Feasibility Study NLR-CCR

Feasibility study of Interoperable Registers for Train Driving Licences and Complementary Certificates

Document Information

Date:	05 March 2013	
Version:	V3 (Final)	
Author(s):	BAZIOTIS Nektarios	(ERA – European Dynamics)
Reviewers	METTE Olaf	(ERA)
	PATACCHINI Anna	(ERA)
	HOLVAD Torben	(ERA)
	MAZZANTI Daniele	(ERA)

Table of Contents

Executive summary

This report represents the **Feasibility Study for a computer-based application fulfilling the basic parameters for the National Register of Train Driving Licence (NLR) and the Register of Complementary Certificates (CCR) and facilitating the exchange of information among competent authorities, railway undertakings and infrastructure managers.**

The outcome of the study represents a written evaluation of the feasibility of such a computer-based application for information exchange as well as a possible business model in order to comply with the requirements as in Article 16b.1(b) of the Regulation (EC) 881/2004[1], Article 22.4 of the Directive 2007/59/EC[2] and Article 3 of the Directive 2010/17/EC[3].

As such these EU legislative measures aim is to assist the interoperability in the field of train drivers' licencing and certification. In this respect, an analysis review of the actual situation revealed that registers are established and working independently at **national level** leading to delays in communication among the different authorities.

To ensure **compliance** with the legal requirements and meet expected business opportunities **different solutions and lack of standardized methods may lead to mismatches and delays in communication among the different parties**.

ERA, along with a dedicated Task Force set up with representatives of the NSAs and sector organisations, as well as with the thorough revision and contribution of the representatives of the Art. 35[4] Working Group, has investigated and evaluated several possibilities and **different** business models, operational procedures, technical approaches and the potential future impact. Two main approaches were proposed:

- Design, development and implementation of dedicated **IT systems** to collect, compile, archive and retrieve information about train drivers was proposed.
- Evaluation of existing systems which could provide solution but would require customisation.

[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)as amended by Regulation (EC) No 1335/2008 of the European Parliament and of the Council of 16 December 2008

[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

[3] Commission Decision 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 (notified under document C(2009) 8278)

[4] Working Group gathering representatives of the competent authorities' (NSAs) to ensure cooperation for the implementation of provisions of Directive 2007/59/EC, in in conformity with Article 35 therein.

Potential risks related to information security and validity, interoperability, costs, language concerns and use have been considered and noted.

The whole feasibility study mirrors the thorough and pragmatic approach developed by the Task Force, showing the different solutions in terms of:

- interoperability, workflows, data collection, exchanges and protection as well as standardization.
- **information management**,
- **estimated cost** (for the envisaged pilot phase of the proposed system),
- **risk allocation** including timeframe.

The technical approach has been drafted based on a survey collection the views of the NSAs. . Since the survey was carried out during the very early stage of implementation of provisions concerning harmonised certification of train drivers, it did not provide purposeful knowledge on data exchange concerning licenses and certificates. In order to compensate for this aspect, the task force adopted a more qualitative approach towards a feasible and viable solution for the interoperability of registers.

The proposed system would need involvement of the following actors: ERA, NSAs, RUs, IMs. The nature and reason of the needs that might arise, lead additionally to the draft of use case scenarios and their related methodology were identified.

A theoretical technical approach allowed three potential business models with secured information exchange to be identified. These models were analysed and compared in terms of their respective impact, as well as technological implications, HR effort, and budget required.

In order to get a complete picture, the **existing practices** of IMI, ISA and TACHONET were reviewed.

After analysing all the factors and the actors' involvement, the differences in technological solution at company and NSA level, development of use-cases and their methodology, a clear **recommendation** concerning the system implementation can be made:

- an immediate comprehensive solution has been found for the data exchange between national license register;
- specific solutions for the data exchange between NLR/CCR is to be found at a later stage.

The intention is to implement a computer-based application, based on a web platform, to **enable the information-exchange of the available data of all national registers (NLR).** This method shall improve the interoperability in the exchange of information, but with specifications:

- in the cases of reasoned requests only;
- accompanied by a high-level control of access-rights for all data input or exchange.
- the expectation to announce the assured current validity of the licences in special cases immediately.

After defining the business case and evaluating all proposed models, **ERA and the TF** has reached the conclusion of proposing the **business model with the customisation of the secure information exchange** system provided by **Internal Market Information System (IMI),**

developed by the General Directorate Internal Market of the European Commission and proceed to the next steps on defining precisely the pilot on the NLR level.

The proposed model is practically providing a solution to the study's main subject, since it is already in production phase for the fulfilment of EU legal requirements that are very similar in scope to the train drivers certification and, in particular it is designed for providing:

- easy customisation;
- a high level of interoperability;
- secured transactions among competent authorities;
- compliance with requirements of personal data protection;
- validated translation.

In addition, the IMI system does not require any investment for the Member States, both in terms of design and maintenance.

For this of course, IMI is considered as the most suitable solution to fulfil, **the needs** of Directive 2007/59/EC and of **Decision 2010/17/EC** as far as the exchange of information between NSAs is concerned, ensuring **the data protection** and **system's integrity** at any process or workflow.

A parallel solution for the exchange of data between NLRs and CCRs might be developed following the use of the proposed system for NLR/NLR exchange.

Based on this the current study is providing **a roadmap to the pilot phase** which should guarantee the expected results.

1 Introduction

This document contains a Feasibility Study for a computer-based application fulfilling the basic parameters for the National Register of Train Driving Licence (NLR) and the Register of Complementary Certificates (CCR) and facilitating the exchange of information among competent authorities, railway undertakings and infrastructure managers.

The outcome of the study represents a written evaluation of the feasibility of this computer-based application for information exchange as well as a possible business model in order to comply with the requirements as in Article 16b.1 (b) of the Regulation (EC) 881/2004[5], Article 22.4 of the Directive 2007/59/EC[6] and Article 3 of the Directive 2010/17/EC[7].

This study was developed in two main steps. The first step was dedicated to an analysis of the subject matter in general terms and the principle options (model I to IV) of developing an IT system assuring interoperability between the concerned registers were developed.

The most important development from step one to step two was that the 'Internal Market Information System' (IMI) was found, evaluated and accepted as a feasible solution for the exchange of data between the authorities concerning NLRs. CCR information may be included indirectly via procedural connections as well (to be further analysed and elaborated during pilot). IMI is an internet based communication system between authorities of the EU. It provides secure and multilingual information exchange and is financed and managed by the European Commission, DG Internal Market. IMI was finally selected as preferred solution and is recommended in the study conclusions as the option to be tested during a pilot period.

