3] Directive 2007/59/EC of the European Parliament and of the Council of 23 October 2007 on the certification of train drivers operating locomotives and trains on the railway system in the Community, O.J. L 315, 3.12.2007, p.51

[4] Commission Regulation (EU) No 36/2010 of 3 December 2009 on Community models for train driving licences, complementary certificates, certified copies of complementary certificates and application forms for train driving licences, under Directive 2007/59/EC of the European Parliament and the Council, OJ L 13, 19.1.2010, p. 1.

[5] It is important to remind that studies carried out for ERA or other institutions mentioned in this document express the opinions of the companies having undertaken them. In the specific case of the PwC study, the content has been accepted as a baseline of knowledge and for further reflection; however it should not be relied upon as a statement of ERA's views. Results and statements therein have been used and further elaborated for the preparation of the current report. ERA does not guarantee the accuracy of the information given in the PwC studies, nor does it accept responsibility for any use made thereof.

1) current experiences with the use of smartcards, investigating in the railway sector all over Europe (all the NSAs were requested to provide information and involving also the RUs and IMs) and also analysing non-railway applications, possibly related to the certification of professional qualification. The sectors investigated were: public administration, civil aviation, public transport ticketing and constructions;
2) technical and operational specifications for the use of smartcards; and
3) impact assessment of such measures.

1.2 Expected outcomes

The main contribution of the present document shall be an overview on

- the possible model for managing smartcards (actors, technical and operational features);
- the associated strengths and weakness, as well as benefits, opportunities and threats for the users and for the railway system as a whole, in qualitative terms and of cost/benefit analysis.

Finally, conclusions and recommendations will also be delivered on the introduction of a smartcard system.

1.3 Timeframe

The milestones for the completion and delivery of the Report on smartcards are:

31/10/2012 Delivery of report, incorporating the cost-benefit analysis, for internal and external (public) consultation

25/11/2011 End of public consultation

04/12/2012 Delivery of the report to the European Commission

1.4 Content of the following chapters

Chapter 2 **Legal background**:

This chapter contains an analysis of the related EC Directive and all complementary legislation that this report will be based on.

Chapter 3 **Current situation**:

This chapter contains a description of the current situation in the railway sector and in other industries.

Chapter 4 **Actors' involvement**:

This chapter outlines roles and involvement of the main actors (as EC / ERA / NSAs / RUs / IMs and train drivers) in the system.

Chapter 5 **Smartcards technical specifications**:

This chapter contains the envisaged technical features of smartcards.

Chapter 6 **Proposed operational specifications:**

This chapter outlines a possible model for operating smartcards throughout their entire life-cycle.

Chapter 7 **The case for and against a smartcard**

This chapter describes evaluating alternatives to the smartcards and between different types of smartcards.

Chapter 8 **SWOT analysis**

This chapter lists:

- immediate and potential benefits that the adoption of a smartcard system may bring to main actors and to the whole sector (strengths),
- the risk factors that could potentially impact the system (weaknesses),
- the business opportunities that are related to the implementation of the smartcard system (opportunities), and
- a qualitative analysis of factors that may have a negative impact on the implementation of a smartcard system (threats).

Chapter 9 **Cost/benefit analysis**

This chapter contains an impact assessment of the instruction of a smartcard system, considering also the comparison of costs for big and small countries.

Chapter 10 **Smartcard system overall evaluation and conclusions**

After analysing the factors and the actors' involvement, a clear recommendation concerning the system implementation can be made.

2 Legal background

Article 34 of the Directive 2007/59/EC, "Use of smartcards" provides for an obligation on the Agency:

By 4 December 2012, the Agency shall examine the possibility of using a smartcard combining the licence and certificates provided for in Article 4[6], and shall prepare a cost/benefit analysis thereof.
Measures designed to amend non-essential elements of this Directive and relating to the technical and operating specifications for such a smartcard shall be adopted on the basis of a draft prepared by the Agency and in accordance with the regulatory procedure with scrutiny referred to in Article 32(3)[7].
If the implementation of the smartcard does not entail any modification to this Directive or the Annexes hereto, the specifications of the smartcard shall be adopted in accordance with the regulatory procedure referred to in Article 32(2)[8].

and Article 16b (e) of the Regulation 881/2004/EC:

"[The Agency shall] *by 4 December 2012, examine the possibility of using a smartcard combining the licence and certificates provided for in Article 4, and shall prepare a cost/benefit analysis thereof. The Agency shall prepare a draft for the technical and operational specifications for such a smartcard*".

In addition, the smartcard system may support the NSA to collect the information pertaining to the monitoring to be carried out according to Article 29 of Directive 2007/59/EC:

1. The competent authority may at any time take steps to verify, on board trains operating in its area of jurisdiction, that the train driver is in possession of the documents issued pursuant to this Directive.

Furthermore, the vision for an electronic interface being used for applications other than the mere combination of two documents, seem to reflect the content of recital 18:

The Agency should also examine the use of a smartcard instead of a licence and harmonised complementary certificates. Such a smartcard would have the advantage of combining these

---

[6] *Article 4*- **Community certification model** (abstract)

1. All train drivers shall have the necessary fitness and qualifications to drive trains and shall hold the following documents:
(a) a licence demonstrating that the driver satisfies minimum conditions as regards medical requirements, basic education and general professional skills. The licence shall identify the driver and the issuing authority and shall state the duration of its validity. The licence shall comply with the requirements of Annex I, until the Community certification model is adopted, as provided for in paragraph 4;
(b) one or more certificates indicating the infrastructures on which the holder is authorised to drive and indicating the rolling stock which the holder is authorised to drive. Each certificate shall comply with the requirements of Annex I.

[7] *Article 32*- **Committee**

[3] Where reference is made to this paragraph, Article 5a(1) to (4), and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof. [**Now Regulation 182/2011/EU, articles 3 to 5 and 11]**

[8] *Article 32*- **Committee**

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.

two items in one and at the same time could be used for other applications either in the area of security or for driver management purposes.

3 Current situation

The current situation is to be considered as the starting state for this report. This part of the report is built on the PwC study and takes into account the result of a survey on all the smartcard systems adopted for the sake of retrieving data on professional qualification or similar purposes. It can be summarised as follows.

3.1 Railway sector

In support of the PwC study, ERA contacted railway sector representatives, in order to launch a survey aiming at detecting the existence of smartcard systems at national or at company level. Letters were addressed to the NSAs and the main sector representative associations (as CER, EIM, ERFA, etc.) and announces to the whole sector were published on the web-site

A questionnaire was circulated to NSAs in May 2011. In October 2011 PwC collected results, deriving from answers of 15 respondents. The survey indicated that to date no Member State had introduced a Smartcard System for train drivers at national level (meaning for all RUs and/or IMs). Two respondents nonetheless indicated they were in the process of introducing a Smartcard System in their country.

Furthermore, we learned that the largest Spanish train operator was introducing a smartcard system at that time and the largest Italian train operator was implementing a smartcard system within their organisations for quite a long time (about 10 years).

Despite the fact that no Member State had implemented a Smartcard System at national level, some general considerations can be extracted from the survey with regards to perceived benefits and barriers vis-à-vis a smartcard system and its alternatives: are included in the following chapters).

3.2 Experiences from other industries

The survey has shown that several examples of smartcard implementation projects can be found in other sectors, but there is limited use of smartcards in other transport sectors for the certification of staff: such cards are mainly conceived for security reasons and access to buildings/restricted areas.

The following experiences were investigated:

Sector	Location	Topic
Road transport	EU	Digital tachograph in road transport
Road transport	Sweden	Swedish driving licence
Road transport	Europe	European driving licence (overall regulation)
Maritime	Europe	European Port Access Identification Card (EPAIC)
Construction	United Kingdom	CSCS - Construction Skills Certification Scheme
Aviation	Netherlands	Schiphol Pass
Urban access restrictions	United Kingdom	Manchester - city level access restrictions
Public transport - Metro	Belgium	MOBIB

Road charging	Croatia	Hrvatske autoceste d.o.o.
Public transport	Netherlands	OV chip card
Identification	Belgium	e-identity card
Identification	Netherlands	Rijkspas
Healthcare	Germany	German Health Card

At first sight, smartcards appear to be a good solution that has the potential to make processes in a wide variety of sectors more efficient.

Among all others, the business case of connecting the smartcards with a digital tachograph in road transport is an interesting case for the railway sector as both are situated in the transport sector.

The digital tachograph is part of a very important EU project: TACHONET: Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards[9] that originates from legal requirements issued in 1985 (Council Regulation 821/85/EEC) and was developed from 1999 (based on Decision 1719/1999/EC) to 2004, under the coordination of the former DG TREN.

The latest tachograph legislation (Commission Regulation (EU) No 1266/2009) requires Member States to exchange electronically information in order to ensure that the tachographs are properly used to apply the social road transport rules. The Commission adopted on 13 January 2010 a Recommendation encouraging Member States to use the TACHOnet messaging system to exchange information on truck and coach drivers when checking tachograph cards. This Recommendation provides the necessary guidelines to implement this new requirement[10].

TACHONET is an information technology system allowing the exchange of messages between the EU Member States, through a smartcard and an electronic on-board tachograph. The digital tachograph guarantees better compliance with rules on driving time periods, resting periods in line with road safety rules and sets an end to the most common misuses of the previous mechanical system (based on the result of accident data collection, demonstrating that after an 11-hour work span the risk of being involved in an accident doubles). It is important to note that the system strongly relies on the effectiveness of the local databases.

Bus and truck drivers just like train drivers need certificates, licences, tests and controls. Therefore this case was used as a reference case in the context of PwC study. The case has shown that working with smartcards:

- improves the efficiency of processes;
- has relatively low cost;
- provides already an idea of the advantages additional applications, such as on-board recording of working hours, might bring to the railway sector.

[9] http://ec.europa.eu/idabc/en/document/2283/5926.html (for initial steps) and http://ec.europa.eu/transport/road/social_provisions/tachograph/tachonet_en.htm. For monitoring, please see: http://www.eu-digitaltachograph.org/DisplayPage.asp?PageId=63

[10] http://ec.europa.eu/transport/road/social_provisions/tachograph/tachonet_en.htm

Studies performed at EU level allow to estimate the population that may be affected by the adoption of smartcards and allow to identify the main differences in characteristics between the two cases is the number of final users of the smartcard. This lead to conclude that the use of the digital tachograph is most cost efficient due to the number of cards required for bus and truck drivers, which is much higher (approximately 4mln)[11] than the number of train drivers, estimated in about 200k[12]. For the latter, depending on the limited number of cards required, the conclusion of a case might be different.

ERA has also examined the final report of the Study on Public Transport Smartcards[13] – that presents recommendations regarding possible actions at the EU level to encourage and support interoperability in the ticketing system between current and future public transport schemes, through the use of smartcards.

It is necessary to underline that, due to this specific target of developing an EU ticketing system, the field of application is different and the extent of potential users of the system is exceptionally bigger than the potential for train drivers' licensing/certification (200k, as stated above). Nonetheless some recommended actions seem to be very useful:

- *Conducting detailed assessments of schemes, identifying and facilitating the sharing of best practice;*
- *Setting out specific 'model' scheme designs, business cases and model agreements between partners;*
- *Engaging with key stakeholders, and supporting relevant research into new technologies, seeking / supporting technological convergence;*
- *Providing incentives to stimulate further public and private investment and delivery;*
- *Ensuring the right 'tools' are available (scheme architecture, standards and specifications) and encouraging their use.* […]
- *review the approach taken and the effectiveness of the funds directed towards these actions after a period of say 3 years to confirm the appropriateness of this approach.* […]
- *developing model Framework agreements for the supply of services and equipment.*

This is an important input for the steps to be undertaken by the railway actors, in case they decide to proceed with the smartcard system for train drivers' licensing/certification.

[11] "**the road freight and passenger transport sector provides jobs for more than 4.5 million EU-citizens**" from the study 'Analysis of professional truck drivers tasks as basis for an European Qualification Framework (EQF) compatible profile', carried out by the University of Erfurt and funded with support from the European Commission (DG Education and culture).

http://www.project-profdrv.eu/fileadmin/Dateien/Downloads_front/ProfDRV_WP3_del11_analysisreport_12_01_27.pdf

[12] this approximate figure sorts out of ERA internal survey on interoperability of registers and of PwC study.

[13] The study was undertaken on behalf of the European Commission by the EC Smartcards Study consortium including AECOM, the lead consultant, The Transport Operations Group (TORG) of Newcastle University, PJohnson Associates, AustriaTech and NEA.

http://ec.europa.eu/transport/urban/studies/doc/2011-smartcards-final-report.pdf

4 Actors' involvement

There are two main considerations in relation to the possible introduction of a smartcard system:

- The legal responsibilities of actors in accordance with the Directive 2007/59/EC (see more in § 4.1)
- The practical roles of the actors in relation to the overall design of a smartcard system (see more in § 4.2)

4.1 Legal responsibilities in accordance with the Directive 2007/59/EC

From the point of view of legal responsibilities set up in Article 19 of the Directive 2007/59/EC, the following actors are involved in the administration of train driving licences:

- **National Safety Authorities**, as competent authorities designated by the Directive 2007/59/EC for:
  - process applications for new, renewed updated or duplicated TDLs[14]
  - issuing new, renewed, updated or duplicated TDLs[15]
  - withdrawing TDLs[16]
  - supervising the possession of train drivers' documents[17]
  - suspending the TDL issued by themselves[18]
- request the suspension of TDL issued by other NSAs[19]
- **Third party entities** delegated by the NSAs (only for issuing and updating licences, and providing duplicates)
- **Railway Undertaking(s)** delegated by the NSA (only for issuing and updating licences, and providing duplicates, under conditions of Article 19.1)

From the point of view of legal responsibilities set up in Article 15 of the Directive 2007/59/EC, the following actors are involved in the administration of complementary certificate:

- **Railway Undertakings** and **Infrastructure Managers** issuing, updating, suspending or withdrawing a complementary certificate[20]
- **National Safety Authorities** can request the suspension of a complementary certificate[21].

4.2 Roles related to the implementations of a smartcard system

At design (cross EU) level the following roles should be considered in relation to the different stages of production of smartcards, summarised in:

1. Pre-personalisation stage (see details at § 6.1.1)
2. Personalisation stage (see details at § 6.1.2 and 6.1.3)

[14] Article 14.2, Directive 2007/59/EC

[15] Article 19.1(a), Directive 2007/59/EC

[16] Article 19.1(c), Directive 2007/59/EC

[17] Article 19.1(g) and Article 29.1, Directive 2007/59/EC

[18] Article 29.4(a), Directive 2007/59/EC

[19] Article 29.4(b), Directive 2007/59/EC

[20] Article 15, Directive 2007/59/EC

[21] Article 29.4(c) and Article 29.1, Directive 2007/59/EC

3. Issuance stage (see details at § 6.1.4)

In stage 1 (pre-personalisation) the most important roles are:

- card producers
- system designers and suppliers

They are responsible for various preparatory phases:

- Card and component manufacturing;
- Application (on-card/off-card) development;
- Infrastructure and off-card application roll-out.

In stage 2 (personalisation) the most important roles are:

- The Physical card Management Entity (PME) will be responsible for the life-cycle of the physical cards, particularly ensuring the Card Personalisers have an appropriate stock, and secure disposal at the end of their life-cycle.

In stage 3 (issuance) the most important roles are:

At national level:

- The Train Driver Licence Management Entities (TDLME) will be responsible for the life-cycle of the TDLs. This role might be mapped on the NSAs or their delegate(s).
- The Complementary Certificate Management Entities (CCME) will be responsible for the life-cycle of the CC's. This role might be mapped on the RUs or their delegate(s);

4.3 Final consideration

The current scenery shows that there are varied and complex relationships between actors involved in the licencing and certification system, as well as further actors should be added if a decision to introduce a smartcard system is taken.

We acknowledge that a European smartcard system should be designed very carefully to ensure that all roles and responsibilities are fulfilled, ensuring that the licensing activity is carried out in a safe, secure and efficient manner.

To that purpose, at least the following aspects should therefore be considered:

- The different responsibilities among actors (e.g.: results of medical visits, the latter often performed under the framework of the companies safety management systems, are to be communicated to the NSA because they have the responsibility of this set of data according to the legal framework. These sort of passages may need to be simplified and shortened, but this would mean to accurately revise the current legal requirements in order to fit with the production flow of the smartcard);
- There are different types of information which are to be available on the same card (an effective system should rely on a timely and efficient network to ensure that the flow of information belonging from each actor is shared without delay and is provided to the entity producing the card in a reasonable time);
- The costs of the IT interfaces to ensure that all actors can provide the information in a timely and consistent manner;
- A time of non-availability of the physical document may be possibly due to the exchange of information and the time for update/reprint of the card. An interim solution, like a temporary permit and relevant management procedure might be necessary to prevent that the train driver has to work without the prescribed document or is forced to be kept out of work for some time.

5 Technical specifications of smartcards

A smartcard is a device that includes an embedded integrated circuit that can be either a secure microcontroller[22] or equivalent intelligent system with internal memory or a memory chip alone. Smartcard technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in GSM mobile phones, and USB-based tokens.[23]

There are two main groups of smartcards:

- contact smartcard, which need to get connected to a reader with direct physical contact. They have a contact area of approximately 1 square centimetre (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader which is used as a communications medium between the smartcard and a host (e.g., a computer, a point of sale terminal) or a mobile telephone. Cards do not contain batteries; power is supplied by the card reader. The reference standards for these cards are ISO/IEC 7810 and ISO/IEC 7816 series, which define:
  - physical shape and characteristics
  - electrical connector positions and shapes
  - electrical characteristics
  - communications protocols, including commands sent to and responses from the card
  - basic functionality
- contactless smartcard are any pocket-sized card with embedded integrated circuits that can process and store data, and communicate remotely with a terminal via radio frequency interface (waves). The reference standard for this type of cards is ISO/IEC 14443 (Identification cards -- Contactless integrated circuit cards -- Proximity cards) is an international standard that defines proximity cards used for identification, and the transmission protocols for communicating with it.

With an embedded microcontroller, smartcards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smartcard reader.

More detailed comparison between non-smartcards, contact and contactless smartcards are contained in Chapter 7

5.1 Smartcard generic technical characteristics

We consider a smartcard to have at least the following generic characteristics:

- Contains a microprocessor chip capable of storing and executing application logic combined with data;

[22] A **microcontroller** is a small computer on a single integrated circuit containing a processor core, memory, and programmable input/output peripherals. A program memory in the form of NOR flash or OTP ROM is also often included on chip, as well as a typically small amount of RAM. Microcontrollers are designed for embedded applications, in contrast to the microprocessors used in personal computers or other general purpose applications. http://en.wikipedia.org/wiki/Microcontroller

[23] http://www.smartcardalliance.org/pages/smart-cards-faq

- Contains a tamper-resistant[24] security system (for example a secure crypto-processor[25] and a secure file system[26]) and provides security services (e.g., protects in-memory information)[27];
- Is managed by an administration system which securely interchanges information and configuration via consoles. The type of information is to be defined according to the scope.
- settings with the card, controlling card blacklisting[28] and application-data updates;
- Communicates with external services via card-accepting devices which can be contact-based or contactless, or both;
- Physical dimensions may be defined as the ID-1 (credit card) format of the ISO/IEC 7810 standard. For convenience of the reader, we mention that the ID-000 (SIM card) format is world's most popular smartcard format. However, it is not considered a viable format for the Train Driving Licence due to its limited size.
- In the popular case of an ID-1 format smartcard, the card body is typically equipped with document security features such as guilloche printing, optical variable ink, laser engraving etc (as currently referred to in Annex I of Regulation (EU) No 36/2010);

In case the card does not contain a microprocessor chip and is not compliant to the specifications, may not be considered as a smartcard.

For completeness of information it is necessary to mention that today embedded solutions in smart phones such as secure MicroSD[29] cards may store equivalent functionality (chip, tamper resistance, management, and interfacing). As a consequence, they can be considered as functionally equivalent to a smartcard. However, in this case, document security is no longer present and the protection offered is not sufficient to prevent misuse or tampering. While such

[24] **Tamper resistance** is resistance to tampering by either the normal users of a product, package, or system or others with physical access to it. There are many reasons for employing tamper resistance. Tamper resistance ranges from simple features like screws with special heads, more complex devices that render themselves inoperable or encrypt all data transmissions between individual chips, or use of materials needing special tools and knowledge. Tamper-resistant devices or features are common on packages to deter package or product tampering. http://en.wikipedia.org/wiki/Tamper-resistant

[25] A secure cryptoprocessor is a dedicated computer on a chip or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures, which give it a degree of tamper resistance. The purpose of a secure cryptoprocessor is to act as the keystone of a security sub-system, eliminating the need to protect the rest of the sub-system with physical security measures. http://en.wikipedia.org/wiki/Secure_cryptoprocessor

[26] A file system (or filesystem) is a means to organize data expected to be retained after a program terminates by providing procedures to store, retrieve and update data, as well as manage the available space on the device(s) which contain it. A file system organizes data in an efficient manner and is tuned to the specific characteristics of the device. A tight coupling usually exists between the operating system and the file system. Some file systems provide mechanisms to control access to the data and metadata. Ensuring reliability is a major responsibility of a file system. Some file systems allow multiple programs to update the same file at nearly the same time. http://en.wikipedia.org/wiki/File_system

[27] The card may have also the name embossed (as credit cards) to avoid any possible fraud attempts.

[28] In computing, a **blacklist** or **block list** is a basic access control mechanism that allows everyone access, except for the members of the *black* list (i.e. list of denied accesses). The opposite is a whitelist, which means *allow nobody, except members of the white list*. As a sort of middle ground, a greylist, contains entries that are temporarily blocked or temporarily allowed. Greylist items may be reviewed or further tested for inclusion in a blacklist or whitelist. http://en.wikipedia.org/wiki/Blacklist_(computing)

[29] MicroSD: http://en.wikipedia.org/wiki/Secure_Digital # MicroSD

embedded solutions may become a viable approach for the Train Driver Licence in the longer term, we still do not consider them sufficiently mature today for operation in the context of the train driving licensing/certification.

We assume a generic smartcard type, interfacing through the traditional APDUs (Application Protocol Data Units). However, this should not be interpreted as a stringent limitation. The same functionality can be offered through a JavaCard that runs an on-card web server. In this case interfacing would be via HTTP (Hyper Text Transmission Protocol) or similar protocols.

We assume a generic smartcard lifecycle. The specification of the smartcard and complementary certificates cannot be defined in isolation, but rather in the light of the overall set of processes of usage. We structure this into four process families:

1. Origin of data, evidence and issuance processes
2. Use processes
3. Control enforcement processes
4. End of life processes.

Further assumptions hold:

The information on the card/stored in the chip is an authenticated copy. The master copy for the information is stored in the TDL/CC system and resides in the master database. This master database can be a real or a virtual database (i.e. distributed over various countries/organisations). The database implementations can be assumed to be Member State specific.

The system is based on the following overall information flow:

- From authentic source to master database;
- From master database to the Card Personaliser for both the card and for the authentic copy.

With regard to printing on the card body, it is assumed that secure printing (requiring specialised equipment) is required during personalisation, which is part of the issuance. As a consequence, we assume that after personalisation, printing is no longer possible. A card is issued with information printed on it which cannot be changed, nor can information be added. Information stored in electronic format can be changed, subject to authorisation. So as a consequence of Regulation (EU) No 36/2010, when some of the information that has to be available also on the surface of the card (printed out) is to be changed, the card has to be re-issued.

5.2 Specific smartcard general features (TDL+CCR)

Article 34 of the Directive 2007/59/EC clearly refers to the possibility of combining data of TDLs and CCs, so the specific smartcard general features refer to a card that contains and makes such data available.

We acknowledge that there could be solutions of cards only containing only authentication codes to verify the validity of the card and (maybe) give access to repository of data, but this report was developed in view of fulfilling the task given by the above mentioned Article 34 and with the final aim of harmonising processes and output at EU level. The authentication features are already part of the overall system (see § 5.10), if expected to be valid throughout Europe, has to be carefully designed as well as the full smartcard system: analysing tasks,

responsibilities and access to the repository of data. For this reason it was decided to explore the full system at this stage.

The basic requirements for the data to be contained in the TDLs and CCS are expressed in Regulation (EU) No 36/2010, which should at any time be considered as the authentic source of data for the smartcards.

The smartcard file features are assumed to reflect the TDL and CC specifications:

- some information is printed on the card only,
- some information may be stored in electronic format only,
- some information is both printed and stored electronically,
- Reading and updating such information is secured in terms of integrity, authenticity and confidentiality.

Furthermore:

- document security features must be in place to fight fraud,
- there should be significant flexibility in the proposed model, catering for the needs of the different stakeholders.

In case the smartcard becomes a project, these choices can be specified in the legal reference (since, it is necessary to remind, the current Regulation (EU) No 36/2010 Annex 1 section 1 today specifies a contact card).

As follows, a structured overview of these requirements, and other to refine or complement Regulation (EU) No 36/2010 to allow stakeholders to make an informed choice with regard to the feasibility of a system with a chip card:

Requirement id	Specification	Source
R 001	Compliance to ISO/IEC 7810:2003's ID-1 format.	Regulation 36/2010 Annex 1 Section 1
R 002	Compliance to ISO/IEC 10373-1:2006 for the physical aspects of the card	Regulation 36/2010 Annex 1 Section 1
R 003	The card should have an active life of at least ten years after issuance.	Regulation 36/2010 Annex 1 Section 4

Remarks

The technology on credit cards especially the cost, data storage, authentication and information exchange is always far more progressed than the simple smartcards. A thorough investigation on this should be considered if the project is to be developed in a later stage .

Whatever technology is chosen – contact or contactless- we consider that some specific choices should be excluded, including magnetic stripes and MRZ:

- Magnetic stripes are considered to be in "phase-out", mainly due to operational and maintenance costs related to the corresponding readers. These readers contain magnetic and mechanical components which form a major source of breakdowns and hence incur relatively high maintenance costs compared to other technologies.

- Machine Readable Zones (MRZ) are not to be included since it will never be able to accommodate the large amount of information of TDL/CC in such zones.

TDL Physical card layout

Requirement id	Specification	Source
R 020	The general layout of the card including the data to be stored on the surface are described in Commission Regulation 36/2010, sections 3 and 6	Regulation 36/2010 Annex 1 Sections 3 and 6

Remark: for data stored on the surface, secure printing is required. (see § 5.12.1 for security aspects and document safeguard).

5.3 Technical specification TDL – chipcard aspects

1. Introduction to envisaged supply side flow

We depict the envisaged supply side flow for the Train Driver Licence as summarised in the picture below, being populated with the main involved actors (green rectangles):

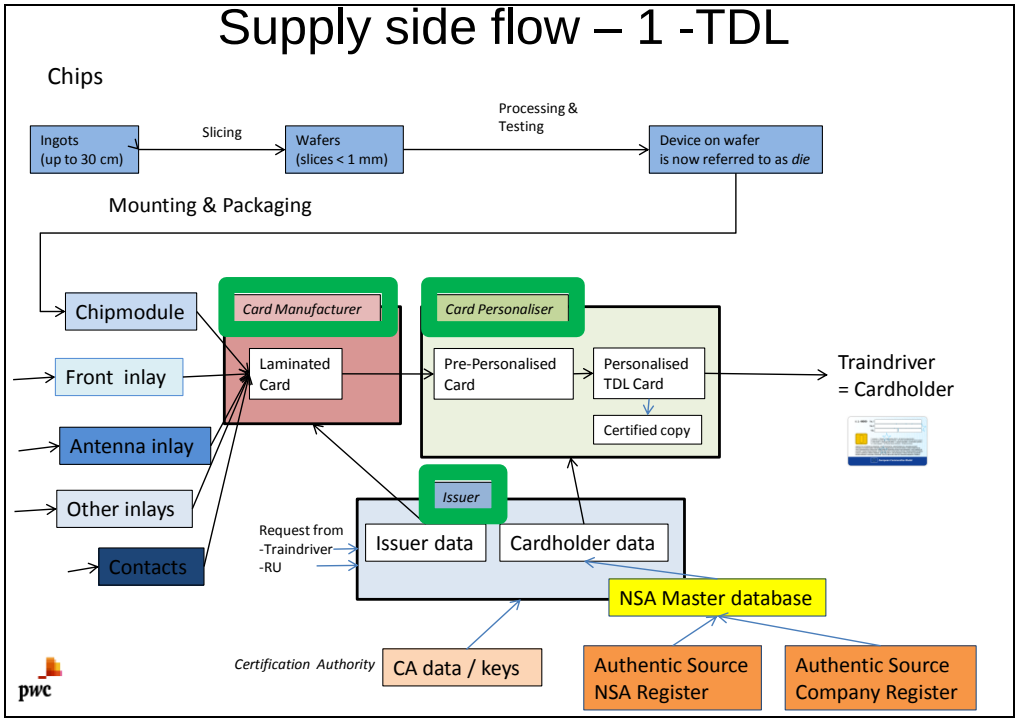


Figure 1: Envisaged supply side flow – part 1 TDL

It is assumed that in such flow, the Issuer may be the NSA, a delegated entity or an RU/IM (which can be delegated to issue licences for their own company). We also refer to the Issuer as 'Licence Managing Entity (LME)'.

In general our assumption is that there is only one issuer per Member State (the NSA or a delegated entity) however there may be more than one (the NSA and some RUs that are

delegated for issuing TDL to their employed train drivers) and any set of each RU-related information on the card should be protected against being changed or overwritten by any other RU.

Each NSA or delegated entity will be responsible for having the appropriate "authentic sources" of cardholder information (which should correspond to the data contained in their register of Train Driving Licences), and to make available the required information for Card Personalisation available to the CP (Card Personaliser). This may e.g. involve an NSA master database, or some other form of (distributed or centralised) register.

It is assumed that each NSA as well as ERA will make an informed decision with regard to the required services for Card Manufacturing, Card Personalisation as well as Certification Authorities (certification of cryptographic keys). Taking into account the current practices in the industry for these services, such services may be subcontracted to specialised entities.

We depict the envisaged supply side flow for the Complementary Certificate as summarised in the picture below, being populated with the main involved actors:

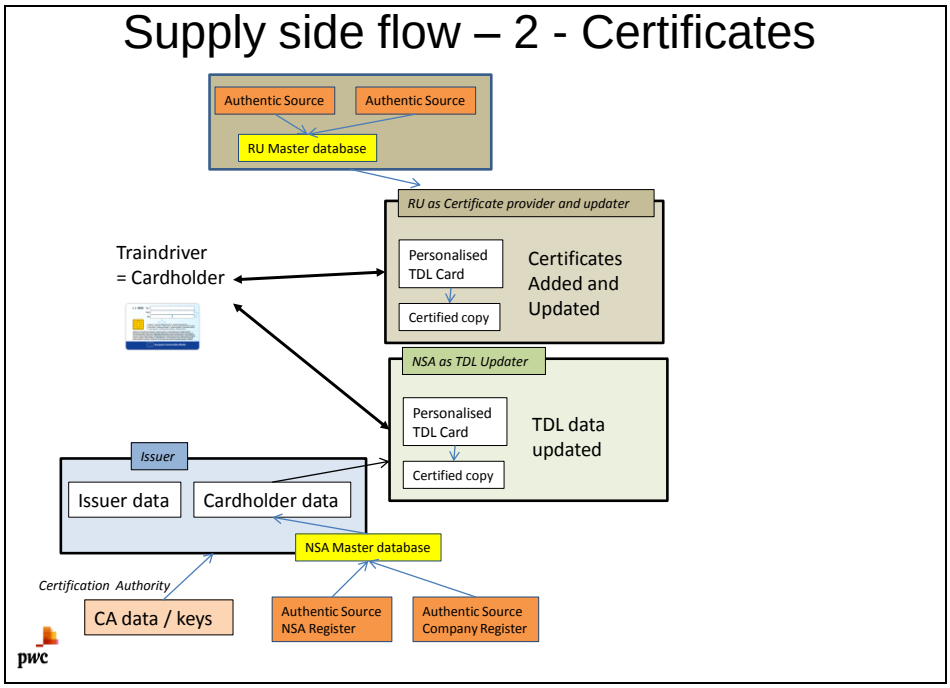


Figure 2: Envisaged supply side flow – part 2 Complementary Certificates

Once the card has been delivered to the cardholder by the Card Personaliser under responsibility of the NSA as issuer, it is valid until suspended/revoked or until it expires after ten years. It contains the static (date and place of birth) and relatively static information which, in case there are no changes, is in most cases valid for 10 years. It would be the case of cardholder picture, outcome of periodical medical tests (with various frequencies) like the obligation to wear glasses or hearing aids devices).

Once the card has been issued it can be extended by the RU's with the appropriate certificates. There may be different RU's that add certificates onto the card. Cardholders will apply for an examination with an RU. The RU will maintain a record of the outcome of such examinations, and will update the certificates on the card accordingly.

Each RU will be responsible for having the appropriate "authentic sources" of cardholder information, and to update the card when required. For example this may involve a RU master database, or some other form of (distributed or centralised) register.

5.4 General requirements

Table 1 below contains the general requirements of the smartcard as far as the supply flow is concerned. The initial requirement, set up by Regulation (EU) No 36/2010, Annex 1 Section 1, while the others are defined through the preliminary analysis of the system.

Requirement id	Specification
R.001	Compliance to ISO/IEC 7816-1:1998 for the physical aspects of the contact card (established by Regulation 36/2010, Annex 1 Section 1)
R.002	The card would contain four applications (TDL-Train Driving Licence, CC- Complementary Certificates, eAuthentication and eSignature), an Operating System and security safeguards.
R.003	Each application will manage the information lifecycle of their respective data elements.
R.004	The lifecycle of these data elements will at least be described in terms CRUD (create, read, update, delete).
R.005	The applications will be installed at the moment of card issuance. It must be possible to securely upgrade each application individually during the further life of the card.
R.006	For card management, security will be based on a model of roles and responsibilities where NSA's, ERA and RU's all participate. This model will technically be implemented on the basis of PKI (Public Key Infrastructure) security. The system will distinguish at least between roles of: - The Train Driver Licence Management Entities (TDLME); - The Complementary Certificate Management Entities (CCME); - The Physical card Management Entity (PME); - Train Drivers; - Operators of Inspection Systems.
R.007	The card will support multiple PINs and PUKs. PIN: Personal Identification Number PUK: PIN Unblocking Key

Table 1: Overview of general requirements

5.5 Operating System

One of the key activities is related to the management of the Train Driving Licence data, and the validity / integrity of the data transmission to the last stage of production (personalisation) of the smartcard. The red arrows direction identifies the relevant flow in the capture from the wider picture in figure 1 above.