For a good understanding of this document it is important to have in mind that a large part of the study – in particular chapters 4 to 11 – refer to the option of developing and implementing a new IT system specifically for the purpose of connecting NLRs and CCRs.

[5] REGULATION (EC) No 881/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 establishing a European Railway Agency (Agency Regulation)as amended by Regulation (EC) No 1335/2008 of the European Parliament and of the Council of 16 December 2008

[6] 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

[7] Commission Decision 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 (notified under document C(2009) 8278)

1.1 Document type: Feasibility study

The feasibility study documents the efforts made by the following actors:

- ERA, having the task of the feasibility study overall project management, assisted by a consultant to ensure IT expertise and preparation of the study;
- A dedicated Task Force set up with representatives of the NSAs and sector organisations (CER, ETF);
- The representatives of the competent authorities (being part of the Art. 35 Working Group),which have the task to cooperate with ERA in order to ensure the interoperability of registers, as stated in Article 22.4 of Directive 2007/59/EC.

All actors were engaged to objectively and rationally uncover the strengths and weaknesses of different options, opportunities and threats as presented by the legal and technological framework, the resources required and ultimately the prospects for success of the options. In this way, the study addresses both the technical / legal feasibility as well as the economic feasibility.

1.2 Aim of the feasibility study

The aim of this feasibility study is to provide sufficient information to the representatives of the NSAs in the Working Group "Coordination of Article 35" on the possibility to develop **an IT utility that ensures the interconnection of the National Train Driving Licences Registers (NLR) and the Complementary Certificates Registers (CCR)** foreseen by the mentioned Article 3 of the Decision 2010/17/EC.

The current work should be leading to a clear understanding of the subject and allow for a decision on developing the pilot phase. The implementation of the pilot phase should then lead to the verification of whether and how to proceed to full-scale implementation.. Such a decision should be made on the basis of clear indications regarding value for money, i.e. improved quality of service together with limited cost implications while complying with the requirement of the Directive 2007/59/EC.

The NSAs, as well as the RUs/IMs, are the main stakeholders in this project, as they:

- have to set up and keep relevant registers
- are obliged to provide information (at least the minimum contained in the Directive 2007/59/EC and on the basis of access rights defined by the Decision 2010/17/EU).

1.3 Working framework

The strategic approach to conduct the feasibility study involves:

- ERA who has the mandate of cooperating with the NSAs, in order to ensure the interoperability of registers and to carry out the feasibility study for a computer-based

application for exchange of information concerning train driving licences and complementary certificates (see Chapter 2 for details regarding the legal background);

- Appointed external consultant to support ERA in providing business and technical analysis including actual use-cases as the core content of the feasibility study;
- Involvement of a task force (TF, hereinafter), including representatives of the NSAs, of the railway companies (CER) and the staff (ETF). The appointed members of the TF have been selected to represent all users of the system in the context of the ERA IT Project Management framework. The practical role of the TF members is to represent all stakeholders currently involved in this process and, therefore, to highlight needs, opportunities and risks from the user's point of view so that the proposed solution is based on a sound, feasible and valid business case.

1.4 Roadmap of the study as per Article 3 – Decision 2010/17/EC

In order to reach a conclusion for the feasibility of the system and understand in particular its potential and the added value that it will bring to the involved stakeholders, the EU as per Article 3 – Decision 2010/17/EC mandated ERA to undertake a feasibility study.

The steps that will follow in case of the acceptance of the conclusions presented in this study, might be to **design a system complying with all identified needs** by **developing a document presenting system functionalities** based on defined **use cases** and **workflow descriptions** which might lead to the **pilot phase where there could be a clear understanding on how the system would work and its potential benefits / costs that would be incurred for the stakeholders**. Such a system should in its pilot phase be tested and verified that all its workflows are in a proper state and are in accordance with the EC's Directive. The final step will be to disseminate the **first pilot version** to all stakeholders and subsequently **establish it as a solution at EU Level**.

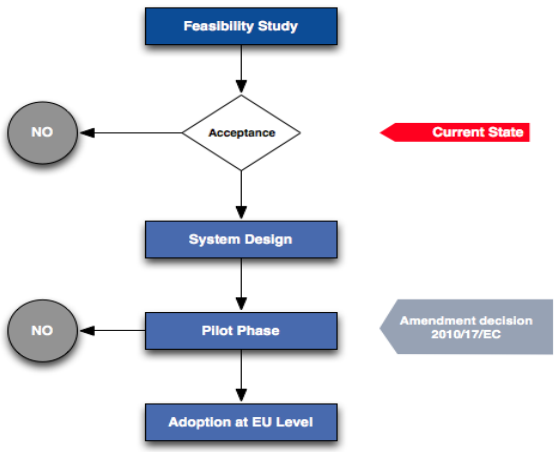


Figure 0: Roadmap of the study

1.5 The Role of the Task Force (TF)

The TF, constituted by Mr Jochen Brandau (JB - CER), Mr Helmut Mundt (HM – ETF), Mr Rolf Helmrich (RH – NSA DE), Mr Morten Brok (MB – NSA DK), Mr Rob van der Burg (RvdB – NSA NL), Mrs Anita Mrozco (AM – NSA PL), Mr Piotr Cukierski (PC - NSA PL), has assisted ERA to develop

the present document with their experience in the field. Their valuable opinions along with the decisions taken by Article 35 group have influenced the course of the study, by leading to further investigations. As such the validity of the outcomes presented in this document are supported by the TF's overall contribution and acceptance.

1.6 Timeframe milestones

The feasibility study in its final shape is the result of a two-step work approach.

A first draft of the study was developed and circulated to relevant stakeholders already in **December 2011**. The Task Force with members representing 4 NSAs as well as CER and ETF, the social partner organisations of the 'European Committee for Social Dialogue Railway', was set up to work on this subject using this first draft as starting point.

In **April 2012** a first final version was issued to the Article 35 group. It presented architecture and characteristics of 3 different types of IT system. These 3 options in principle cover the range of different approaches for a feasible IT solution in this context. These basic options differ first of all in regard to the level (EU, MS or RU) on which they assume the main data storage. A fourth option 'model IV' was developed in course of the Task Force work proposing to 'merge' two basic models.

None of the four models in the feasibility study found sufficient support of the Art35Gr for being approved as possible pilot implementation. The majority of Art35WG members showed reluctance to assign resources for development, application and maintenance of a complex IT system at a moment where there is not much experience on the new train driver certification model in general and on the frequency of occurrence of mutual requests concerning register data exchange in particular.