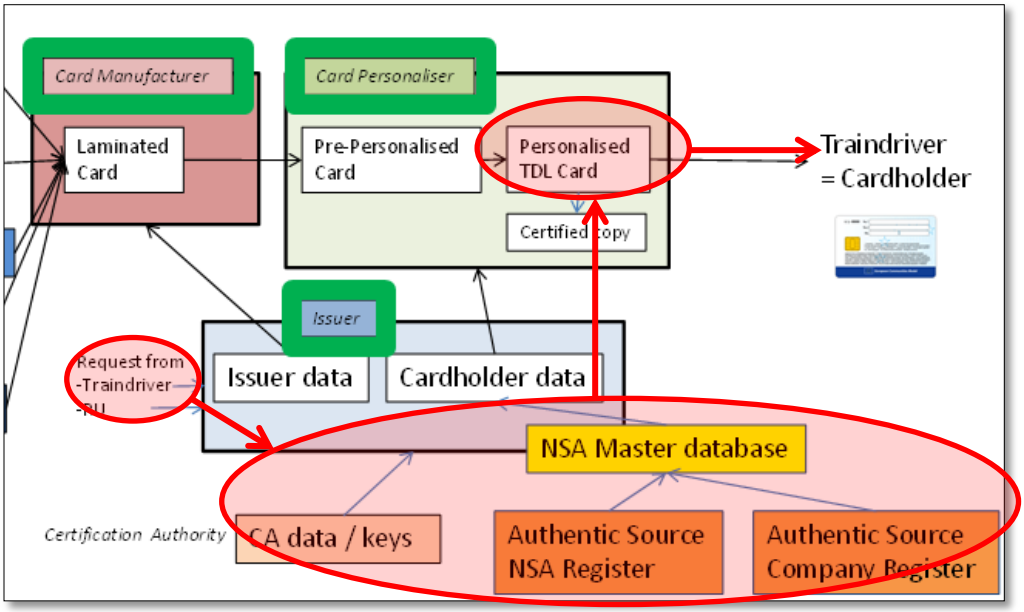


Figure 3 : Overview of the flow to check the validity of data

The application will be selected through the SELECT DF-commando (ISO/IEC 7816-4) using the appropriate application -identifier (AID). The Application Identifier-value is requested from an institution nominated for this purpose by the European Commission.

Data will be selected by the SELECT-commando (ISO/IEC 7816-4). The FCP-template will contain the size of the data. Data will be read by the READ BINARY-commando (ISO/IEC 7816-4).

Authenticity and integrity of data will be verified though the use of the LDS Data Groups Security Object.

The public keys required for verification will be obtained from the issuer. Verification of the signature will include appropriate CRL/OCSP checking.

5.6 Requirements for the Train Driver Licence and Complementary Certificate applications

These two applications are aimed at storing information on the smartcard in a secured way. For the time being we prefer not make too many assumptions here but aim for an approach that makes the card "universally readable" from a technology perspective. Scenarios should allow data exchange via:

- Use by a native terminal application or PC;
- Use over the internet (it could be through the HTTPS)[30].

These data exchanges will be secured by appropriate safeguards, including PIN and PUK. The access rights to the system will have to be established, in order to match the role of the party accessing the card.

[30] **Hypertext Transfer Protocol Secure** (**HTTPS**) is a widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. http://en.wikipedia.org/wiki/HTTP_Secure

5.7 Train Driver Licence file organisation

The Train Driver Licence Logical Data Structure (LDS) must contain following mandatory Data Elements: all elements listed in Table 2 below, except for 1.7 and 1.11 which are optional.

The overall organisation is similar to a Windows or Unix file system organisation, with:

- MF: Master File, the "root" of the tree "/"
- DF: Directory File, a folder or directory;
- EF: Elementary File, an individual file, stored in a specific DF, under the MF;
- DE: Data Elements, the individual information objects containing the data, stored in an EF.

The Train Driver Licence Logical Data Structure may contain following Data Elements: 1.7 and 1.11.

The content will be as follows:

MF (Master File, or "root")

|

| ------DF – TDL LDS Mandatory for the TDL issuer application with AID

|--- Set of cryptographic keys Kn

|--- EF.CMN (common information such as LDS version, Unicode version, list of DG's present)

|--- EF-DG1 Holder data (i.e. train driver data)

|---EF-DG2 Issuance data (i.e. issuer, data, validity, ...)

|---EF-DG3 Optional data

|---EF.LSO1 (LDS Data Groups Security Object with hash values/ electronic signatures of the protected data)

5.8 TDL data elements

This section highlights the content of the Train Driving Licence that should be also available in electronic format inside the chip and the associated logical data structure (**LDS**).

Content of the Train Driving Licence on chip:	**LDS**
0.1 the words 'train driving licence', printed in large type in the language or languages of the Member State issuing the licence	Common data – EF.CMN
0.2 the name of the Member State issuing the licence	Common data – EF.CMN
0.3 the name the Member State issuing the licence, based on ISO 3166 alpha-2 code, printed in negative in a blue rectangle and encircled by 12 yellow stars	Not required
1. Information specific to the licence issued: 1.1 The surname(s) of the holder matching that (those) displayed on the passport/national identity card/other recognised document proving identity. (1)	EF – DG1 – holder data
1.2 The name(s) of the holder. The name(s) must match that (those) displayed on the passport/national identity card/other	EF – DG1 – holder data

recognised document proving identity (2)	
1.3 The date and place of birth of the holder (3)	EF – DG1 – holder data
1.4 The date of issue of the licence (4a)	EF – DG2 – issuance data
1.5 The date of expiry of the licence (4b)	EF – DG2 – issuance data
1.6 The name of the issuing authority (4c)	EF – DG2 – issuance data
1.7 The reference number assigned to the employee by the employer ***Optional*** (4d)	EF – DGn – optional data
1.8 The number of the licence giving access to data in the national register is based on the European Identification Number, (EIN) as stated in Commission Regulation (EC) No 653/2007 (5)	EF – DG2 – issuance data
1.9 a photograph of the holder (6)	EF – DG1 – holder data
1.10 the signature of the holder (7)	EF – DG1 – holder data
1.11The permanent place of residence or postal address of the holder ***Optional*** , (8)	EF – DGn – optional data
1.12Additional information (identified as '9a' boxes), or medical restrictions (identified as '9b' boxes) for use imposed by a competent authority. Medical restrictions will be displayed in code form. (9)	EF – DG2 – issuance data
1.13Additional information shall be displayed in boxes identified with number 9a, in the following order: a.1 Native language(s) of the train driver, according to the classification in use in the Member State	EF – DG1 – holder data
a.2 Space reserved for entries by the Member State which issues the licence, for necessary information according to national legislation	EF – DGn – optional data The chip may contain some more information than those displayed on the surface
1.141Medical restriction shall be displayed in boxes identified with number 9b. Codes 'b.1' and 'b.2' will constitute harmonised Community codes for medical restrictions: b.1 Mandatory use of glasses/lenses b.2 Mandatory use of hearing aid/communication aid	EF – DGn – optional data The chip may contain some more information than those displayed on the surface: e.g. date of next expected medical check

Table 2: Overview TDL data elements

5.9 Complementary Certificate's file organisation

The CC LDS must contain following mandatory DEs: all elements listed in Table 3, except for 0.4, 1.1.4 and 1.2.5 which are optional.

The overall organisation is similar to a Windows or Unix file system organisation, with:

- MF: Master File, the "root" of the tree "/"
- DF: Directory File, a folder or directory;
- EF: Elementary File, an individual file, stored in a specific DF, under the MF;

- DE: Data Elements, the individual information objects containing the data, stored in an EF.

The CC LDS may contain following DEs: 1.1.4 and 1.2.5.

The content will be as follows:

MF (Master File, or "root")

|

| ------DF – CC LDS Mandatory for the TDL issuer application with AID

|--- Set of cryptographic keys Kn

|--- EF.CMN (common information such as LDS version, Unicode version, list of DG's present)

|--- EF-DG4 CC Issuance data

|---EF-DG5 Employer data

|---EF-DG6 Optional data

|---EF.LSO2 (LDS Data Groups Security Object with hash values/ electronic signatures of the protected data)

Content of the Complementary Certificate on chip	**Comments**
0. General 0.1 a reference to the licence number	Should be included if we secure each CC as an individual unit. This will allow the protection of the integrity of the CC, and will identify cases where CC's are copied from one TDL to another.
0.2 the surname(s) of the holder: Member States may include all the surnames recognised, but the priority should be given to the main family name and the listing of names should be consistent with that displayed on the licence	Idem
0.3 The name(s) of the holder. Member States may include all the first names that they recognise, but the listing of the name shall be consistent with that displayed in the licence	Idem
0.4 Reference number given by the employer *Optional*	This element is optional (legal requirement in the Directive 2007/59/EC and consequently in Regulation (EU) No 36/2010). However we have concluded that it may be useful for the smartcard since it identifies the train drivers in each specific RU –important in case of a train drivers contracted by several RUs.

0.5 Issuing and expiry date of the complementary certificate. The duration of validity for the complementary certificate is established by RUs/IMs employing or contracting drivers, and set in the procedure to be published by RUs/IMs in conformity with Article 15. If the certificate is valid indefinitely, the expiry date is made void	EF.DG4 CC issuance These dates are set by the company and do not have a big importance, since the inner expiry dates of competencies may affect the whole validity of the certificate. The deletion of this element should be considered for the single document.
0.6 Data related to the issuing organisation. The complementary certificate may be issued by a central or regional RU/IM's department, designated under the procedure in conformity with Article 15 of Directive 2007/59/EC	EF.DG4 CC issuance This information seems to be strictly linked the levels of delegation. Data related to the issuing of information concerning the certificate might go in the chip only.
0.7 it may include a company internal number for administrative purposes	EF.DG4 CC issuance Further reflection on the use of too many numbers and take a decision. Maybe some automatic codes can be generated all times and information is created / updated / deleted?
1. Specific data **1.1** Data on the employer 1.1.1 the company name and, if relevant, the workplace (e.g. the depot to which the driver is assigned), 1.1.2 the category of entity employing or contracting the driver: 'railway undertaking' or 'infrastructure manager', 1.1.3 the postal address: street address, post code, city and country, 1.1.4 the train driver's personal reference number within the company. Optional	EF.DG5 Employer This information concerning the certificate should go in the chip only. It is necessary to remind that a driver may be contracted part-time by more than one company, so it would be necessary to find a solution to manage the information provided by the different companies.
1.2 Data on the holder 1.2.1 the place of birth (place and country), 1.2.2 the date of birth, *1.2.3* the citizenship of the driver, *1.2.4* the postal address (street address, post code, city and country). *Optional*	Ref 0.1
1.3 Categories of driving. The categories and types of driving, for which the driver is authorised to drive, shall be displayed	EF.DG5 Employer This is an important element. It gives immediate information on the type of service that a driver is allowed to carry out, so it should be also on the surface. Having this information on the surface allows the prevention of misuse.

1.4 Additional information. This part is reserved for additional information that may be requested by national applicable legislation or by the company's internal procedures.	EF.DG5 Employer The chip may contain much information. It would be very difficult to store them on the surface
1.5 Data related to language skills The list of all languages, others than the native language, that are necessary to operate on the relevant infrastructure and that are known by the train drivers and comply with the requirements of Annex VI to Directive 2007/59/EC, shall be inserted here.	At TDL level only the native language is displayed, hence the chip may contain more information. It would be difficult if not impossible to store them on the surface.
1.6 Restrictions This part shows restrictions related to the characteristics and capabilities of the driver in relation to the content of the complementary certificate (e.g.: driving allowed only in daylight) NE0 1/31L If the restrictions concern rolling stock (e.g.: speed restrictions when driving certain types of locomotives) and/or infrastructure, the information in text format shall be provided in the box 'notes' beside the relevant rolling stock and/or infrastructure.	EF.DG5 Employer This is an important element. It gives immediate information on the limitation of extent of the drive. Having this information on the surface (maybe in a coded form) allows the prevention of misuse.
1.7 Data relating to rolling stock This part lists types of rolling stock the driver is authorised to drive, following an assessment of competences listed in Annex V to Directive 2007/59/EC. Data shall be displayed in the following boxes: 1.7.1 a box for the date of the beginning of validity of the relevant competence, 1.7.2 a box for each type of rolling stock.	EF.DG5 Employer The chip may contain much information. It would be very difficult to store them on the surface, unless totally revising the licence's feature. It is assumed approximately 20 records would be a maximum.
1.8 Data related to infrastructure This part lists the infrastructure on which the driver is authorised to drive.	EF.DG5 Employer The extent of these data may be huge. The Chip may contain much information that would be difficult if not impossible to store on the surface Very different ways of describing the relevant set of information is expected. Many records may be expected (up to some hundreds).

Table 3: Overview of complementary certificates on chip

5.10 Requirements for the eAuthentication and eSignature applications

5.10.1 Requirements for the eAuthentication application

The smartcard should allow the card holder to engage in standard authentication protocols, e.g. against a local terminal, PC, Kiosk or webserver. This should include:

- the typical web-based authentication protocols used in the context of a Windows authentication (NTLM, Kerberos, Claims...), or
- HTTP, including SAML (Security Assertions Mark up Language) authentication assertions.

For asymmetric solutions, key-lengths should be in line with the "state-of-the-art" in cryptography. At the time of this Study, up to 2048 bits should be supported.

5.10.2 Requirements for the eSignature application

The smartcard should allow the card holder to engage in electronic signing processes. The card should support multiple signature transformations such as based on RSA, DL and ECC.

For asymmetric solutions, key-lengths should be in line with the "state-of-the-art" in cryptography. At the time of this Study, up to 2048 bits should be supported.

The card should be compatible to any eSigning application used. It must be possible to use the common eSigning applications from Microsoft, Adobe, in-house developed, or other.

Standards should be supported, particularly from ISO, CEN, and ETSI, particularly as emerging from mandate M460. Furthermore industry and de-facto standards such as PKCS-family (notably PKCS#11 and 15) and the Microsoft CryptoAPI should be supported.

5.11 Overall file organisation

5.11.1 Basic concepts

Inside the smartcard at the lowest level, data is stored in elementary files (EF), grouped in directories (DF). To ensure interoperability, data will be stored in an organised way, based on the following concepts.

- The **Logical Data Structure** (LDS) represents the highest level grouping of data in a smartcard. There are two types of LDS, the **TDL LDS** and the **CC LDS**. Each issued smartcard should mandatory have at least a TDL LDS. Zero, one or more CC LDS can be added at discretion of the CCMEs (Complementary Certificate Management Entity);
- The LDS contains a number of mandatory and optional **Data Elements** (DE), stored in files such as **Elementary Files** (EF), and grouped together in **Data Groups** (DG).
- To allow confirmation of the authenticity and integrity of the recorded details, an **authenticity/integrity object** is included. We refer to this as the **LDS Data Groups Security Object** Each DG must be represented in this authenticity/integrity object, which is recorded into a separate Elementary File.

These authenticity and integrity safeguards will be based on the Public Key Infrastructure (**PKI)**[31], bearing in mind that PKI should not be relied upon as the single determining factor.

The different parties playing a role in the issuing of TDL and CC are expected to **manage the life-cycle** of the public- private key pairs and where appropriate symmetric keys that are required to act as TDLME (Train Driver Licence Management Entity), CCME (Complementary Certificate Management Entity and Physical Card Management Entity (PME). Furthermore, access should be foreseen for Train Drivers and for Operators of Inspection Systems.

[31] A public-key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

The overall organisation of the PKIhierarchy must be decided by the Stakeholders. For the time being we assume it will be based on well-established concepts such as demonstrated by:

- the EU-wide ERCA (European Root Certification Authority) for the digital tachygraph, please refer to http://dtc.jrc.it/erca.html
- the EU-wide Trusted List, please refer to http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm
- the global PKD (Public Key Directory of the ePassports), please refer to http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx

On the basis of information available at the time of executing this study, we assume a model such as the ERCA one is probably the most appropriate candidate PKI model.

5.12 Security aspects

5.12.1 Document safeguards

With regard to document security aspects, we adhere to the de-facto standard taxonomy for safeguards that distinguishes between iridescent and non-iridescent safeguards. Iridescence is the capricious flow of fluctuating colours which has become a cornerstone of document security. It is illustrated by the inside of an abalone shell.

The popular taxonomy for document safeguards can be represented as:

- Non-iridescent safeguards:
  - Substrate (paper, plastic, card body);
  - Printing (inks, techniques, patterns);
- Iridescent (OVD – Optically Variable Device) safeguards:
  - Diffraction-based (DOVID – Diffractive Optically Variable Image Device) such as holograms and kinegrams:
  - Interference-based (ISIS - Interference Security Image Structure) such as thinfilm and single/multilayer films:
  - DOVID/ISIS combinations such as chromagram, CLP and DiOViS.

From regulation, for TDL/CC, following mandatory and discretionary safeguards are already specified:

Safeguard	Specification	Source
SG.DS.01 Mandatory	Mandatory security features: card body shall be UV dull, security background pattern, OV elements, overlap photograph and security design background This should support: First line inspection, an examination done without tools or aids that involves easily identifiable visual or tactile features for rapid inspection at point of usage Second line inspection, an examination that requires the use of a tool or instrument (e.g., UV light, magnifying glass, or scanner) to discern a real from a fake document.	Regulation 36/2010, Annex 1 Section 2 Anti-forgery measures
SG.DS.02	Discretionary techniques of which at least one should be	Regulation 36/2010,

Discretionary	used: colour-shifting inks, thermo-chromic ink, custom hologram, variable laser images, tactile characters, symbols or patterns. This should support: First line inspection, an examination done without tools or aids that involves easily identifiable visual or tactile features for rapid inspection at point of usage Second line inspection, an examination that requires the use of a tool or instrument (e.g., UV light, magnifying glass, or scanner) to discern a real from a fake document.	Annex 1 Section 2 Anti-forgery measures
SG.DS.03 Third line	Additional support for third line of inspection, an examination in a specialised laboratory. In-depth physical inspection of the document security safeguards by experts.	Not applicable, Safety Management System is considered the third line of defence.

Table 4: Document safeguards TDL)

For the Complementary Certificate there are additional specifications in Regulation (EU) No 36/2010, Annex 2 Section 3 Anti-forgery measures:

- Technical measures (company logo, paper texture and permanent ink, display of internal reference number and stamp). Updates confirmed by date and stamp and consistent with information in the register.
- Procedural measures to check that information on the certificate is valid and has not been altered, in accordance with Article 18(1) of Directive 2007/59/EC.

However, as the TDL and CC will share the same physical media, the latter are considered to be integrated into the TDL safeguards.

Safeguard	Specification	Source
SG.SS.01 Tamper	Hardware tamper resistance and hardware protection safeguards (sensors and alarms, memory content protection, bus protection)	Best practice
SG.SS.02 RNG	Hardware random number generation	Best practice
SG.SS.03 ACC	Logical access control Commission Decision 2010/17/EC of 29 October 2009[32] defines the access rights for licence and certificate data when residing in the registers. We suggest aligning those for the smartcard applications/file system in an identical way. The CD proposes to distinguish following roles: Competent authorities of other Member States The Agency (i.e. ERA);	Best practice

[32] Commission Decision 2010/17/EC of 29 October 2009 on the adoption of basic parameters for registers of train driving licences and complementary certificates provided for under Directive 2007/59/EC of the European Parliament and of the Council (OJ L8, 13.1.2010, p. 17).

	An employer of drivers Railway Undertakings and Infrastructure Managers, employing or contracting train drivers; The train drivers themselves for their own information; Investigation bodies. As such, the card's logical access control grants access to the applications and files as per the requirements of these different roles. This always requires asymmetrical authentication. This will be based on role attributes embedded in public key certificates.	
SG.SS.04 Crypto	Cryptographic key management All keys should be stored in trusted hardware. There should be individual keys or key pairs per actor. Each actor should be responsible for his keys or key pairs. Appropriate root key certificates and all intermediate certificates required to validate a certificate should be stored on-card during the card issuance process. Public key certificates should be embedded in the trusted storage of the card under responsibility of their owners.	Best practice
SG.SS.05 SecChan	Secure communication channel. Appropriate mutual authentication protocols should be used to guarantee the authenticity of the communicating parties, and to protect the contents of the communications.	Best practice
SG.SS.06 APPSEC	On-card application security There should be guarantees provided with regard to the integrity of the on-card application and the information processed by this application. There should be guarantees provided with regard to the integrity and confidentiality of the information stored on the chip. The latter should include the use of electronic signatures over the stored information.	Best practice
SG.SS.07 EAL4	There should be a certificate of Common Criteria Evaluation EAL4, preferably with augmentation (EAL4+). This certificate should address all aspects of the smartcard, i.e. all logical and physical components.	Best practice
SG.SS.08 Inspection	Inspection system with black-list. This inspection system should be available on-line, and should invoke all interactions or transactions with the on-chip application.	Best practice
SG.SS.09 Other	*Other off-card safeguards - [pro-memori]*	Best practice

Table 5: Document safeguards (CC)

6 Proposed operational specifications

The choice of vendor(s) for the various supporting systems dictates the technology, the procedures and the detailed processes to use.

In the case of this specific application there is not yet a reference standards with regard to card issuance and personalisation, therefore the operational procedures will be to a large extent proprietary. This includes the distinction between hardcoded applications (stored in ROM and therefore impossible to update) and upgradeable applications (stored as a whole or partly in electrically erasable memory).

6.1 Supply side flow of Train Driving Licence

We depict the supply side flow for the TDL/CC card as in the picture (already presented at page 22 as Figure 1):

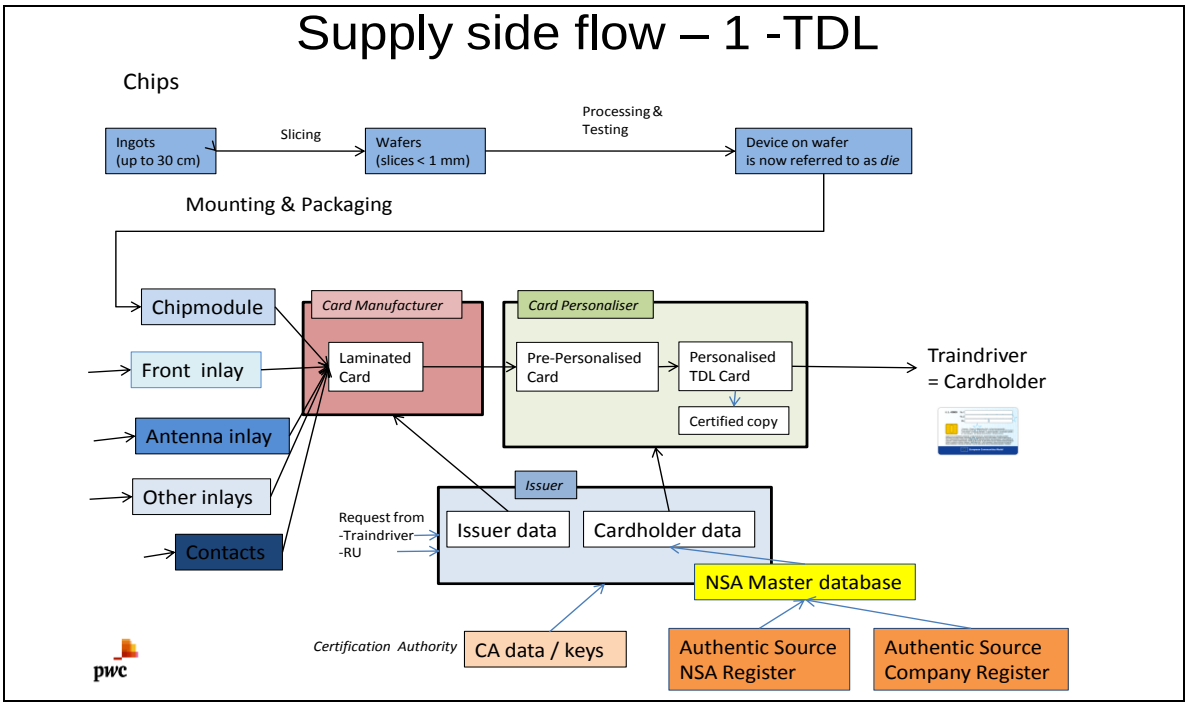


Figure 4: Envisaged supply side flow – TDL/CC

It is assumed that in such flow, the Issuer may be the NSA, a delegated entity or an RU/IM (which can be delegated to issue licences for their own company). We also refer to the Issuer as 'Licence Managing Entity (LME)'.

6.1.1 Pre-Personalisation procedure

The pre-personalisation phase handles all activities regarding card management prior to the moment the card is allocated to a specific individual. This phase is comprised of:

- **Interface with card production:** all actions before issuing are prepared;
- **Issuer aspects:** the actual issuing, e.g. Certification Authority (CA) aspects, logo of the train driving licence, etc.

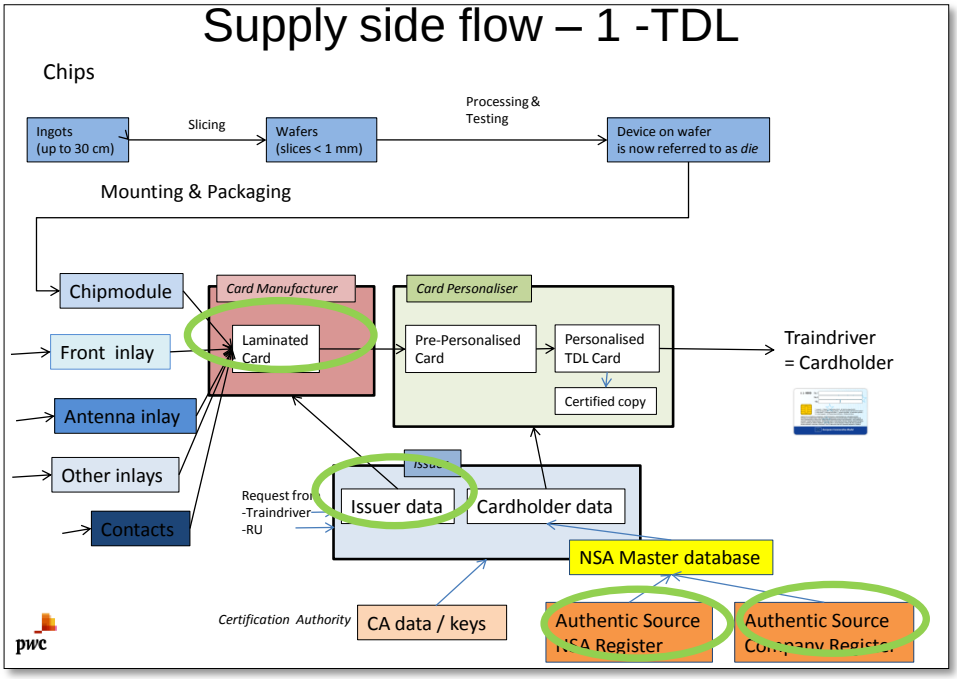


Figure 5: Supply side flow – Pre-personalisation procedure

The main actors and sources are highlighted in green within Figure 5. These steps are described more in detail in the subsequent paragraphs.

After having verified that the Physical Card Management Entity (PME) has produced the right type of card (in terms of hardware and software), the issuer static data is uploaded on the card in the following data element: “EF-DG2 Issuance data”. The TDLME is involved in this action, e.g. they may indicate which logo needs to be printed. Other pre-personalisation aspects need to be taken care of by the PME. The set of cryptographic keys may be uploaded, and the EF.LSO1 data element may be changed.

The issuer can act as the Certification Authority (CA), in compliance with the the ETSI TS 101 456 standards[33]. Below, the high-level procedure related to the CA aspects is described:

1. The CA generates the key pair and ensures that the private key is securely stored. This key pair generation preferably takes place in a Hardware Security Module (HSM).
2. The CA sends the public key to the Root CA for certification and receives the certificate and the Root CA’s public key of the European Root CA.
3. The CA receives the certificate request, consisting of the personal (HR) data and validity period of the card producer and if necessary, the public key of the card personaliser.
4. The CA generates a certificate based on the Private Key and sends this certificate to the card personaliser, together with the Root CA’s public key.
5. The CA records a list of all certified public keys, including a Certificate Renovation List (CRL).

[33] Technical Specification. Electronic Signatures and Infrastructures (ESI);. Policy requirements for certification authorities issuing qualified certificates

6.1.2 Personalisation and issuance procedure

This phase is comprised of personalisation and issuance actions. The main actors and sources are highlighted in green within Figure 6.

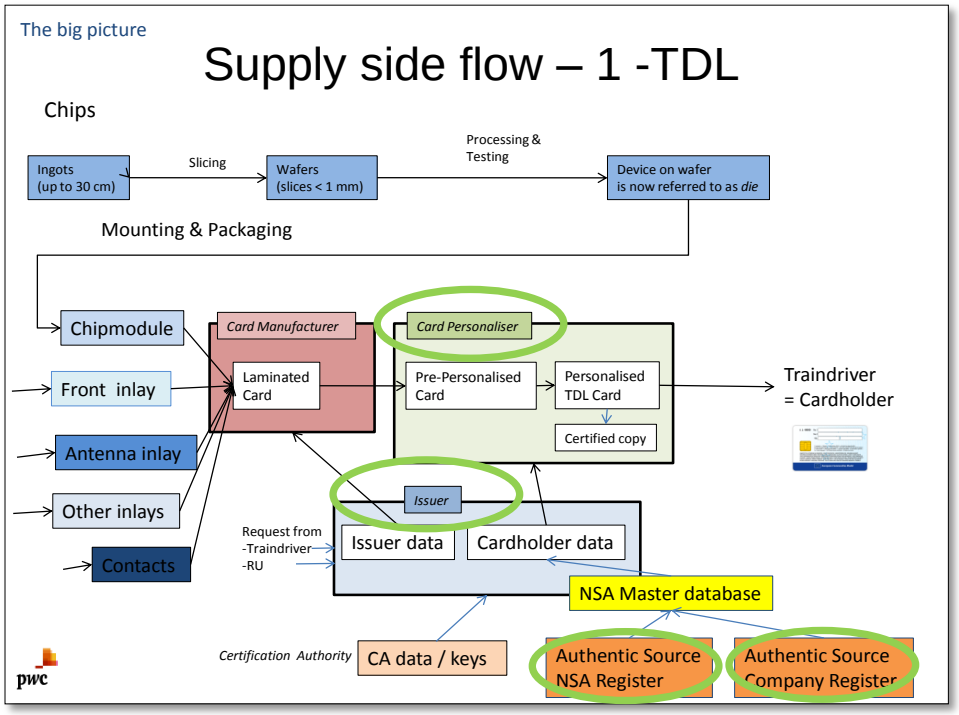


Figure 6: Supply side flow – Personalisation and issuance procedure

6.1.3 Personalisation procedure

Personalisation is the operation that transforms a generic card into an individual specific card that can be used in one or more applications. Personalisation usually includes one or several types, each of which may be done in different stages. The main types of personalisation are:

- Electrical personalisation: loads application codes, user data and cryptographic keys within the chip
- Graphical personalisation: the printing or embossing of text or pictures on the card and associated carrier product(s).

For completeness purposes, magnetic personalisation (encoding the magnetic strip with user data) is also mentioned.

This process is carried out by the card personaliser based on the card request form completed by and received from the train driver of the involved employer.

The competent authority shall issue the licence as soon as possible and no later than one month after receiving all the necessary documents.

In summary, the personalisation procedure can be structured as follows:

- Acquisition of identity of licencee
- Safeguarding licencees data in the TDLME's master file
- Acquisition of initial certification data
- Safeguarding certification data in the CCME's master file

- Data verification (source and outcome should be equal)

These steps to transfer the "EF-DG1 Holder data[34]" are described more in detail in the subsequent paragraphs. The TDLME is involved for licensee's identity information, as opposed to the CCME for certification data.

The PME receives a personalisation file (on the card request form) from the TDLME and ensures that the licencee's identity information is transferred to the card. In addition to the required personal data, this file contains the digitalised photo and signature, and other data as mentioned in the 2007/59/EC Directive. In addition to the actions for a secure data transfer to the card, the necessary controls need to be applied to safeguard the licencee's identity information in the TDLME's master file.

As is the case for the acquisition of licencee data, the correct certification data needs to be obtained and securely transferred to the card. In this case, it is the CCME who provides the initial certification data to the PME and ensures that the required controls are applied to safeguard those data in their master file.

Once the personalisation actions related to the licences and certificates have been performed, the card is ready to be issued to the cardholder.

6.1.4 Issuance procedure

The PME will perform two steps during the issuance procedure:

- **Issuance of licences and certificates**
- **Delivery of the personalised card**

This process is carried out based on the card request form mentioned above.

The PME will take the necessary actions to issue the licences and certificates. They will ensure that the personalised cards are unlocked using the fabricator key and will set the PIN for the user and the transaction key that will be used as part of the final application. They will also ensure that the fabricator's secret key is reset to the card issuer's secret key. The cards are now enabled for operation.

The card issuer prepares the personalised cards for delivery and dispatches the smartcard(s) to the address indicated at the card request form. The card issuer prepares a PIN-letter and dispatches it to the address indicated on the card request form.

The cardholder may use this card in its workplace (e.g.: a depot) where the correct entry of the PIN is necessary before the smartcard will generate an authentic transaction certificate.

The risk that an attacker can take the card at any stage and reprogram the data to his advantage can be hereby assessed and minimised. At each point in the life cycle (pre-personalisation, personalisation and issuance), the data on the card is protected by a secret key. Without knowledge of this key, it is not possible to modify any of the card data in an unauthorised way.

[34] The machine mandatory readable zone(MRZ, EF.DG1) is specified in ICAO Doc 9303 part 1 volume 1. http://www2.icao.int/en/MRTD/Downloads/Doc%209303/Doc%209303%20English/Doc%209303%20Part%201%20Vol%201.pdf

6.1.5 Post issuance procedure

Once the personalised card is delivered, the cardholder can start using it in the day-to-day operations. The main actors and sources are highlighted in green within Figure 7.

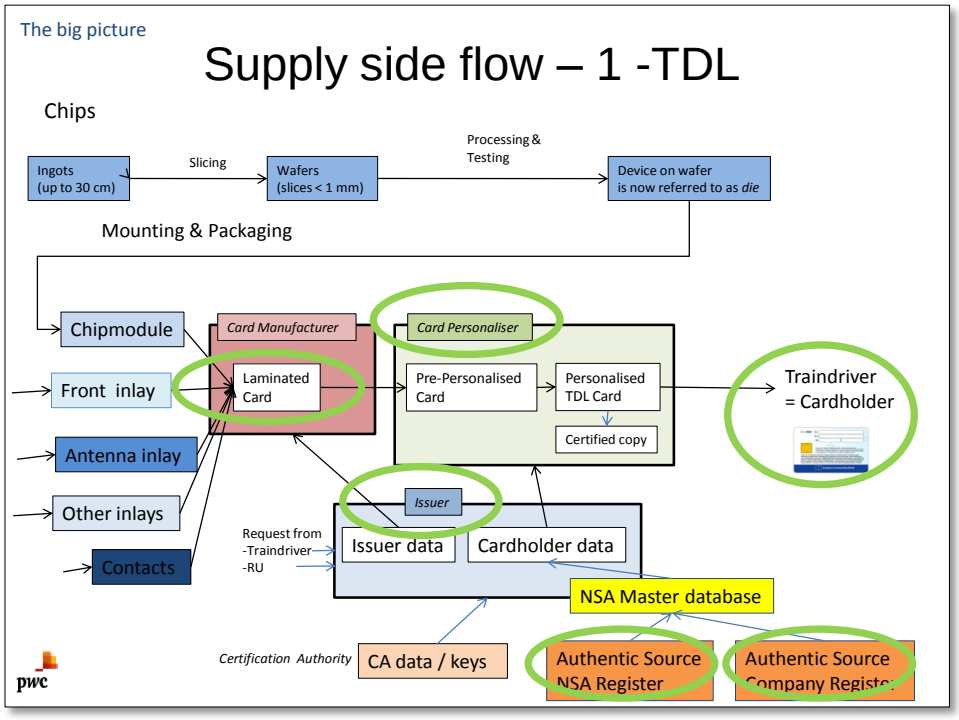


Figure 7: Supply side flow - Post issuance procedure

During these day-to-day operations, additional services by the TDLME and CCME are required to guarantee the efficient use and management of smartcards in the operational environment:

1. Day-to-day support;
2. Revoking licences;
3. Adding/revoking certificates;
4. Modifications;
5. Disposal.

These steps are described more in detail in the following paragraphs.