Around that time the Agency became aware of the **'Internal Market Information System' (IMI)**. IMI is a communication system using the internet as a platform to exchange in secured and multilingual manner information between public authorities of EU Member States. It was developed and is managed by the EU Commission, DG Internal Market. The Agency established contact to the management of IMI in order to find out if IMI would be a feasible option for the exchange of data concerning train driver registers. It was agreed that IMI easily could be used to allow exchange of information between NSAs in accordance with Article 29 of Directive 2007/59/EC and has the potential to be further developed for an (indirect) integration of the registers on company level (CCRs).

On that background the Agency decided in **September 2011** to re-launch the work on the feasibility study proposing to include IMI as further option in addition to IT systems model I – IV. With support from DG Internal Market we discussed the feasibility of IMI for our purpose in depth within several task force meetings. In addition, IMI was presented and discussed at a meeting of the Art35Gr. A new version of the feasibility study was drafted with support of the task force and after consultation of Art35Gr members and integrating amendments proposed the Agency concluded on the final version by the beginning of **2013.**

It is foreseen to ask members of the Art35Gr to approve the final version of the feasibility study by using a dedicated procedure agreed by the Commission. Further details, in particular on the IMI System, are displayed in chapter 13 'Conclusions and Recommendations' as well as in Annex 3 'Existing Practices'.

1.7 Document structure

This document is structured as follows:

Chapter 2 - Legal background

This chapter contains abstracts of the Directive2007/59/EC and all complementary legislation on which this study will be based on. This is an important step as the reason for the initiative and decisions taken by the EC was to assist the interoperability in the field of train drivers' certification.

Chapter 3 - Actual situation & proposed solution bases on EU legal framework:

This chapter represents a presentation of the actual situation. The registers are working at national level relatively independently from each other. This leads to delays in communication among the different national authorities of the EU Member States.

Chapter 4 - Features of the IT Solution with interoperable registers & information exchange:

This chapter shows how the system should allow the collection and archiving of information about train drivers, but it should, ideally, also allow information and data retrieval by all involved parties according to their individual access rights.

Chapter 5 - Challenge of the IT Solution with interoperable registers & information exchange:

This chapter contains the identified risk factors that could potentially impact on the proposed application including information security and validity, interoperability, costs, language concerns and use.

Chapter 6 - Compliance with the requests and expected business opportunities:

This chapter contains the screening of the immediate and the potential opportunities that the system may bring to the EU, the involved institutions and the train drivers. These need to be evaluated based on business models, operational procedures, technical approach and future impact.

Chapter 7 - Technical considerations

This chapter describes the technological approach needed to achieve the desired goals, whenever the implementation of a pilot phase is approved, in terms of interoperability, workflows, data collection, compile, exchange and protection as well as standardisation of data.

Chapter 8 - Information Management

This chapter outlines the necessary information management for the proper functioning of the system.

Chapter 9 - Model approach

This chapter describes the approach followed by ERA and the TF in order to conclude on a proposal for the potential modelling of the system in discussion.

Chapter 10 - Cost model and assumptions:

This chapter outlines the estimated cost incurred during the pilot phase.

Chapter 11 - Risk allocation matrix:

This chapter contains the visualisation of an identified risks matrix as well as a proposal for a possible timeframe.

Chapter 12 - Impact Analysis

This chapter contains the analysis of the overall system, where the potential business models, are evaluated in terms of their respective impact, as well as technological implications, HR effort, and budget.

Chapter 13 - Conclusions & Recommendations

Taking into consideration the evaluation of the models, all comments / remarks / proposals of representatives during meetings and incorporating results of a survey circulated among NSAs, the study concludes that the most feasible solution at this stage is the adoption of the IMI Internal Market Information System.

Annex 0 - Definitions

This annex contains key definitions used in this document.

Annex 1 - Glossary

This annex contains some specific IT related terms that have been used in the document.

Annex 2 - Acronyms and Abbreviations

This annex contains Includes main acronyms and abbreviations used in the study.

Annex 3 - Existing practices

This annex describes the existing practices of IMI, ISA and TACHONET, which are reviewed as benchmark and to identify best practices.

Annex 4 – Customisable tool (IMI Presentation)

This annex contains the presentation of the information exchange system developed at EU Internal Market level (IMI system) as a tool that could be easily customisable and in good part fulfil the requirements of the Directive 2007/59/EC.

Annex 5 - Mandatory requirements concerning registers and exchange of information

This annex contains the summary of the relevant legal requirements for the system including reference, explanation and consequences.

Annex 6 - Questionnaire on interoperability of NLRs/CCRs

This annex contains the questionnaire initially sent to the NSAs for data collection.

Annex 7 - Survey to NSAs on Interoperability of NLRs – CCRs (FEB 2012)

This annex contains the results of the questionnaire to NSAs circulated at the beginning of 2012 and related interpretation of results.

Annex 8 - Business models supporting interoperable information exchange:

This annex contains the description of the main business models that have been identified that would be compatible with the legal requirements.

Annex 9 - Process oriented model IV

This annex contains two variations of Model IV which have a process-oriented approach, use a combination of Model I and II, and have a special emphasis special emphasis on data storage and access rights security.

Annex 10 - Business model with secure information exchange:

This annex refers to the discussions between ERA and IMI showing that IMI's current system covers the communication needs amongst stakeholders of the proposed system.

Annex 11 - Business models of interoperability evaluation:

Having identified the potential business models, they need to be evaluated in terms of their respective impact, as well as technological implications, HR effort, and budget. This concludes that among the three generic models, the **hybrid model II** would perform best in business terms.

Annex 12 - Actor's involvement:

Annex 13 - Technical approach

This annex contains the technical approach follows specific principles including low cost for all stakeholders, high level of interoperability, immediate response and high level of security standards.

Annex 14 - Use-Cases:

This annex contains the proposed methodology, possible classification and analysis of the identified use cases.

Annex 15 - Use-Cases concept idea:

This annex provides new details concerning the identified use cases.

2 Legal background

Article 16b (**Train drivers)** of the Regulation (EC) 881/2004, as amended by Regulation (EC) No 1335/2008, contains the mandate for the Agency to cooperate with the competent authorities (NSAs) in order to ensure the interoperability of registers:

1. On matters related to 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 (1) (hereinafter referred to as the 'Train Drivers Directive') the Agency shall:

[…]

(b) cooperate with the competent authorities in order to ensure the interoperability of the registers for train drivers' licences and certificates. To this end the Agency shall prepare a draft on the basic parameters of the registers to be set up, such as data to be recorded, their format and the data exchange protocol, access rights, the duration of data retention and the procedures to be followed in cases of bankruptcy;

According to the Directive 2007/59/EC, Article 22, "Registers and exchange of information", paragraphs 1 and 2 it is mandatory for NSAs and companies to set up registers for train driving licences respectively for complementary certificates. The exchange of information among competent authorities, railway undertakings and infrastructure managers is expected in defined cases:

> *1. The competent authorities shall be required to:*
>
> *(a) keep a register of all licences issued, updated, renewed, amended, expired, suspended, withdrawn or reported lost, stolen or destroyed. This register shall contain the data prescribed in section 4 of Annex I for every licence, which shall be accessible using the national number allotted to each driver. It shall be regularly updated;*
>
> *(b) supply, upon reasoned request, information on the status of such licences to the competent authorities of the other Member States, the Agency or any employer of drivers.*
>
> *2. Each railway undertaking and infrastructure manager shall be required to:*
>
> *(a) keep a register, or ensure that a register is kept, of all certificates issued, updated, renewed, amended, expired, suspended, withdrawn or reported lost, stolen or destroyed. This register shall contain the data prescribed in section 4 of Annex I for every certificate, as well as data relating to the periodic checks provided for in Article 16. It shall be regularly updated;*
>
> *(b) cooperate with the competent authority of the Member State where they are domiciled in order to exchange information with the competent authority and give it access to data required;*

(c) supply information on the content of such certificates to the competent authorities of the other Member States upon their request, when this is required as a consequence of their transnational activities.

The European Railway Agency (ERA) has been requested by the European Commission to assist the competent authorities (NSAs) in order to ensure the interoperability of the registers demanded by the aforementioned provisions, namely by Article 22, paragraph 4:

4. The competent authorities shall cooperate with the Agency in order to ensure the interoperability of the registers provided for in paragraphs 1 and 2.

In addition, the involvement of ERA and the vision for an electronic interface are described in the Whereas 7:

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. However, for economic and technical reasons, this kind of interface cannot be adopted without further investigation. Firstly, it is necessary to agree on methods to ensure that access is granted subject to certain conditions, as required by Directive 2007/59/EC. Secondly, a survey of the number of transactions is necessary to perform a cost benefit analysis and propose a feasible solution that does not impose administrative costs that might be disproportionate to real needs. The European Railway Agency therefore proposed to implement an interim solution, with simplified exchange of information, and proceed with the development of an electronic interface at a later stage.

More recently, the necessity to carry out a feasibility study for a computer-based application and the extent of it has been stated in Article 3 of the Decision 2010/17/EU:

Article 3: Within 24 months from the taking effect of this Decision, the European Railway Agency (hereinafter 'the Agency') shall carry out a feasibility study for a computer-based application fulfilling the basic parameters for the NLR and CCR and facilitating the exchange of information among competent authorities, railway undertakings and infrastructure managers.

The Commission's decision of 29 October, 2009 – 2010/17/EC "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" provides further explanation on the envisaged steps towards an electronic interface for the exchange of information:

> *Recital 7: 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. However, for economic and technical reasons, this kind of interface cannot be adopted without further investigation. Firstly, it is necessary to agree on methods to ensure that access is granted subject to certain conditions, as required by Directive 2007/59/EC. Secondly, a survey of the number of transactions is necessary to perform a cost benefit analysis and propose a feasible solution that does not impose administrative costs that might be disproportionate to real needs. The European Railway Agency therefore proposed to implement an interim solution, with simplified exchange of information, and proceed with the development of an electronic interface at a later stage.*

The solution should provide all stakeholders with the ability to proceed with reasoned requests and retrieve information.

The solution may also enable 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.*
>
> *2. Notwithstanding verification as provided for in paragraph 1, in the event of negligence at the workplace the competent authority may verify if the driver in question complies with the requirements set out in Article 13.*
>
> *3. The competent authority may carry out enquiries regarding compliance with this Directive by drivers, railway undertakings, infrastructure managers, examiners and training centres pursuing their activities in its area of jurisdiction.*
>
> *4. […] At all events, if the competent authority considers that a particular driver creates a serious threat to the safety of the railways, it shall immediately take the necessary action, such as asking the infrastructure manager to stop the train and prohibiting the driver from operating in its area of jurisdiction for as long as necessary. It shall inform the Commission and the other competent authorities of any such decision.*

All above-mentioned provisions are expected to contribute to the overall aim of the Directive 2007/59/EC and to the wider European framework of ensuring the free movement of labour. For instance, they should contribute to pursue the Regulation 1612/68 objectives by promoting the removal of barriers affecting train and locomotive drivers as well as other qualified personnel in the field who are holding a valid licence and certifications. The aim is for them to be able to seek labour opportunities across the EU 27 countries. As stated and expected, all EU countries will benefit from this decision. Such benefits could be extended to EU Countries like Malta and Cyprus that currently have no railway but are considering of creating one, candidate

countries that may become EU Member States in the future, as well as countries belonging to the European Free Trade Association (EFTA).

For the achievement of the above-mentioned purposes, and especially in order to secure the interoperability of the sector, the implementation of a computer-based system is under consideration to facilitate the provision and retrieval of information.

The feasibility study shall be discussed and approved within the cooperation between the representatives of the competent authorities specified in Article 35 of Directive 2007/59/CE.

The specific study will include a business, operational, technical and impact analysis in order to consider the advantages and disadvantages of such a system while taking into consideration various political and other cultural factors.

3 Actual situation & proposed solution based on EU legal framework

The current situation to be considered as the starting point for the feasibility study is derived from the legal framework in force and can be summarised as follows:

3.1 Concerning NLRs

- The data of train driving licences are recorded and stored in the registers already set up or under development in the NSAs. Such registers are mandatory based on Directive 2007/59/EC, Art 22.1;
- The information on the train drivers' licences are exchanged among the parties that have access rights (Commission Decision 2010/17/EU, Annex I.4);
- Any allowed requester has rights to obtain information on the status of the train driving license (Directive 2007/59/EC, Art. 22,1,(b));
- The information is provided by phone, fax or email and upon “reasoned request” by the NSAs. The NSA must ensure secured exchange of information. (Commission Decision 2010/17/EU, Annex I.5);
- The “reasoned request” is not defined and each NSA supplies the information on an ad-hoc basis;
- No specific time limit for the response in the single cases of requests has been defined.