1. *Day-to-day support*

Day-to-day support should be in place to assist operating staff in deploying the smartcard and relevant document safeguards, as specified in § 5.12.1 . IT Service Management can be deployed in accordance with the ISO/IEC 20000 standards and standardized Frequent Asked Questions list could also be implemented, based on the identified error scenarios.

2. *Revoking licences*

When a cardholder retires or leaves a RU (or the licence needs to be revoked for another reason), the smartcard should be returned to the PME, who then provides a proof of receipt. The PME will update the "EF-DG2 Issuance data[35]".

If a licence needs to be revoked, the smartcard might not be returned automatically. In any case, the status of the smartcard should be adapted. The local data on the chip (both licence as well as certificates) should have an expiry date, such that smartcards with revoked licences could only be used during the period before the expiry date (in case the smartcard was not yet presented to a reader in order to update the data). A trade-off needs to be made between user convenience (the user needs to periodically go to a place with an on-line reader) and safety (user can continue to drive with a revoked licence).

3. Adding/revoking certificates

If a certificate needs to be added/revoked in the "EF-DG1 Holder data", the smartcard needs to be presented to the CCME, who will adapt the smartcard with a reader.

4. Modifications

Due to several occasions, the "EF-DG1 Holder data" can be changed after card production. In addition, the card itself (other data elements and the application(s) running on the card) could be required to undergo significant modifications. Therefore the smartcards should be modifiable. Some cases are shown as follows.

New employer

The licence shall remain valid, provided that the conditions in Article 16 of Directive 2007/59/EC remain fulfilled. A certificate shall become invalid when its holder ceases to be employed as a driver. Therefore, the card needs to be modified.

Renewal

- **Expiry date is reached:** A smartcard is valid for 10 years from its issue date. It is preferably replaced before the old card expires, in order to prevent any inconvenience.
- **Damaged card**: A card with visual damage can be presented to the card issuer to be checked. If it becomes clear that the damage is the result of inappropriate use of the card, a fee could be charged to replace the card. The card holder (or his RU) will be asked to sign a document in which he confirms the card replacement request. The card can then be immediately replaced by the card issuer.

[35] Biometric data (EF.DG2) are contained in the following standards:

- ISO/IEC 19785-1 and NISTIR6529A: Specification of the CBEFF format.
- ISO/IEC 7816-11: Specification of storage format for biometric templates.
- ISO/IEC 19794-5: Biometric Data Interchange Formats - Part 5: Face Image Data: Specification of face images in DG2.
- ISO/IEC 19794-6: Biometric Data Interchange Formats - Part 6: Iris Image Data: Specification of iris images in DG4.

- **Faulty cards:** Faulty cards can be presented to the card issuer to be checked. If no external damage to the card is detected, it will be immediately replaced there and then free of charge.
- **Lost cards:** In case a driver's smartcard is stolen or lost, the following steps should be taken:
  - First, the card must be blocked immediately.
  - The RU should be informed as soon as possible.
  - In case the smartcard already expired when stolen, the employee should apply for a new card according to the regular procedure. In case the card was still valid, the cardholder has to report the theft to the card issuer with a valid passport or national identity card. Then, a new pass will be issued.
  - If the card is lost, the employee may need to file a lost property report at the police station before he can receive a new card.
  - An administrative fee could be charged for every lost or stolen smartcard.

5. *Disposal*

When the cardholder returns the card to the issuer, then the application can be reset by means of the issuer key.

As per regulatory requirements in 2007/59/EC, every card needs to be disposed of after 10 years. However, there might be specific cases in which the card needs to be disposed of earlier on in the card lifecycle. The card should be returned to avoid the existence of non – authorised cards which could end up in the wrong hands.

Also, the card will be disposed of in case the user no longer needs it, cfr. Revoking licences.

6.2 Supply side flow of Complementary Certificates

We depict the envisaged supply side flow for the Certificates as:

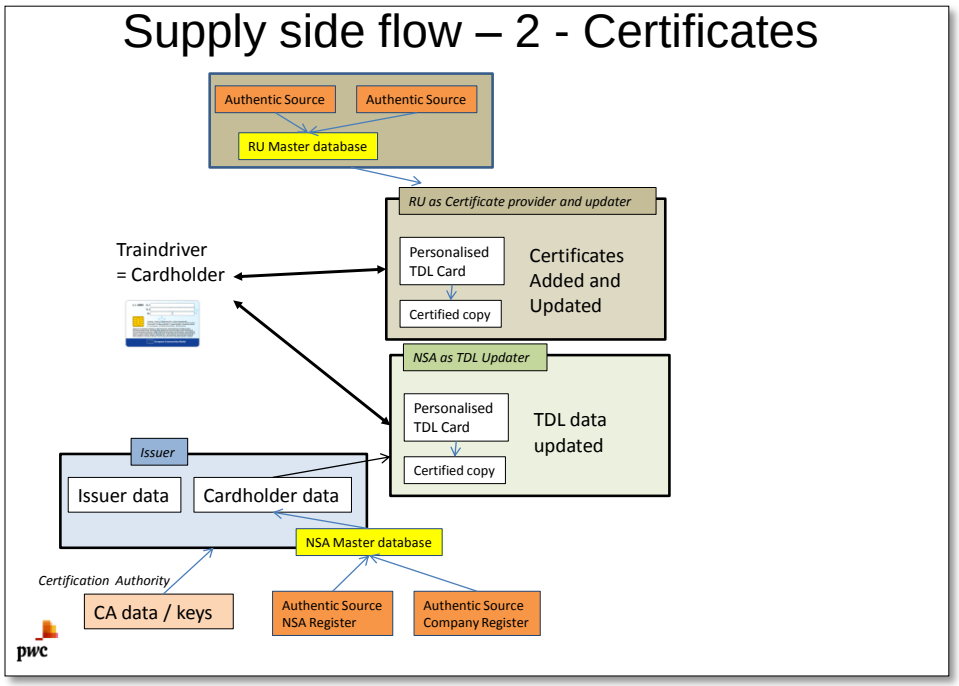


Figure 8 Envisaged supply side flow – part 2 Certificates

Once the smartcard has been delivered to the cardholder by the Card Personaliser, which is under the responsibility of the NSA as issuer, it is valid until suspended/revoked or until it expires after ten years. It contains the relatively static information which is in most cases valid for 10 years. This addresses information such as the examination of the generic tests, the cardholder's picture, the outcome of the period medical tests (with various frequencies).

Once the card has been issued it can be extended by the RU's with the appropriate certificates. There may be different RU's that add certificates onto the card. For instance: in case a cardholder will undergo an examination concerning the professional competence with an RU, the RU will maintain a record of the outcome of such examinations, and will update the certificates on the card accordingly.

Each RU will be responsible for having the appropriate "authentic sources" of cardholder information, and to update the card when required. For example, this may involve a RU master database (CCR), or some other form of (distributed or centralised) register.

7 The case for and against smartcards

This chapter contains the evaluation of the main alternatives using some examples on the use of smartcards, derived from the experience of industry and public administrations. The examples allow a reflection on the possible generic advantages and disadvantages of having cards without chips (non 'smartcards') or having contact or contactless smartcards.

7.1 Chip versus Non-chip card

7.1.1 Advantages of not having a chip

It is cheaper not to have a chip. Typical price ranges are:

- For a basic media in paper or plastic, prices are well below 1 Euro and can go down to below 10 cents. Such media is used e.g. in public transport and is not usable for the TDL/CC solution.
- For a non-chip card, prices range typically from 2-5 Euros. According to the Belgian newspapers, the new (2011) Belgian driving licence has a price of 5,09 Euro charged by the supplier (Zetes). The car driver will be charged about 20 Euro for the licence.
- For a chip-based smartcard the all-inclusive price is often in the bracket of 10-12 Euro or above, depending on the various features.

The management of the card life-cycle is simpler and shorter, since the card cannot be updated. If a change is required, it means reissuing the card. As such, there is no need for 'update' process of the card.

7.1.2 Disadvantages of not having a chip

Not having a chip means it is not possible to store the Complementary Certificates on the card due to the volume of information. As a consequence, this information will only be available for consultation via a register, in practice this means that a Database and the relevant access (according to rights) is required. This incurs the costs of an on-line transaction.

Not having a chip means it may be necessary to issue cards more often. This is depending on the lifecycle of the printed attributes. The more attributes are printed, the more useful the card is. However, since the printing cannot be 'undone', it may mean reissuing a card when an attribute has changed.

Not having a chip means the card cannot be used in electronic transactions. The card cannot be used in electronic workflows or processes to authenticate the driver, nor can it be used to electronically sign documents, requests, or transactions.

7.1.3 Advantages of having a chip

Having a chip essentially means:

- It is possible to store information such as those contained in the Complementary Certificate;
- It is possible to avoid re-issuance in a number of scenarios of changing attributes of TDL and CC (e.g. the estimated frequent updates of route knowledge);
- It is possible for the cardholder to participate in electronic workflows, to authenticate themselves or, to electronically sign documents.

Furthermore, the card may have security features stored on the chip, which makes it significantly better protected against forgery. Particularly, smartcards can contain cryptographic

keys and certificates, both of the card itself and of the card holder. The validity of these keys and certificates can be managed independently from the physical aspects of the cards.

While cloning a card without a chip has a certain degree of difficulty, cloning a smartcard is significantly more complicated. This is the reason why passports are migrating to include a chip, and it is also the reason why debit and credit cards migrated to chips (ref the "pin & chip" debate of EMV – Europay-MasterCard-Visa).

Having a chip will also facilitate usage in other scenarios such as:

- Physical access control to buildings or infrastructure;
- Putting a copy of the Complementary Certificate at the disposal of the card holder, e.g. by allowing him to generate a signed pdf document from his card;
- Tachygraphs or other similar devices.

In a most 'open' scenario such as proposed by e.g. Global Platform[36], the chip allows trusted issuers of applications to install their applications. The scheme holder/original issuer (e.g. ERA, NSAs or the RU) could then actually charge a fee or other compensation for allowing this.

7.1.4 Disadvantages of having a chip

Having a chip makes the card management processes more complicated and makes the card more expensive. Please refer to the target prices listed above.

Having a chip forces the application designer to think well ahead about the applications offered by the chip, including access control to the information on the chip. This is illustrated by comparing e.g. the Belgian versus the German eID card. In the case of the Belgian card, anybody can read out a card (including if it was acquired through theft). However, only a civil servant with the right equipment can update the card. In case of the German card, the card can only be read out by a terminal that has the right cryptographic keys and certificates. Those are managed by the government. As such, the German card is protecting the privacy of the card holder better, but is more complicated to design and manage.

Having information stored inside the chip also has as a consequence that this information needs to be kept synchronised with the register. This means that when reading the information from the chip, there is also a need to go on-line at intervals that need to be defined. To guarantee complete consistency between smartcard and register, and to guarantee validation of the card, an on-line validation should be performed when the card is used. However, often the "Use Cases" of the card can be structured in two sets: those that do require verification on-line (e.g. authentication, inspection), and those that do not (e. g. signing an electronic document).

[36] "*Global Platform is a cross industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. Its proven technical specifications are regarded as the international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models*" (from http://www.globalplatform.org/aboutus.asp). Technical specifications are available at the following address: http://www.globalplatform.org/specificationscard.asp

7.2 Contact versus contactless

7.2.1 Introduction

Contact-based chips make use of physical contacts for their communication with the CAD (Card Accepting Device) or terminal. The connection to electrical power source is required for the operation of the chip that is provided via a contact. Communication protocols are based on the ISO 7816 standards.

Contactless chips make use of radio frequencies for their communication with the CAD (Card Accepting Device) or terminal. The electrical power required for the operation of the chip is drawn from the radio energy. These communication protocols may be based on ISO standards such as

- ISO/IEC 10536 Close Coupling Cards;
- ISO/IEC 14443 Proximity Integrated Circuits Cards;
- ISO/IEC 15693 Vicinity Integrated Circuit Cards;
- ISO/IEC 18000 Family of Air Interface Standards.

As an example, the chips may be based on proprietary protocols such as the popular Mifare©[37] solution from NXP, that is compliant with the ISO/IEC 14443 standard.

7.2.2 Advantages of contact-based chip card

The interaction with the card is under control of the card-holders since they need to insert the card in the terminal or reader.

The transfer of information is inherently reliable, since there is little room for interference between card and terminal. However, skimming attacks have clearly shown that many malicious devices can be built and deployed between card and terminal without the cardholder being aware of this.

As contact-based solutions have been longer on the market than contact-less, there are more manufacturers of readers and terminals, which means competition and lower prices.

7.2.3 Disadvantages of contact-based chip card

The main disadvantage of a contact-based chip-card is the fact that the card needs to be inserted into a terminal or card reader. This takes time and is not always convenient for the card holder.

Furthermore, as the card is physically inserted and contact is made, there is mechanical wear on the contacts of the card. As such, in general, the maximum lifespan of contact-based cards is estimated at five years. Obviously, vendors are continuously working on improving this lifespan.

7.2.4 Advantages of contactless chip card

The main advantage of using a contactless chip is the convenience and ease of use for the cardholder. The card does not need to be inserted; it only has to be brought in the vicinity of the reader or terminal.

As a consequence, contactless cards can have a longer lifespan than a contact card. Vendors are claiming up to ten years of active use for contactless cards.

[37] http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/

7.2.5 Disadvantages of contactless chip card

As already mentioned, as contact-based solutions have been longer on the market than contactless, there are more manufacturers of readers and terminals, which means competition and lower prices for contact-based equipment. It can be expected that this gradually changes over time, e.g. with the rise of contactless readers embedded in smartphones (e.g. some Nokia models already today) and laptops (e.g. some Dell laptops already today).

Contactless chip-cards pose also higher risks if compared with contact cards: in fact there is the risk of remote reading, resulting in potential security and privacy issues (i.e. the card could be read remotely by the company, without the user being aware and using this record to keep a presence log, or could be read/written by a malicious device without the user being aware).

7.2.6 Dual interface cards

Obviously, it is possible to use dual-interface cards which include both contact and contactless interfaces. As a consequence, the card is more expensive and complex.

7.3 Smartcard versus Smart Phone

At the time of elaborating this report, Smart Phones such as Apple's *iPhone* and the various Androids, were becoming increasingly present. They all include a SIM smartcard, and it may be possible in the near future to provision additional applications from other application providers onto the SIM. Some versions of these phones also contain the contactless interfaces. This allows such a phone to engage in a transaction as either a contactless card, or even as a reader. While they hold a promise for the longer term, we do not consider them to be valid alternative for a contact or contactless card for TDL/CC.

We justify this based on following observations:

- The market of Smart Phones is and will remain for some time in full evolution, with significant potential for lack of interoperability. The economic footprint of the TDL is probably too small to drive standards that would guarantee interoperability. Latest development as secure applications via HTTP or HTTPS protocols designed for mobile devices and mobile barcodes may be further investigated in order to evaluate applicability to the system to be designed.
- For various years the arrival of Smart Phones with NFC (contactless readers) has been announced, but so far there are only limited types really available.
- Given the scope and variety of TDL/CC cardholders it seems unrealistic to assume a common hardware or software platform. As such, it might be required to have many variations of the TDL/CC solution, which is costly both in development and maintenance.

7.4 Conclusion

Today's tendency in many industry sectors is towards contactless smartcards, which combine the advantages of those technologies.

It seems feasible to establish a TDL/CC solution based on contact or contactless smartcards. This would bring significant benefits over a non-smartcard, especially from the point of view of having the possibility to remotely update information that is bound to be changed quite frequently. We refer in particular to information related to the professional qualification, namely the locomotives that the driver is authorised to drive and the infrastructure on which the driver is authorised to drive (route knowledge).

8 SWOT Analysis

The appended table summarises the results of the SWOT analysis of a possible smartcard system for the TDL/CC, highlighting factors that can help or harm the implementation of such system. All the factors are further developed below.

	HELPFUL	HARMFUL
	STRENGTHS Harmonised approach and processes throughout Europe Centralised design at EU level (shared decisions and costs) Flexibility (new functionalities can be added beside the pure use for TDL/CC) Specific for RUs/IMs: ensure compliance with requirements Specific for NSAs: improved controls (assist on inspections) Ease of use and information management	**WEAKNESSES** Technology may not be sufficient to manage the whole system No reference standard for building the system Complexity of relations (mainly for source of information and roles in managing data) Lack of harmonisation in display of data Update of information (needs a procedure) The approach of a European system is not sufficient for taking into account RU's specific change request in due time. Production costs Cost of technological components Cost-effectiveness of the system Protection of personal data and security of transactions Resources needed for adding functionalities
	OPPORTUNITIES Adoption of common standards/procedures Development of a centralised system, optimising design, interfaces, database, purchases and costs Automated access to databases/registers Immediate authentication Develop a reference standard	**THREATS** Absence of a reference standard Smartcards can be hacked/affected by viruses Possibilities that cards are lost/stolen (unavailability/misuse/need of procedures) Non familiarity with technologies Persistent lack of harmonisation in display of data In case the smartcard includes function to start a train, a defective cards or mal-functioning card-readers may prevent it to run

8.1 Points of strength

Strengths: characteristics of the system that give it an advantage over others

Two points of strength of implementing a smartcard system are the compliance with legislation and improved control system by the competent authority:

- The implementation of a smartcard system will mainly fulfil the requirement set by the Directive 2007/59/EC: all data concerning a train driver (typically personal data and

limitations, as contained in the TDL and data concerning professional qualification, as contained in the CC) are contained in a single document instead of two as foreseen by the current legislation (Article 4 of the Directive 2007/59/EC).