3.2 Concerning CCRs

- The data of complementary certificates are recorded and stored in the registers already set up or under development by RUs and IMs. Such registers are mandatory according to Directive 2007/59/EC, Art 22.2;
- The information on the train drivers' complementary certificates are exchanged among the parties having access rights (Commission Decision 2010/17/EU, Annex II.4);
- There is no explicit limitation to the information to be provided on complementary certificates (Directive 2007/59/EC, Art. 22.1,(b));
- The NSA may verify, in case of negligence at the workplace, if a driver complies with the requirements on professional competence (Directive 2007/59/EC, Art. 29.2);
- The NSA may need to inform the other NSAs about driver(s) that have been requested to stop driving because they pose a threat to the safety of the railway (Directive 2007/59/EC, Art. 29.4);
- The RUs/IMs provides information by phone, fax or email or grants the NSA access to the websites of the companies. The RU/IM must ensure secured exchange of information. (Commission Decision 2010/17/EU, Annex II.5);
- No specific time limit for the response in the single cases of requests has been defined.

3.3 Potential benefits linked to a system of interoperable registers in the field of train drivers certification

A number of specific reasons for using systems to exchange register data concerning train drivers:

From the point of view of the system's concept

- Adoption of harmonised processes and of a common policy throughout the EU (overall interoperable and harmonised framework for the railway sector and promotes the removal of barriers)
- Design of the system involving all actors so the output reflects all needs on:
  - Monitoring of the system (through functions, to provide reports, statistics, frequencies, etc.)
  - Periodical review to implement corrective action(s), if necessary
- Possibility to include new functions based on the sector's demand
- Reassure security of transactions based on roles and access rights
- Automatic check of duplicated information (to facilitate detection of abuses) in all databases and relevant notifications to identified stakeholders
- Automatic notifications in case of expiration dates

- **From the operational point of view**
  - Availability of a common framework (based on Decision 2010/17/EU) or possibility to liaise to existing registers through a system;
  - Responses in a time-frame, adequate to information needs
    - Exchange of information in an appropriate time-frame amongst NSAs
    - Exchange of information in an appropriate time-frame among NSAs and RUs/IMs employing or contracting drivers;
  - Improved quality of communication;
    - Standardised language facilitates easy understanding
    - Automatic translation can overcome language barriers
  - Automated acceptance of request
    - Approved catalogue of reasoned requests adopted
    - Possibility to include reasons unidentified (first using an open field, then advanced criteria);
  - Controlled access to information according to rights;
  - Freedom for NSAs to include other actors by logging (or requesting log to ERA);
  - Alert of duplicated information in one database and relevant notifications to identified stakeholders;
  - Automatic notifications in case of expiry dates.

3.4 Survey of NSAs' views and expectations

ERA circulated a questionnaire to NSA's the 3rd of February, 2012. On February 7th ERA had collected 21 results from respondents of the following countries: UK, NO, DE, BE, NL, FI, DK, AT, SE, LV, IT, FR, LT, RO, EE, CZ, BG, PL, SK, HU, IE. The questionnaire and conclusions are available in Annex 6 and Annex 7.

3.5 Use cases

It has to be highlighted that specific business cases (use cases) will be designed, in collaboration with the NSAs, as well as the RUs and IMs, in order to determine the most accurate business model that will most likely support the prerequisites of the decision taken by the EU. Therefore:

- Expected business cases are to be asked from the NSAs and RUs; each of the actors involved are to be determined (as in a use-case description);
- These business-cases are to standardize and it is to ask which modalities of treatment are generated: pressure, effort of labour, resources, man-power, extent of the request, frequency;
- These modalities together with the criteria (referred to the earlier section) are to establish to the actors in a scheme. It may be shown in detail for several business cases (period of validity, medical checks);
- The NSAs and the RUs / IMs will have consider these cases in terms of their importance.

In a case model on NLRs and NSAs we would have results alike to:

Questions on the current state of your NLR	Time	Frequency	Required
1. Inform of validity of license			
a. Accidents	**Low**	**Low**	**Yes**
b. Incidents	**Low**	**Low**	**Yes**
c. Inspection on sight			
i. Control of validity	**Critical**	**High**	**Yes**
ii. Check of license possession	**Medium**	**High**	**Yes**
d. Audits	**Critical**	**High**	**Yes**
e. Application phase	**Medium**	**High**	**No**
f. Check "double give out"	**Medium**	**Medium**	**Yes**
2. Inform of license's invalidity	**Critical**	**High**	**Yes**

Factors may vary from time, frequency and required process to extensive requests, proof of legitimacy / verification and access rights.

- **Time-Critical Factor:**
  - Law enforcement forces will request immediately;
  - Undertakings are more interested in secondary data: other engagements, medical appointments. In this case 4 weeks response time would be satisfactory;
  - NSAs of other countries will ask time-critical and time-uncritical requests.

- **Extensiveness of requests:**
  - Law enforcement forces might be interested in the verification of the licences and the data of the validity only;
  - RUs and IMs and the train driver themselves will ask for abridgements of the registers;
  - NSAs of other countries single data or abridgements.

- **Efforts to prove the legitimacy and to verify the requesting organisations and persons:**
  - NSAs are known.
  - Law enforcement forces could be verified in a simple manner
  - To legitimate and to verify RUs and IMs of all MS and their contact persons need a large effort.
  - Train Drivers are legitimated at their NSAs.

- **Administrative installation of the access rights:**
  - All NSAs are to install for one time, and then to maintain only
  - The law enforcement forces of all MS are to install for one time, and then to maintain only
  - The installing and maintaining of RUs and IMs – this means: their contact persons – in all MS of the EU needs very significant efforts.
  - How many train drivers will ask how much, is not easy to say, therefore: a middle level of efforts is assumed.

- **Frequency of the business cases:**
  - From the NSAs some requests might be expected.
  - RUs and IMs could ask seldom, because the train driver licence contains all relevant information.

3.6 Circumstances under which a computer-based system might assist

According to statistics available by ERA and ESTAT, we may observe that despite the evolution in the field of railways in Europe, there are still accidents / incidents and their non-probability or non-diagnostic should be treated with extreme caution, and unfortunately despite the continuous effort to increase safety in the field, the lowest figure the last ten years (1999 – 2009) appears in 2007 and since on there has been an increment the years 2008 and 2009.

The implementation of such a system, that will mainly support interoperability of registers and increase the validity level of information, may not necessarily decrease mortal incidents or injuries, though, by bringing closer all stakeholders on exchanging specific information for driver licences and certificates, will at least secure the ground that all drivers are in a position to document their competency to drive certain rolling stock and that they are authorised to drive on a certain infrastructure.

Since such structured information does not currently exist and such experience does not exist as well, we cannot measure any results but only study the potential effects that could be estimated. Therefore, it has been estimated that such system might assist:

- providing a rapid and not complicated access on exchanging information upon reasoned request by all stakeholders (through granting access rights beforehand);
- creating a specialized computer based system, which can be financed and created by common effort and provide the of completion tasks that all stakeholders are handling;
- support proper communication channels by informing all beneficiaries about various situations in terms of the validity of licences and certificates, as well as having archival information concerning each driver

Further to these it will assist on:

- **inspection**: validate credentials of train drivers
- **operation**: useful for RU and IMs by bridging with their IT systems as it happens with HR processes
- **audits**: NSAs will be able to audit companies more accurately and less time will be necessary for this operation
- **licence-checks**: provide valid information and allow its exchange (according to user credentials and specific reason) between RU/IM and NSAs for:
    - A driver could request for multiple licences in different countries and currently there is no possible online cross-validation;
    - A driver may relocate and request for exchange of licence to the new country;
    - A license may be withdrawn;
    - A license may be suspended;
    - Status of health approvals.

3.7 Method of the Analysis of Use-Cases via Work-Flows

Use-cases are the formalisation of situations, which trigger – in the considerations of this study – the working-processes of information exchanges in a network. These processes could be identified in terms of work-flows, where each work-flow has its characteristics in the above mentioned criteria – e. g. time-criticalness, frequency, quantity, etc. – to fulfil the needs of the situation in question. The combination of the values of these criteria – high, middle or low – gives the characteristic profile of the processing of a work-flow. But this is nothing else than the requirements, which the exchange-system – however it will be IT-supported – has to perform later.

Starting with the listing of all possible request-response-combinations there can be – in Annex 15 theoretical at first – generate a collection of work-flows, which can be used for general considerations, but are the challenge to concretise the use-cases later, too.

If conditions are made of time-criticalness/time-non criticalness, access-authorisation, quantity, frequency, then accumulations of work-flows with similar characteristics occur. This signifies that several use-cases could be bundled in same proceedings (see Figure 1, for details see Annex 14). Therefore, it can be an option, to create different systems, each optimised for its task, only performed under one IT-desktop. And it indicates on the other hand, that the development of one system-structure only could increase the cost of the system: because all lower level-workflows then will be treated in a system of high equipped quality.

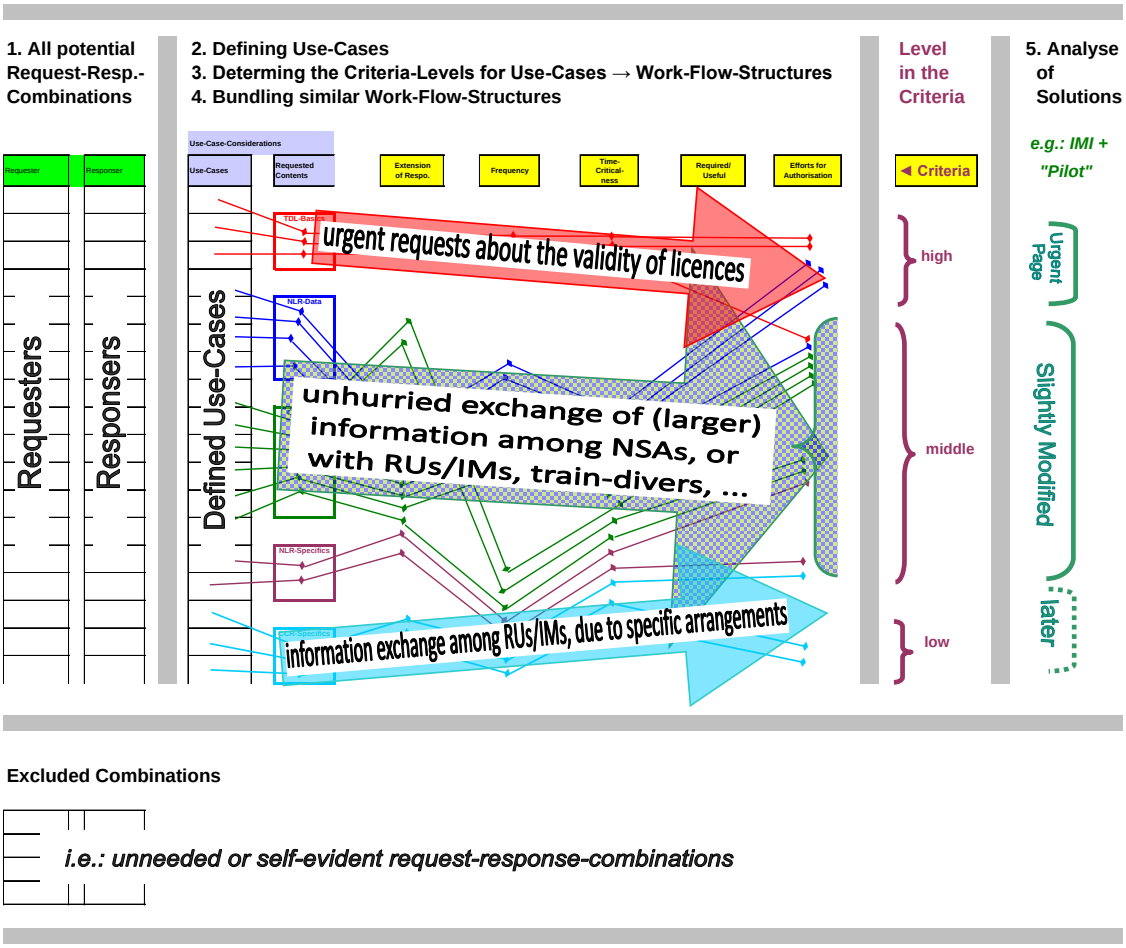


Figure 1: Steps from use-cases via work-flows to an analysis of solutions

If the solution of the IMI would be chosen (as shown in Figure 2 on the right side), the following figure describes the basic constellation of those use-cases (for details see Annex 14).