- The implementation of a smartcard system will assist on inspection foreseen by Article 29[38] of the Directive 2007/59/EC: ensuring a complete list of information on the train drivers in a unique document. Please note though that the accuracy, validity and up-to-date information for each train drivers cannot be ensured by possessing a smartcard, if the driver does not follow the necessary steps to update it (see Chapter 6 for operational features).

In addition, the system is expected to provide a solution that foresees:

- Adoption of harmonised processes and of a common policy throughout the EU (fits in overall interoperable and harmonised framework for railway sector);
- Centralised design of the system involving all actors (shared decision making and costs) so the output (the smartcard) reflects all needs on:
  - Harmonised technical features, like
    - high accuracy in design,
    - use of biometric types ,
    - ease of use,
    - dedicated spaces/functions for national-wide and local-wide requirements;
  - Operating the system (roles, authorisations, possibility to delegate authorisations to different levels of the organisations, personalisation modes, updates, etc.)
    - Stability. A common policy may establish periodical review to implement corrective action(s), if necessary
    - Security of transactions based on roles and access rights;
  - Possibility to include new functions based on the sector's demand, as:
    - starting a train
    - counting working hours
    - access to restricted areas (so enabling prevention of fake access passes).

8.2 Points of weakness

Weaknesses or Limitations are characteristics that place the system at a disadvantage compared to others

There are also weak points in the project of implementing a smartcard system. Here are some general ones:

- Smartcard technology is useful but it may not be sufficient for the realisation of many of the potential benefits desired. Technological and operational aspects need to be carefully considered and a system is to be accurately designed to ensure that it can bring real improvement and benefits.
- There is no standard reference or procedure to describe an entire life-cycle of a smartcard system. Each system is highly customised and requests a careful preliminary analysis and design.

[38] *Article 29* - **Controls by the competent authority**

1. The competent authority may at any time take steps to verify, on board trains operating in its area of jurisdiction, that the train driver is in possession of the documents issued pursuant to this Directive.

For the specific case of the TDL/CC we identify the following point of weakness in relation to the current situation and in relation to the possible additional functionalities that are seen by the sector as adding value to the smartcard system.

8.2.1 Weaknesses in relation to the current situation

- **Complexity of relationships**

The responsibilities for processing data originating from TDL and CC are laid upon different actors:

- NSAs and/or delegated entities[39],
- RUs/IMs that due to their size may have centralised, partially decentralised or fully decentralised tasks related to certification of competencies and administration of complementary certificate (issuance, update, renewal).

These factors are likely to affect the complexity of design and limit the possibility to achieve an efficient system.

- **Lack of harmonisation in the display of data**

The description of the infrastructure (or part of it) on which the driver is authorised to drive is not harmonised. This factor affects very much the capacity, in terms of memory, of the chip that has to contain the information, and consequently, its cost.

- **Update of information**

The smartcard system in itself does not ensure that the data on it are up-to-date. The accuracy, validity and up-to-date information for each train drivers is to be ensured by the prompt recording of data in the register that has to be created to retrieve the information and feed the data in the smartcard. It is therefore necessary to develop both:

  - a technical methodology to update the cards, and
  - a procedure for ensuring that each involved actor promptly proceeds with its part of the update.

- **Cost of technological components**

---

[39] *Article 19* - **Tasks of the competent authority**

1. The competent authority shall fulfil the following tasks in a transparent and non-discriminatory manner:

(a) issuing and updating licences, and providing duplicates, as provided for in Articles 6 and 14;

[…]

2. The competent authority shall not delegate the tasks referred to in points (c), (g) and (i) of paragraph 1 to third parties.

3. Any delegation of tasks shall be transparent and non-discriminatory and shall not give rise to a conflict of interests.

4. Where a competent authority delegates or contracts tasks referred to in points (a) or (b) of paragraph 1 to a railway undertaking, at least one of the following conditions shall be complied with:

(a) the railway undertaking issues licences only to its own drivers;

(b) the railway undertaking does not enjoy exclusivity in the territory concerned for any of the delegated or contracted tasks.

5. Where a competent authority delegates or contracts tasks, the authorised representative or contractor shall be required, in performing such tasks, to comply with the obligations imposed on competent authorities by this Directive.

6. Where a competent authority delegates or contracts tasks, it shall set up a system for checking how those tasks have been carried out and shall ensure that the conditions laid down in paragraphs 2, 4 and 5 are complied with.

The respondents to PwC survey identified hardware and software components as the main barriers for the production of smartcards, mentioning substantial investments as a reason that could represent a high risk in the absence of common specifications.

- **Regulatory aspects**

Regulatory, political as well as network concerns tend to be regarded as main barriers, since they may affects processing of personal data (privacy) and security (as ownership of data in certain Member States).

- **Cost-effectiveness of the system**

The cost/benefit ratio of the entire system, as well as the role of different actors in the financing of the system is a delicate issue. The impact of the system and the cost/benefit analysis are part of the report, in Chapter 9.

We can conclude that to overcome many of the weaknesses, the design of a smartcard system has to be very accurate and take into account several variables, in order to fulfil the requirement currently apportioned to the several actors in the process related to the administration of TDL and CC.

8.2.2 Weaknesses in relation to new functionalities

Some possible additional functionality that may give an added value to a smartcard system (as starting a train, accessing restricted buildings/areas and/or counting working hours) have been identified, however there are some weaknesses that may be configured as:

- **Requirements for a very accurate design in respect to new functions on the sector's demand**
- **Resources needed to include new functions.**

Such new functionalities need to be agreed to a detailed extent and designed in a very accurate manner, taking into account the following constraints:

- **Starting a train** is a task that requires a design agreed at a very comprehensive level. It cannot be limited to having a smartcard with software enabling the desired action. It means that the railway system should agree on having specific on-board equipment to perform this task and we assume that the following aspects should be considered:
  - The project should be included in a high level design (ERTMS?, TSI?) to be adopted at European level;
  - Its life-cycle from conception to disposal should be clearly designed;
  - The obtainment of the authorisation to place into service should be foreseen
  - Resources and plans for equipping all rolling stock and operating the system
- **Counting working hours** would require a set of processes that may be compared to those listed for starting a train; in addition, the system should be designed to be adapted to rules that are currently set at national level.
- Current **access to restricted buildings/areas** is not based on a unique technology, therefore, in view of using a single smartcard, decision should be taken for the equipment or for the migration from the old to the harmonised equipment

8.3 Opportunities

External chances to improve performance of the system

The introduction of a smartcard system may create / lead to opportunities because of the identified strengths described above. In addition, the consulted representatives of the railway sector identified a number of actions that may help to overcome certain weaknesses or limitations on the use of smartcards and, more generally, would help with the production,

introduction and use of smartcards for train drivers if it would be decided to use them. The proposed actions are listed below:

a) **The European smartcard system should be designed centrally**, in order to facilitate and complete the adoption of common standards/specifications for documents and generic information related to train drivers licensing and certification that is in force since 2010 (Regulation (EU) No 36/2010 and Decision 2010/17/EC).

b) **Ideally, the same regulations and systems are implemented across Member States as this would avoid duplication of efforts and positively impact the cost effectiveness of the scheme.**
The overall design of the smartcard system is not achievable by the single actors involved in the train drivers licensing and certification activities.

A common effort, at European level, would be necessary to achieve such a challenging task. It would be therefore desirable that that an overarching entity with the role of coordinator would be responsible for the following activities:

- system high level design (with the sector's involvement);
- procurement of an independent designer possessing all necessary competencies for the whole project;
- development, pilot and test; and
- propose amendment of the legal framework (based on the results of the pilot phase).

The railway sector should take part to each phase of the project as users' representative and provide their contribution as per:

- Description of the relationships in the management of relevant data,
- Extent of layers in the decentralisation (especially for RUs/IMs),
- Security and privacy constraints.
- Data storage

c) **TDLs and CCs databases could be centrally hosted by ERA.** Decentralized implementation with a number of local databases is considered less cost effective, increasing the potential for local variation, difficulties with updates and poor network connectivity.
This very important remark concerns the strong belief of one participant that driver's licences and certificate databases should be centrally hosted by ERA. The main reasons for stating this relate directly to the experience they have with the European Virtual Vehicle Register (ECVVR) where it was proven that a decentralised database is more difficult to set up and maintain.
Centrally hosting the data could:
- Simplify construction, maintenance and adaptability characteristics of the system;
- Minimize set up costs and administrative support;
- Prevent problems when interchanging data between systems/countries;
- Enable harmonization and data sharing across countries;
- Enable single updates/upgrades across Europe.

It should be reminded that the functioning of a smartcard system strongly depends on the existence of databases (the authentic source of data mentioned in § 5.3) and that the Directive 2007/59/EC, complemented by Decision 2010/17/EC, already foresee that such data concerning the TDL and CC are retained in the appropriate registers (NLRs and CCRs), so also the compliance with applicable legal requirement could be also ensured.

d) **The smartcard should give access to the register where this information is available. (in this case privacy concerns are focused on the database and not on the information on the card).**
The interoperability of NLRs and CCRs, and the consultation via the EIN should already give access to registers where the information is available. The privacy and security concerns are to be solved through an accurate design of the tool connecting the registers and the creation of specific rules for authorisation according to the access rights defined in the afore-mentioned Decision 2010/17/EC.

e) **A demonstration project of the System (pilot) may help in surfacing problems and identifying appropriate mitigating actions.**
A pilot phase of interoperability of register is due after the approval of the feasibility study mentioned above. This step may facilitate the understanding of problems and the decisions on the adoption of smartcard system.

f) **A further potential optimisation may reside in the centralization of the purchasing of smartcards at the European level, e.g. by ERA.**
We are aware that a centralised contract for the purchase of smartcards could offer cost and time-saving advantages, especially to small Member States. By preventing local variants, it would also facilitate conformity and a uniform approach in case it was decided to use smartcards. This possibility has to be further investigated, in connection with the development of the system in detail.

In addition, a chip-based solution would allow improved flexibility in distributing the data, since the data would be embedded/stored in the chip, therefore easily recalled and cross referenced. Given the current state of technology with regard to card readers and applications, a standard PC with a card reader (or in the future even a smartphone with a card reader) could be a low-cost platform to read out the data. This would simplify and improve the quality of today's large set of usage and enforcement scenarios. It is assumed that such a chip-based solution is feasible. However, the downside to this would be that as data on the chip will be a "shadow-copy" from a register (database), the data on the chip could be outdated with regard to the register. This can be mitigated by going on-line. The latter obviously implies a connectivity and transaction cost.

We would like to conclude that one opportunity would be to design the smartcard system at the most appropriate time:

- when there is a very limited number of smartcard systems deployed on the field, and that would mean not to have to consider the migration costs, or
- after a first life-cycle is expired, that means approximately 10 years[40], so that the migration can coincide with the obsolescence of the current systems.

This implies that a decision should be taken in due time for ensuring a limited impact on current investments and on spontaneous initiatives that may start to populate the EU scenery.

8.4 Threats

External elements in the environment that could cause trouble for the system

Due to the weaknesses of the envisaged smartcard system, certain threat may emerge: lack of harmonisation, complexity of relations and costs of the system may affect the whole project

[40] Whole life-cycle for IT systems can be estimated in 10 years, as stated in the document: **Electronic Part Life Cycle Concepts and Obsolescence Forecasting,** Rajeev Solomon, Peter Sandborn, and Michael Pecht, in IEEE Trans. on Components and Packaging Technologies, Dec. 2000, pp. 707-717

and impair its accomplishment. To complete the picture, the following threats have been collected from literature[41] and adapted to the specific case of TDL/CCs:

- **There is no standard reference or procedure to describe an entire life-cycle of a smartcard system.** Each system is highly customised and requests a careful design.
- **Smartcards can be hacked into, or even be affected by computer viruses.**

  These threats are all related to system design, which has to take into account from the conception phase all levels (regulatory, technological, operational) in order to fit with:

  - legal requirements
  - roles and responsibilities of the involved actors,
  - security issues
  - safety issues.
- **The cost of production of each card and the whole process of installing a system compatible to the usage of a smartcard is relatively high.**

  It is clear that the cost of the whole system is to be related to the difference in technology used, in the capacity of the memory of each single card, in the necessary equipment for writing/reading and, last, the number of cards to be issued and to the difference in costs to be incurred in different situations, like:

  - Big countries / small countries
  - Big companies / small companies.

  The cost benefit analysis (Chapter 9) will highlight these aspects further.
- **There are chances of the smartcard being stolen or lost.**

  This is a typical risk for all objects/document. The overall system design should consider also the risk that a smartcard is no longer available and the card owner has to receive a copy within a certain delay or can work for a certain period with a substitute document demonstrating the possession of necessary requirements and qualification to perform the assigned tasks (driving certain rolling stock, driving on a certain part of the infrastructure).
- **People who are not familiar with technology may face difficulties in using smartcards.**
- **At times, some information to be included in the complementary certificate is not harmonised** (locomotives that the driver is authorised to drive, infrastructure on which the driver is authorised to drive)**.**

We expect that the design of the system also include appropriate information/training initiatives in order to facilitate the design and implementation of the system.

We can conclude that, apart from costs, the major risk is in the system design. This is the most important message that we can derive from this list.

[41] http://www.buzzle.com/articles/what-is-a-smart-card.html

9 Cost-benefit analysis

9.1 Introduction

As set out in Article 16b.1 (e) of the Regulation (EC) No 881/2004 and in Article 34 of the Directive 2007/59/EC (), the Agency shall by 4 December 2012 prepare a cost/benefit analysis of the introduction of a smartcard where the licence and certificates are combined. The present chapter includes this cost-benefit analysis. Our analysis is based on the impact assessment work undertaken by PwC as part of their study on smartcards (see further details about the study above). As such the chapter presents and discusses the key considerations developed in the PwC study. Furthermore, the assumptions used by PwC in the cost-benefit analysis will in this section be set out and examined in terms of their validity. This step is crucial in order to ensure that the results of the cost-benefit analysis are reliable and robust. Finally, the chapter outlines the key conclusions that can be drawn from the cost-benefit analysis. This is then taken forward in the final chapter where the Agency's position regarding the possibility of using a smartcard for train driver licences and certificates.

The rest of the chapter is structured as follows. Section 9.2 provides an overview of the methodology used. Details on the problem description are outlined in Section 9.3 setting out the rationale behind considering smartcard in this area. In Section 9.4 the objectives for using a smartcard in this context are presented while Section 9.5 gives details about the scenarios used for the cost-benefit analysis. Section 9.6 provides information about the assessment of impacts highlighting the costs and benefits. The various barriers concerning the introduction and use of smartcards are considered in Section 9.7. Finally, Section 9.8 concludes with final remarks.

9.2 Overview of methodology

The methodology adopted for the cost-benefit analysis is in line with the EC Impact Assessment Guidelines[42] consisting of the following steps:

- Problem description
- Identifying objectives
- Developing scenarios
- Analysis of impacts

This approach provides a logical structure for the impact assessment by starting with identification of the problem and subsequently examining possible solutions. Detailed information about these items is given in following sections.

The analysis of impacts is based on a cost-benefit analysis approach comprising a comparison of the reference scenario (do-minimum) and the two alternative scenario (do-something) where costs and benefits are identified / measured. Both quantitative and qualitative analyses are used in order to provide a comprehensive picture of the possible impacts of a smartcard system. Cost estimates expressed in monetary terms are set out, while relevant benefit categories are outlined qualitatively. Although it would have been preferable to have monetized results also regarding benefits it should be noted that such estimates at the moment are very difficult to determine on a reliable and robust basis given the limited empirical evidence and the nature of the benefits linked to smartcard systems in this context.

[42] http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf

In addition to the assessment of costs and benefits the study also considered the various barriers to the introduction of smartcards. One of the barriers concerns the availability of writing and reading devices in the market. This barrier has been examined through a market availability assessment.

The impact assessment has been informed through dedicated data collection. In particular, the data collection consisted of the following steps:

- Desk research where publicly available information about smartcards was retrieved and examined
- Two surveys were launched: one concerning the current use of smartcards in the railway sector and the other on recent experiences in other sectors (e.g. road transport, civil aviation and social insurance)
- Case studies were utilized from both inside and outside the railway sector. The case studies looked at five key aspects: project trigger, implementation specifics, expected benefits, incurred / expected costs and technical characteristics
- Furthermore, the PwC study involved definition of the technical and operational specifications for a smartcard system and the generation / distribution of the smartcards. These specifications will have a significant influence on costs and benefits of the introduction of a smartcard. For the impact assessment the analysis is undertaken using these specifications as the basis

In addition, as part of ERA's review of the PwC work a number of cost-benefit analysis studies on smartcard systems (mostly applications regarding public transport ticketing) have also been reviewed in order to further validate the study findings.

9.3 Problem description

The context for the possible introduction of a smartcard system for train driver licences and complementary certificates is the steps towards gradually establishing a harmonised system for train driver licences and certificates by 2018 as provided for through the Train Drivers' Directive (2007/59/EC). As such a smartcard system is considered relevant particularly in order to support effective inspection and control procedures across Europe. Therefore, Directive 2007/59/EC provides for that the Agency '…shall examine the possibility of using a smartcard combining the licence and certificates provided for in Article 4, and shall prepare a cost/benefit analysis thereof'.

At a more detailed level the general acceptance of smartcards can be linked to several factors:

- Technology is evolving, providing better and faster applications at lower costs (this is key to smartcards where economies of scale is important both regarding development and production)
- Reduced scope for counterfeiting compared to ordinary plastic and paper cards
- More effective inspection process which could lead to higher level of security / safety (although other solutions may fulfil this aspect which are currently also being studied by the Agency)
- Possible efficiency gains in the checking of cards: chip-less cards need to be checked manually whereas smartcards can be checked automatically resulting in reduced lead times

9.4 Objectives

The PwC study identified a range of objectives behind the possible introduction of a smartcard replacing a paper card for train driver licences and complementary certificates. These objectives include:

- To take advantage of combining licences and certificates on a single card
- To improve security through increasing control (this may in turn have positive impact on safety and overall quality of the service provided)
- To move towards one overall access control system (where access can be interpreted as physical access and / or authority to carry out certain activities)
- To allow the possible utilization of additional applications and features (such as registration of working hours and the digital tachograph)

The first one of these is linked specifically to train driver licences and certificates (although could be relevant for other industries). Indeed, the Train Drivers' Directive (2007/59/EC) states in Whereas 18 that 'Such a smartcard would have the advantage of combining these two items (licence and complementary certificate) in one…'. As such the other objectives are not specific to railways although it is mentioned in the Whereas 18 in the Train Drivers' Directive that '...at the same time could be used for other applications either in the area of security or for driver management purposes'.

9.5 Development of scenarios

One reference scenario (without a smartcard) and two alternative scenarios (with a smartcard with variable range of applications) are specified. PwC specified these scenarios and the Agency's review concluded that the scenarios are appropriate for undertaking a cost-benefit analysis regarding the use of a smartcard for train driver licences and complementary certificates. As such the scenarios are specified such that the only difference between reference and project scenarios is whether a smartcard is used or not.

9.5.1 Reference scenario

The reference scenario considered in this impact assessment corresponds to a "minimum scenario". By a minimum scenario we mean that all necessary actions will be taken in order to comply with regulations, but nothing extra is undertaken. These actions are defined in the Commission Regulation (EU) No 36/2010 and do not include the introduction of a smartcard.

The train driver licence shall follow the Community model, the reference colours and the patterns, whose lay-out is provided in annex I to Commission Regulation (EU) No 36/2010.

It should be reminded that detailed information on qualification of train drivers (infrastructure on which the driver is authorised to drive, rolling stock that the driver is authorised to drive, linguistic competence) is contained in the complementary certificate, that is today a paper document.

9.5.2 Alternative scenarios

Several alternative scenarios can be envisaged for the introduction of a smartcard, of which we selected two. One alternative is the use of a basic smartcard that stores data regarding train driver licences and certificates. Another alternative is the use of an enhanced smartcard, which not only stores data regarding train driver licences and certificates but also carries other applications and features. Our research undertaken as part of this work revealed that additional applications and features for smartcards are readily available and/or can be developed relatively easily.

Thus, we define the two alternative scenarios:

Alternative scenario 1 - A basic model of the smartcard:

> In this scenario, the chip embedded in the smartcard only includes data about the driving licence of the train driver and additional certificates.

Alternative scenario 2 - An enhanced model of the smartcard:

> In this scenario, the chip embedded in the smartcard not only includes data about the driving licence certificates of the train driver but also carries other data and/or applications (e.g. credentials to start a train, record of driving time)

The impact of these scenarios will be assessed in the following sections.

9.6 Analysis of the impacts

This analysis focuses on the costs and benefits associated with the two alternative scenarios (introduction of smartcard for train drivers with varying range of applications) compared to the reference scenario without a smartcard. As such the impact is the difference between the alternative scenario and the reference scenario. As such it is important to stress that analysis of costs and benefits of smartcard systems contains substantial uncertainty at the moment due to the relative short period of time in which such systems have been in place in practice limiting the possible robust empirical indications.

9.6.1 Assumptions

Before going into the details regarding costs and benefits an overview of the assumptions used in the analysis will be given. This will also consider the validity of these assumptions.

Under the reference scenario, card design has been specified in EU Commission Regulation(EU) No 36/2010, and there is no chip hence no on-card or off-card application

This assumption is valid to make in order to facilitate the comparison between alternative scenarios and reference scenario.

- *Under the reference scenarios, however, the application(s) have to be designed, both on-card and off-card. For each alternative scenario, we elaborated two estimates for these application development costs*

The assumption regarding development costs is correct. As such this would facilitate analysis at a more detailed level in terms of cost categories.

- *The cost per card for the body+chip is assumed to range from 3,5 to 5,5 Euro (per card, in large quantities, i.e. > 10.000 units)*

These unit costs seem consistent with available evidence in this field. Therefore, this assumption is valid.

- *A price ranging between 25 to 50 Euros can be charged to the end-user*

This price range seems realistic taking into account that this expense may be covered by the train driver or his employer.

- *Also, a smartcard based solution typically relies on a Public Key Infrastructure / Certification Authority (PKI / CA) and the modeling is undertaken with the assumption that the two alternative solutions can be secured in this way*

This assumption is justified by reference to available examples, e.g. the digital tachograph systems in the road sector are based on a PKI. On this basis it appears to be reasonable to include this assumption.

- *The model assumes that it is a subsidised system from public institutions or railway undertakings, i.e. the commercial income does not need to match the cost.*

As such this assumption seems appropriate. If this is not the case it should be noted that the assumption does not influence the cost estimates but only the net-cost after taking into account total external income streams. In effect, the assumption allows due attention to the benefits of a smartcard system (irrespective of whether the railway sector or society cover the incurred costs). The size of the commercial income is only of importance for the financing of the system but not linked to the actual benefits incurred.

- *We assume that registration, production and management of cards are all performed in-house. Therefore, specific set-up costs for card production and registration need to be taken into account as well as specific bureau staff costs.*

The Agency agrees with this assumption as the focus should be on identifying all relevant costs related to a smartcard system. It may be that if these functions are performed externally (not in-house) by specialized entities there could be possible cost savings but on the other hand there may also be an increase in transaction costs.

- *The model includes the following smartcard applications: an application to store driving licences and certificates, (Alternatives 1 and 2); a digital tachograph (only Alternative 2). Other applications can be added, but cost estimates of them have not yet been included in this model.*

This means that the enhanced smartcard in Alternative 2 comprise only a digital tachograph as an additional application compared to the basic smartcard in Alternative 1. The cost incremental by going to the enhanced smartcard version therefore only reflects this aspect. Additional costs may therefore be incurred if other applications are added as well. However, it should be noted that this application is probably the most important additional application.

- *We assume that the full set of smartcard enabled services can be implemented in year 1 and that cardholders will be transferred to the multi-application card either when their existing licence needs to be renewed, or when a decision is made for the phased transfer of all cardholders (by individual service) to smartcard by a certain point in time.*

This type of assumption is necessary for allowing the calculation of yearly based cost and revenue figures over the relevant appraisal period (7 years). Obviously, it is an empirical question whether the full set of smartcard enabled services can be implemented in the first year (Year 1). However, we find that this trajectory is reasonable. Basically, it means that set-up costs are incurred in the beginning of the appraisal period rather than later which may also have implications for the income stream.

- *The model assumes that all the technical elements of the scheme will need to be upgraded after 7 years. In order to fund this, it makes a yearly provision for a "technology refresh" and future development costs. This is calculated by spreading the total technical set-up costs over 7 years.*

It is appropriate to take this cost aspect into account as part of the analysis of the costs involved for a smartcard that is assumed to be upgraded after 7 years. Such upgrade addresses also the risk of obsolescence which can be a major factor for life cycle costs. Especially, in the context of IT systems or parts the normal life cycle (without upgrade) can be rather short (typically around 10 years or even shorter) compared to other products.

- *The model calculates values for the full cost of production and implementation. However, elements of application development and ongoing support and maintenance can be outsourced. In that case, the model has to be adapted slightly.*

The Agency agrees with this assumption. Our view on this aspect is similar to the points put forward regarding the assumption that registration, production and management of cards are performed in-house.

- *This cost model does not consider any revenues from, for example, sponsorship. The only revenues included in the model are the revenues received at the time the card is issued. It is assumed that train drivers will pay a moderate fee when they receive their driving licences (as mentioned above).*

It would be rather speculative to assume positive income streams from sponsorships or other sources. Therefore, assuming no revenues linked to the smartcard system (other than the fees charged to the user) is appropriate. As such the assumption does not influence the costs of the system but merely the financing of it which is outside the scope of this impact assessment.

Additional assumptions regarding the various cost elements (incl. unit costs) and related parameters are documented elsewhere in the PwC study. In particular, the following cost categories are considered:

- Set-up costs
  - Infrastructure
    - Servers & software
    - Comms (per connection)
    - PC & software
  - Public Key Infrastructure
    - Design of secure facilities
    - Design and development of PKI
    - Implementation of PKI
  - Card production
    - Printer (with integrated smartcard readers) & software
    - Card Management System
    - Letter printer
  - Registration
    - Image Capture-Digital camera standard licence
    - Image Capture per seat licence
    - Image capture – Scanner Installation and Configuration
    - Reader (If required)
    - PC (As required)
  - Cards
    - Card design Costs
  - Accommodation
    - Office Costs General
  - Project cost
    - Project management / consultancy / user requirement
    - Technical staff
    - Business staff
    - Legal costs
  - Training
    - Staff Card Production and Procedures
  - Application development costs
    - Applications
- Operational costs
  - Cards
    - Card production cost
    - Replacement cost
    - Wasted cards cost
    - Hardware and software maintenance
    - Consumables

        - CMS S/W Maintenance
        - CMS Server licence
        - PKI costs
    - Registration
        - Application form production
        - Post cost
    - Bureau staff costs
        - Manager / Supervisor
        - Operators
    - Ongoing support and maintenance
        - Applications
        - Technology refresh

The Agency has reviewed these other assumptions and finds these appropriate for modelling the key cost elements related to the introduction of a smartcard system for train driver licences and certificates.

9.6.2 Costs

The results of the cost calculation are provided in table 7. These cost estimates have been reviewed internally in the Agency and validated. As expected, the costs for the alternative scenarios are higher than those for the reference scenario. The introduction of the basic model of the smartcard results in significant higher costs than the introduction of an ordinary card. The cost difference between the enhanced model of the smartcard and the basic model of the smartcard is not that big. These cost increases for on the one hand the basic model of the smartcard and on the other hand the enhanced model of the smartcard, have to be compared with the benefits these models imply.

It is also clear from these tables, that the final balance is better for large countries (estimated for 22,000 licences) than for small countries (estimated for 170 licences). This is due to the fact that large countries receive significantly more revenues. These revenues seem to outweigh the additional costs large countries have to bear. Another factor would be economies of scale regarding card production costs with lower unit costs for higher volumes that are available for the bigger countries (in fact it can be noticed that the operational costs under Alternative 1 are only about 3,5% higher for a large country compared to those incurred by a much smaller country). This is factored in within the minimum and maximum values.

It should be noted that these results should be read and interpreted together with the benefits defined in the next section.

Small country (170 licences)						
	Reference scenario Ordinary card		**Alternative scenario 1** Basic model of the smartcard		**Alternative scenario 2** Enhanced model of the smartcard	
	Min	**Max**	**Min**	**Max**	**Min**	**Max**
Setup costs Including Application Development	88.800€	185.550€	1.148.270€	2.666.550€	1.398.270€	3.166.550€
Other operational costs	721.822€	1.142.916€	1.906.073€	4.520.299€	2.374.823€	5.457.799€

Total External Income Streams	5.441€	6.716€	5.596€	11.193€	5.596€	11.193€
Balance	-805.181€	-1.321.750€	-3.048.747€	-7.175.656€	-3.767.497€	-8.613.156€

Large country (22.000 licences)						
	Reference scenario Ordinary card		**Alternative scenario 1** Basic model of the smartcard		**Alternative scenario 2** Enhanced model of the smartcard	
	Min	**Max**	**Min**	**Max**	**Min**	**Max**
Setup costs Including Application Development	88.800€	185.550€	1.280.270€	2.864.550€	1.530.270€	3.364.550€
Other operational costs	786.695€	1.234.806€	2.009.095€	4.680.563€	2.477.845€	5.618.063€
Total External Income Streams	703.013€	868.013€	723.344€	1.446.688€	723.344€	1.446.688€
Balance	-172.483€	-552.344€	-2.566.021€	-6.098.425€	-3.284.771€	-7.535.925€

Table 7: Cost calculation – 7-year total including set-up cost for a small and a large country

As such the additional total costs across Europe, over and above the ones incurred in the Reference Scenario, could then be determined on the basis of the information contained in table 7. As for the set-up costs (incl. application development) that would be incurred in Year 1 totals for EU 27 (excl. Malta and Cyprus) have been calculated based on these estimates. The results suggest that for EU 27 there would be costs of 68 mln Euros under Alternative 1 and 82 mln Euros under Alternative 2 over and above the costs incurred in the Reference Scenario. To these costs should obviously be added the operational costs (which are significant higher for both alternative scenarios compared to the Reference Scenario).

9.6.3 Benefits

Two types of benefits can be identified:

- Benefits linked to both alternative scenarios
- Benefits linked to additional functions (alternative 2)

9.6.3.1 *Common benefits for Alternatives 1 and 2*

Below, the benefits relevant for both alternative scenarios from the introduction of a smartcard system are set out(for details about the scenarios see above). These benefits are linked to specific stakeholders.

- *The **competent authorities** or National Safety Authorities referred to in Article 16 of Directive 2004/49/EC.*

The competent authorities are responsible for tasks such as issuing and updating licences, organising periodic examinations and tests, suspending and withdrawing licences, publishing and updating registers of accredited persons and bodies that cooperate with the European Railway Agency to ensure interoperability of the registers.

- It will be possible to update licences without issuing new cards assuming that all variable data such as expiration date, name of employer, and address is not printed on the card but only stored on the chip. Data printed on the card is invariable data such as name, date and place of birth, and licence number. The updating process for the alternative scenarios will be simplified and will result in time as well as cost savings.
- The results of periodic examinations and tests, as well as other relevant data, can be easily stored on the chip (as well as in the database). As a result, train drivers who have their driving licence on them can prove they took the necessary tests should there be a dispute at the time a check is performed. This is not unimportant as Member States today do not have access to the database of other Member States. If all data is stored on the chip, access to the other Member State's database is no longer required for checking purposes. This facilitates the inspection process and may lead to detection of non-conformities that may otherwise potentially lead to accidents and therefore increase safety in the railway sector.
- The update of registers should go hand in hand with the update of the data on a train driver's licence. If any data in the register is changed, the licence will automatically be updated the next time the card is connected with the register. If additional certificates are added to the chip of the train driver's licence, the register will be updated automatically the next time the card is connected with the register. There will be fewer inconsistencies or errors, which again results in better control conditions and an increased level of safety.
- Due to the fact that smartcards are hard to falsify, there will be less fraud and more trust in the railway sector, facilitating the integration between different NSA's and between RUs/IMs and NSA's.

- *The **train drivers**, meaning the person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous responsible and safe manner.*
  - Reduced risk of tampering with data, which leads to increased fairness between all train drivers. Their qualifications and certificates will not be questioned, even when they change employers or their licences are checked in another Member State that has no access to the registers in which their data is stored. Train drivers who have their driving licence on them can always prove they took the necessary exams and periodic tests should there be a dispute at the time a check is performed.
  - Checks will be performed more efficiently, saving time not only for the persons performing such checks (i.e. the inspectors) but also for train drivers in their daily operations.
  - A higher level of scrutiny and a lower number of counterfeit cards will contribute to the safety of railway operations.
- *Other **crew members performing safety-critical tasks**, meaning staff who are not train drivers but who help to ensure the safety on the train and of the passengers and goods being transported.*

- Checks will be performed more efficiently, saving time for the persons performing such checks (i.e. the inspectors).
- Inspectors will only have to carry a small handheld card reader instead of a laptop in order to perform their checks. Moreover, their checks will be more effective since they will be able to read the data on the driving licences of train drivers from their own Member State as well as of train drivers from other Member States.
- Normally, train driver licences and certificates are issued in a single language, that of the company employing or contracting the driver. Information on the train driving licence and on the complementary certificate would benefit of availability in more than one language, which is possible when smartcards are used. The chip allows storing the same data in different languages.
- Simplification of the inspection process and reporting to the NSA's, regarding:
    - number of drivers holding a licence;
    - number of trained drivers, type of certificate they hold, type of trains they can drive, etc.;
    - number of "sanctioned" drivers (e.g. who is suspended/whose licence has been withdrawn?).

- *The **railway undertakings or infrastructure managers employing or contracting train drivers** :*
    - Railway undertakings / infrastructure managers will be sure that the driving licence a train driver possesses will not be falsified. This will save them time and money since they do not have to carry out additional research or tests in order to make sure that the train driver has the needed qualifications.
    - Due to the fact that smartcards are hard to falsify, there will be less fraud and more trust in the railway sector, facilitating the integration between different RUs/IMs and between RUs/IMs and NSA's.
- The **Passengers**, people making use of the services the railway sector offers
    - Due to the efficiency gains in the inspection process and the safety improvements, passenger satisfaction is likely to increase. At the same time, communication towards passengers will be very important in order for the satisfaction levels to go up. Increased safety and passenger satisfaction may result in increased railway usage, but there is still substantial uncertainty regarding the influence a smartcard may in fact have on passenger satisfaction and patronage.
- **Society at large**
    - The opportunity for European Member States to achieve a leadership position in the smartcard business may result in wider socio-economic benefits such as increased employment.
    - There will be a reduced risk of tampering with data. Movements of goods across Member States can be improved thanks to a simplified and safer access policy.
    - Data storage on the chip will result in better inspection of foreign train drivers' qualifications. This will ease cross-border traffic and may lead to better train driver mobility. This mobility is important with an eye to balancing the shortage of train drivers in some Member States with the surplus of train drivers in other Member States.