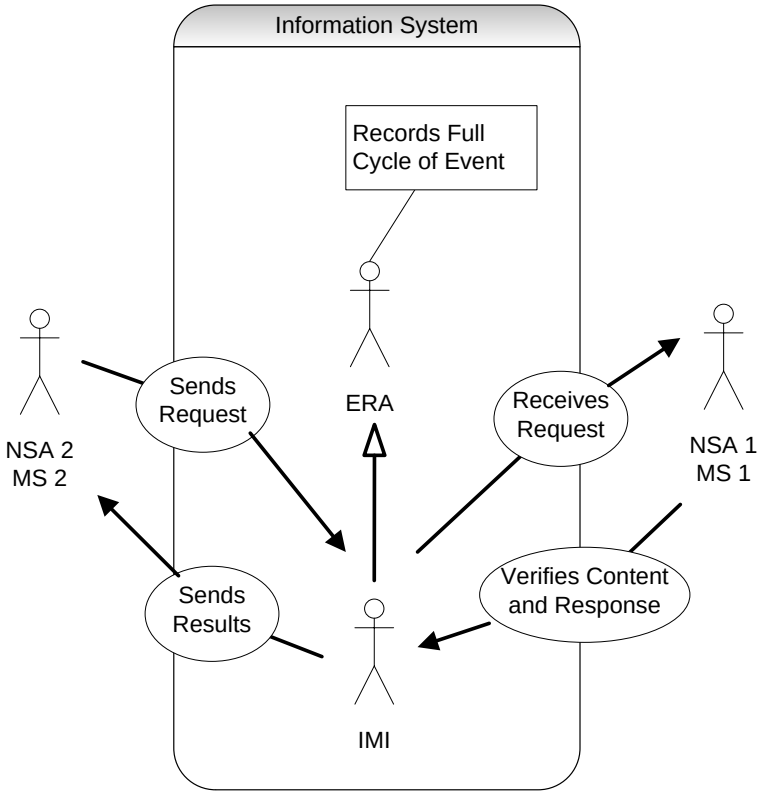


Figure 2: Basic constellation of use-cases in the IMI-stucture

4 Features of the solution to implement a system of interoperable registers

The system in discussion might secure:

- the valid and up-to-date information for each registrant, thus train drivers, including all basic information as well as educational, training, certification and medical records;
- the validity of information contained in these licences or harmonized complementary certificates that will be used by the safety authorities and driver employing companies;
- the legitimacy of each request in relation to the licence and certification records as well as the personal information;
- the archival and documentation of all information for each party according to the definitions, for a duration according to the particular legislation;
- the documentation of all relevant information of each user of the system for a duration according to the particular legislation.

and assist:

- authorities from each Member State plus RUs, IMs to exchange information on drivers' licences and certificates;
- rapid and non-complicated information exchange and report retrieval concerning incidents, such as accidents that have happened and a train driver was involved;
- authorities to monitor if a specific record of a person exists in another country;
- safety authorities to perform evaluation for the staff certification processes;
- authorities to cross-reference the information of each candidate;

This aim could be achieved by the design and development of a computer-based system based on the following principles:

- Definition of user credentials and provision of specific or full access to core information, according to user credentials in accordance with the EC decision;
- Users will be classified by hierarchy into the following macro-categories

ERA	NSAs	RUs	IMs
• System administrator • Responsible for query server and access rights database maintenance • Query handling should be respecting specific access rights	• Own information administrator • Administering RUs/IMs and drivers under their regional jurisdiction • Responsible for their own data validity and update • Able to request to other to retrieve specific information	• Own information administrator • Administering contracted drivers • Responsible for their own data validity and update • Able to request others to retrieve specific information	• Own information administrator • Administering contracted drivers • Responsible for their own data validity and update • Able to request others to retrieve specific information

	• Verify if a driver complies with requirements on professional competence in case of negligence		

- Information should be in appropriate and non-complicated reach and search functions should be available to allow and assist operators as well as administrators;
- Clear and distinct information concerning drivers;
- System should provide search and advanced search functions;
- System should export reports;
- System should be secure;
- All information should be kept in a standardised data-pool constituted by a collection of databases or tables (for the case that there would be a unique database);
- All information should be kept using standardised methods of information exchange, formed in an computer supported system;
- System should be user-friendly and be compliant with accessibility rules;
- An administrative interface (back-end) should exist, allowing administrators to manage all sections of the system, thus information owners may proceed with updates and can verify the reasoning per request and allow access to specific information to any other stakeholder;
- Online input forms could be developed and data should be stored securely;
- Specific disclaimers should be in reach to clarify the use of personal information;
- System should be accessible by web browsers, and should have no compatibility issues;
- System should be updated and have back-ups in order to prevent any data loss on a daily basis;
- System should respect all confidentiality, integrity, availability, authenticity, non-repudiation aspects;
- System should be scalable;
- System should be based on a specific structure (bridges) when exchanging or delivering information from other systems that currently involved parties are using;
- Extra care in communicating among involved parties should be taken according to the EC Decision on top of correctly managing their access rights;
- Online support and FAQs should be in reach at any time as well as contact forms to reach out to the administrators or even a dedicated helpdesk;

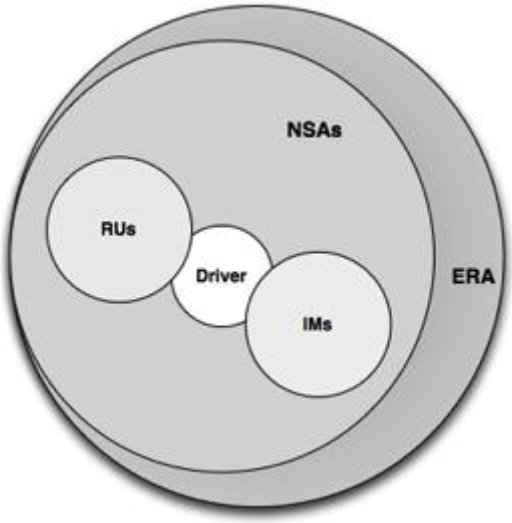


Figure 3a: Involved actors / users origin and their hierarchy

In *Figure 3a*, an initial attempt of a graphical representation of user origin and hierarchy based on first assumptions is displayed:

- **ERA** system creator
  - **NSAs** per EC Member State (27)
    - **Drivers** that are directly registering at NSA's
    - **RUs & IMs** various under a specific NSA
      - **Drivers** registering through RU or IM

The hierarchy is displayed in this way because **ERA** has been appointed by the EC to facilitate the present study and has all prerequisites to implement the system in case its implementation is accepted. **Drivers** are registered directly at the **NSAs** or at the **RUs / IMs** or they are registered at an **RU / IM**, who, in turn, are regulated by a specific **NSA**.