9.6.3.2 *Benefits solely linked to Alternative 2*

A number of extra applications may be loaded onto the chip of the smartcard. This brings extra costs (as highlighted in Table 7) but also yields additional benefits.

Digital tachograph

The most important and most obvious application for the smartcard is the digital tachograph. A tachograph is a device fitted to a vehicle that automatically records its speed and distance. It can be used to record driving times and rest periods. As such, it is a monitoring tool that ensures that train drivers comply with the mandatory rest times. According to the survey and follow-up interviews performed in Task 1, it remains difficult to monitor the rest times of international train drivers.

The benefits of this application are likely to be:

- enhanced safety;
- identification of violations of regulations governing driving times. This is important as it is difficult today to check the driving times of international train drivers. Moreover, regulations governing driving times differ from one Member State to another. With the help of the digital tachograph, driving times can be monitored, also when train drivers are working outside their (EU Member State) home country;
- improved drivers' working conditions;
- improved operational processes for driver companies.

Mandatory requirements and voluntary requirements

The train driving licence and the complementary certificate have been developed in the specific context of the RUs/IMs safety management system, which is a mandatory requirement that covers core railway operational activities. However, a smartcard could also be linked with an integrated management system, which would be a voluntary requirement incorporating data that pertain, for example, to the qualifications of the driver covered by other management systems, such as a health and safety (occupational) management system or an industry scheme supporting the quality and safety of the transport of dangerous goods.

Physical access control

The card can also be used as a means to provide access to the driver's compartment. Without a card, it should be impossible to access the area and start the train. As a result, incidents involving unauthorised people gaining access to the driver's compartment can be prevented. These tasks are more for registers of the company: the result should be a suspension of the validity of the card (that may be reflected in the denial of access to trains.

Recording continuing personal and professional development)

Train drivers acquire experience on the job as well as by attending certain training programmes that are in addition to the competence management system concerning professional competencies on infrastructure, rolling stock and language skills necessary for maintaining a valid complementary certificate. This may be the case for drivers who have qualified as trainers.

All records tracking the development of personal and professional competence of the train driver could be stored on the card, so that there is transparency and up-to-date information about the life-long learning experience of every train driver. This may motivate train drivers to attend training programmes, e.g. for transport of dangerous goods.

Use of data for in-house applications

If driving times are automatically stored on the card, this information can be sent to in-house applications such as payroll, HR and financial management databases. This will lower the administrative burden particularly for train drivers who work across different Member States.

Cashless vending

Smartcards can also be used for cashless vending. The benefits of this application depend on the amount of restaurants and vending points for drinks and food for railway personnel.

9.6.4 Comparison of benefits and costs

Based on the different applications, smartcards with different features can be developed. The figure below shows how the applications can be accumulated into a multi-application smartcard. Every additional application will result in additional benefits as well as additional costs. The additional costs and benefits of all applications should be weighed.

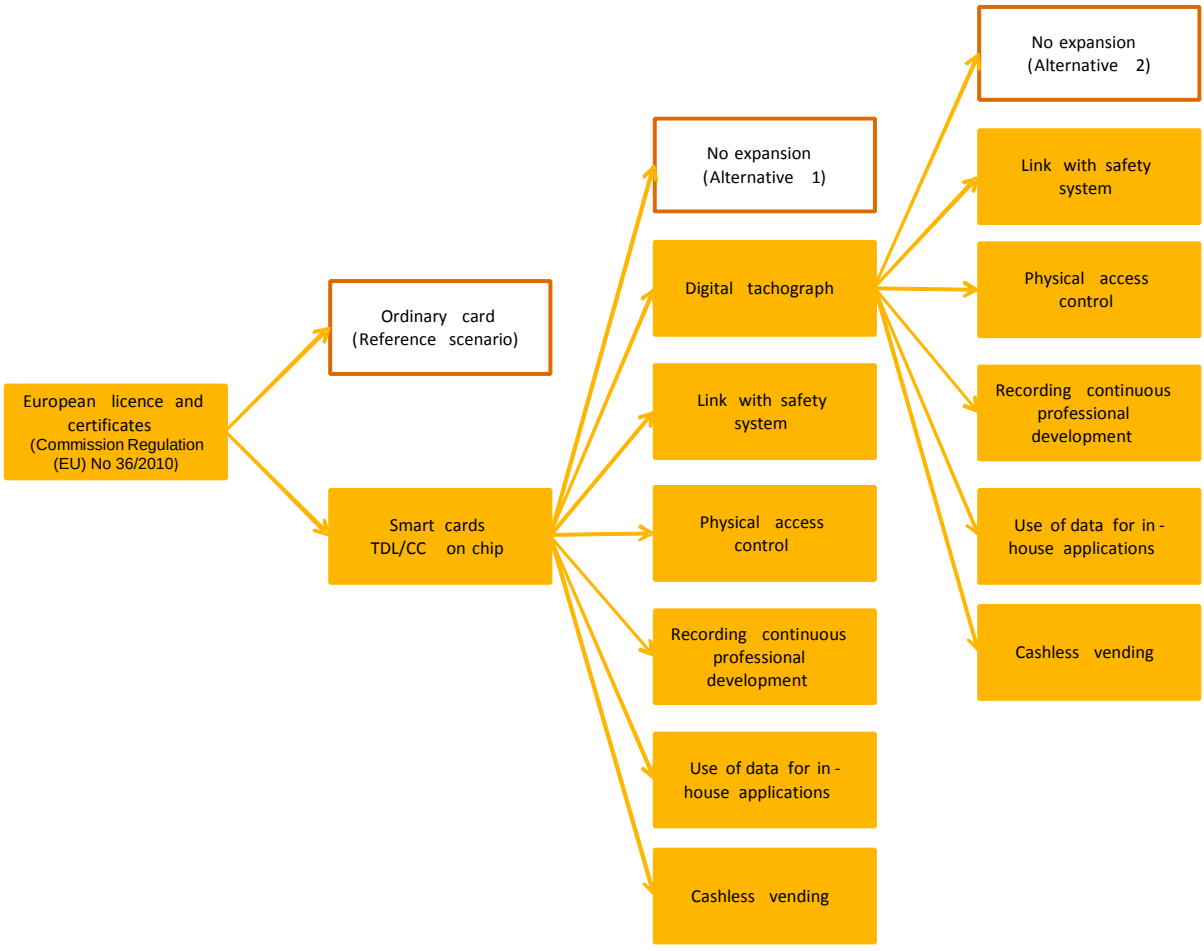


Figure 9: Alternative scenarios

For the reference scenario and the two alternative scenarios, costs and benefits have been identified and monetised where possible. It is very difficult to capture the benefits in formal monetary terms, which complicates setting them off against the costs. Nevertheless, we are

convinced that there is a great opportunity for introducing smartcards in the railway sector as long as careful attention is paid to the selection of applications and features of the smartcards.

One of the key benefits we envisage with the implementation of smartcards is the additional usage of smartcards for driving time and rest time registration. According to our analyses, the cost to implement a smartcard with the digital tachograph as an additional application is only between 24 and 30% higher than for the case without digital tachograph. Some other applications and features could be added at relatively low costs but with significant benefits.

The costs of implementing a smartcard solely for the purpose of data storage of train drivers' licences and certificates are significant, compared to the expected benefits. If smartcards are enhanced with additional applications, however, the benefits outstrip the additional costs at a certain point in time. Depending on the number and choice of additional applications, the final balance may vary considerably. The exact impact of a multi-application smartcard for train drivers should be assessed in more detail.

9.7 Potential barriers for smartcards

The various stakeholders (notably NSAs and RUs) may face a number of barriers in introducing a smartcard system. In particular, the following aspects were put forward in the PwC study:

- Lack of a fully harmonised train driver certification system across Europe where the current situation being a transitionary one moving from a non-harmonised system
- Data protection relating to personal data
- Lack of common specifications for hardware and software which main limit deployment of smartcards due to significant investment in production and implementation
- Regulatory, political and network concerns when introducing smartcards: Certain stakeholders may have limited interest in smartcards for competitive reasons
- Disproportional costs for small countries of introducing smartcards compared to larger countries due to the strong presence of economies of scale
- Migration costs for those Member States that have already introduced smartcards or are in the planning phase of doing that. These Member States may therefore have a certain resistance should European legislation require a specific type of smartcard

These aspects are important to take into account in the Agency's recommendations regarding the possibility for introducing a smartcard system.

On the other hand concerns regarding availability of smartcard writers and readers appear to be less significant. These are broadly available in the market and the PwC study includes a small selection of different types without being exhaustive. It is mentioned that the actual selection needs to be based on a careful analysis of the entire market.

9.8 Conclusions of impact assessment

The results of the cost-benefit analysis reported in preceding sections demonstrates that a smartcard system in this area would entail significant costs particularly (fixed) set-up costs. A smartcard limited to allow for the data storage of train drivers' licences and certificates (alternative 1) is likely to lead to substantial costs compared to the benefits. On the other hand moving to an enhanced smartcard system with additional applications may only lead to limited further cost increases (notably the case of a smartcard system with a digital tachograph). These additional applications are likely to bring additional benefits which may even outweigh the costs incurred. However, there is limited quantified information available about the benefits (in contrast to costs where orders of magnitude estimates are available). A further difficulty is that small countries face disproportionate costs of smartcard system compared to larger countries due to the presence of economies of scale in this area.

Overall, our view is that further analysis is required to weigh the costs and benefits of the smartcard system, particularly with respect to additional applications and features that may be integrated in the smartcard (a multi-application smartcard). This conclusion seems to be consistent with other recent cost-benefit analysis studies regarding smartcards (though in the area of public transport ticketing). Indeed, one of these studies stated in its conclusions that *'…more are clearly needed*[43]*'* with reference to more detailed information on the impacts of smartcards. As such postponing the eventual introduction of a smartcard system would allow further harmonisation for train drivers' licences and certificates such that by 2018 all drivers would hold a harmonised European licence / certificate. At the same time postponement would facilitate gathering of additional evidence incl. further indications regarding the situations where more effective inspection and control is required as well as practical examples of smartcard systems in this area.

[43] http://www.its.berkeley.edu/publications/UCB/2008/PRR/UCB-ITS-PRR-2008-14.pdf

10 Conclusions and recommendations

Once analysed all the information on the use of smartcards (technical, organisational and economic) as also the challenges related to the design, implementation and maintenance of a smartcard system for the licensing/certification of train drivers, we can highlight some important messages:

1. Smartcard technology is useful but it may not be sufficient for the realisation of many of the potential benefits desired. Technological and operational aspects need to be carefully considered and a system is to be accurately designed and a pilot phase is to be considered, to ensure that it can bring in real improvement and benefits.
2. The operational context and the articulate relation between actors having different responsibilities (NSA for data concerning the train driving licence and RUs/IMs for data concerning the complementary certificate) make the system more complex than some similar scenario (Tachograph/Tachonet for lorry and bus drivers) and therefore more expensive and maybe not sufficiently precise. Please refer to § 3.2 for details on Tachograph and the Chapter 5.3 for the identification of the TDL/CC scenario.
3. The number that is expected to be using the smartcards is around 200k train drivers. The cost pro-rata of a single card would be very high and it would be relatively high for small countries. The benefit of having an up-to-date information on train drivers qualification and medical fitness could be achieved by using an IT utility to access the registers of entities involved (NSAs that issued the TDL and RU/IM that issued the CC), via internet, consultable from pc, laptops or smartphones.
4. The data pertaining to the professional qualification in the complementary certificates (rolling stock that the driver is authorised to drive; extent of the infrastructure on which the driver is authorised to drive) are not yet harmonised. Therefore the quantity and type of information cannot be foreseen. The quantity and length of records is not fixed, so it may depend from national implementation rules and on company practices in relation to EC's legislation. There may be a harmonised codification for the infrastructure part as and when the Infrastructure Register to be created in accordance with the TSI Infrastructure[44] and with the Commission Implementing Decision 2011/633/EU[45] will be adopted. For the time being it is necessary to foresee a wide memory for the microchip which has significant influence on costs.
5. The use of smartcards could be more efficient in case they are used for further purpose than for monitoring only. Some actors have indicated functions as the recording of driving time and/or the use of the card for starting a train. Such functions request a very broad reflection and involvement of a wide range of actions, which include the preparation of the

[44] Commission Decision 2008/217/EC of 20 December 2007 concerning a technical specification for interoperability relating to the 'infrastructure' sub-system of the trans-European high-speed rail system (OJ L 77, 19 March 2008, p. 1) and Commission Decision 2011/274/EU of 26 April 2011 concerning a technical specification for interoperability relating to the 'energy' subsystem of the trans-European conventional rail system (OJ L 126, 14 May 2011, p. 53).

[45] COMMISSION IMPLEMENTING DECISION (2011/633/EU) of 15 September 2011 on the common specifications of the register of railway infrastructure (OJ L 256, 1.10.2011, p. 1).

legal basis, the technical specifications for the system in order to include all functionalities and identification, design, testing and approval of necessary equipment (hardware and software).

6. Last but not least, the data to be inserted in the smartcard should mirror those contained in a register that already must be kept and made available by RUs/IMs according to Article 22.2 of Directive 2007/59/EC. The update process should be accurate and succeed in defined periods.

The current scenery shows that there are varied and complex relationships between actors involved in the licensing/certification system. However this report provides only a snapshot of the situation: whenever a decision to introduce a smartcard system would be taken, a thorough investigation of the involved actors will have to be carried out, especially as far as the centralization, decentralisation and delegation of tasks in the licensing and certification processes are concerned. Further actors may have to be considered as a result of the necessarily detailed analysis of the reference scenario, preliminarily to the system design.

Then, a European smartcard system should be designed very carefully to ensure that all roles and responsibilities are fulfilled, ensuring that the licensing activity is carried out in a safe, secure and cost-effective manner.

We can conclude that the introduction of a smartcard system involves remarkable challenges in regard to data storage concerning infrastructure und rolling stock competence due to missing harmonised specifications. The low number of cards needed by the market in addition reduces the cost-effectiveness in particular when taking into account a relatively limited benefit (facilitated supervision). Additional operational functions could increase the benefit but would assume major and time requesting preparatory work on other regulatory fields.

The current work on improving interoperability of licence and certificate registers may show that the prompt availability and updated plus accurate information from the authentic source is already sufficient for the needs of the railway sector. Costs of designing, implementing and maintaining a smartcard system could then be avoided.

On this background, the following recommendations should be taken into consideration:

- Further steps on the implementation of a smartcard system for train driver licences should be delayed until the processes mentioned above will provide for more supportive circumstances.
- Appropriate solutions to use smartcards combining train driving licences and complementary certificates should be related to the solution that will be found for the interoperability of the Registers.
- In addition, projects developed at EU level[46], as the IMI (Internal Market Information System), as platform for the exchange of information and the forthcoming European Professional Card (the latter currently under discussions in the European Parliament and Council).

[46] Further information on the website of the EC, DG Internal Market:

http://ec.europa.eu/internal_market/imi-net/news_archive_en.html

http://ec.europa.eu/internal_market/qualifications/docs/policy_developments/modernising/COM2011_883_en.pdf

ERA, in co-operation with the NSAs and the representative organisations, has recently started to investigate the systems described at the last bullet point, in order to propose the European railway sector with a cost-effective and accurate solution.

Annex 1: Acronyms frequently used in the text

Acronym	Description
Art. 35 WG	Working Group established at ERA, including the representatives of the NSAs in the context of the cooperation to be established as part of the implementation of Directive 2007/59/EC on the certification of train drivers and in particular in conformity with the Article 35 therein.
CA	Competent Authority (it is the National Safety Authority as defined in the Directive 2004/49/EC (Railway safety Directive – see below)
CC	Complementary Certificate
CCR(s)	Register(s) of Complementary Certificates
EIN	European Identification Number
IM	Infrastructure Manager
NLR(s)	National Register(s) of Train Driving Licences
NSA	National Safety Authority
PwC	PricewaterhouseCoopers
RU	Railway Undertaking
TDL	Train Driving Licence
TDL/CC	Process related to the delivery of a smartcard including data of the train driving licence and of the complementary certificate

Annex 2: Terminology

The glossary below provides the reader with an overview of activities, literature, techniques and terms used to prepare this report.

Term	Description
Computer Based solution / System	Whereas 7 of Decision 2010/17/EC: *Ideally, each Member State should set up a computer-based driving licence register to achieve full interoperability of the registers and allow competent authorities and others who have access rights to obtain information.*
Information System	A system, whether automated or manual, that comprises people, machines, and/or methods organised to collect, process, transmit, and disseminate data that represent user information
Interface / Bridge	A function that will unite and make information accessible between different systems.
Project	Projects are performed by people, constrained by limited resources, and planned, executed, and controlled. A project is a temporary endeavour undertaken to create a unique product or service. Temporary means that every project has a definite beginning and a definite ending. Unique means that the product or service is different in some distinguishing way from all similar products and services. Projects are often critical components of the performing organizations' business strategy.
Stakeholder	An individual who is materially affected by the outcome of the information system. Stakeholders of an information system (amongst others) are: the business units, the users of the system, the supplier of the system, etc.
SWOT Analysis	An analysis whereby the (internal) **S**trengths, (internal) **W**eaknesses, (external) **O**pportunities and (external) **T**hreats involved in a project are being evaluated.