One of the purposes behind Directive 2007/59/EC had been the promotion of labour mobility in the choice of the work place for Train Drivers (TD). So constellations are to expect as shown in Figure 3b

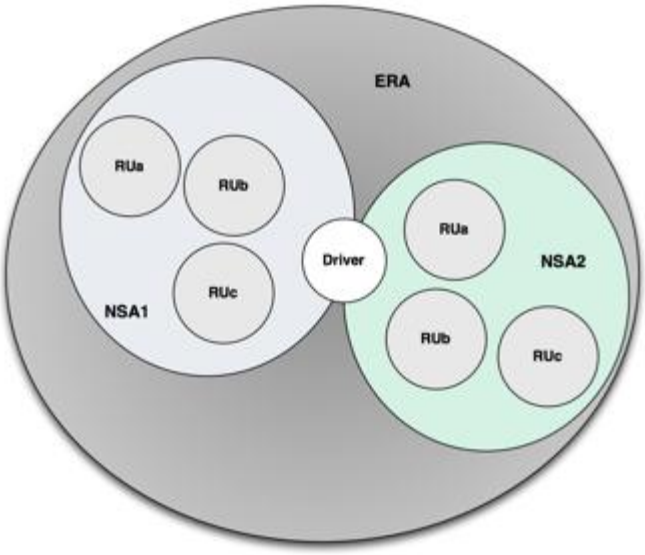


Figure 3b: Basic scheme of expected relationships of an TD to the competent NSA his RUs/IMs. (Not included: his operational area)

5 Challenge of the IT Solution with interoperable registers & information exchange

The solution should meet specific criteria in order to be viable and bring added value. There are six main challenges identified that should be taken into consideration:

- **Information security**: all information should be secured, stored safely and accessed according to specific user rights as mentioned in Decision 2010/17/EC, 22 Annex 1 – 4;
- **Validity of information**: all information submitted should be valid, taking into consideration all regulations in force and be available to cross-reference with registered authorities;
- **Interoperability**: information accessed and/or stored in the system should be available to those who have been assigned with access privileges, irrespective of location or language origin;
- **Budget**: system implementation, maintenance cost, clients' cost and their maintenance should be set at a normal range, in order not to create any additional economic burden for any of the involved parties;
- **Language**: all system functions should be able to visually adapt to all 23 official working languages of the European Union, since it is expected that many operators will not be able to perform in a language other than their native language;
- **Use:** despite the apparent diversity of the above-mentioned challenges, there is a core point where all of them meet, which is the **use of the system**. Thus, not only how operators and administrators will introduce data information needs to be paid attention to, but also system processes and speed of interaction for each request needed to be analysed.

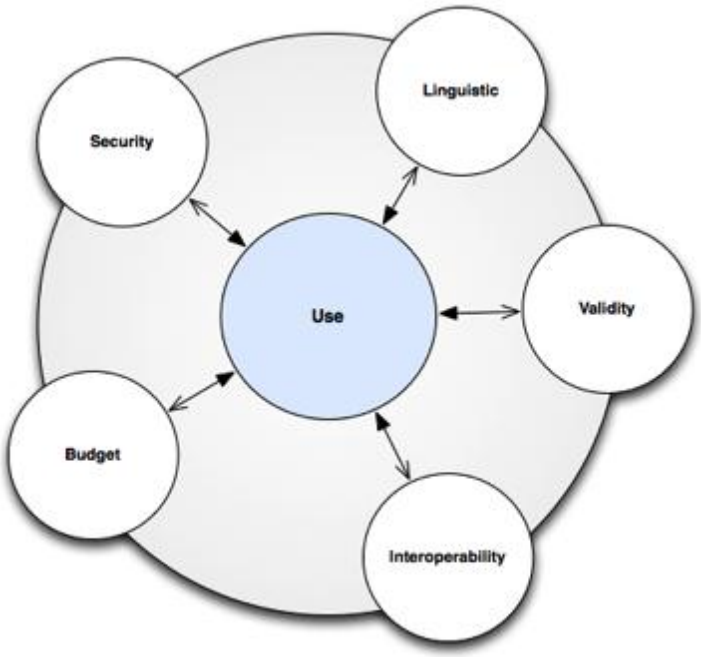


Figure 4: Interaction of Challenges

6 Compliance with the requests and expected business opportunities

Creating such system and, in particular, making specific data information of **licences and certificates per driver** available to the **competent authorities per Member State (NSA)**, **railway undertakings (RU)** and **infrastructure managers (IM)** is likely to bring immediate and future opportunities to all involved parties. These opportunities will be validated through a detailed analysis of user needs and experiences.

The anticipated opportunities are derived from the below-mentioned IT-Solution properties:

- **Immediate compliance with the request (related to the core objective)**:
  - One central data exchange point of all information in order to standardize the method of data input, information retrieval and increase interoperability;
  - Retrieval of necessary information with immediate response or in a specific timeframe according to the needs;
  - Secure interoperability;
  - Securing validity of information;
  - Standardized system on the method of exchanging information;
  - Monitoring of up-to-date or expiration of stored information and data;
  - Operate in an harmonised manner and comply with the EU Decision;
  - Address linguistic barriers;
  - Ensure standardised and timely exchange of information;
  - Manage large number of single or multiple transactions on EU level;
  - Allow check prior to the issue of Train Driving Licences (for instance, in order to prevent that a person requests more than one);
  - Allow immediate checking of validity of specific information displayed on the Train Driving Licence (for instance, in case of suspect tampering);
  - Detection of fraud attempts;
  - Allow tracking, reporting of all transaction types for statistical purposes.

- **Additional properties – Long term potential opportunities**:
  - Increasing trust among involved parties;
  - Creation of a strong data pool merging all involved parties;
  - Approaching the competent authorities of all Member States with RUs and IMs and creating common strategies or sharing existing Best Practices;
  - Allowing drivers to view their personal information;
  - Allowing drivers to initiate a process for changing specific personal or contact information;
  - Less cost on allocating Human Resources on the validity process;
  - Less cost on necessary infrastructure;
  - Increased security of data storage level and archive.

It should be noted that the long-term opportunities should be a matter of investigation in order to avoid increment of system's complexity or security issues.

Focusing mostly on meeting the requested properties related to the core objective, the EC's Decision criteria are met by the implementation of a computer based IT-Solution having four main characteristics, namely:

- **Enhancing the level of interoperability among stakeholders;**
- **Easy data entry and update;**
- **Tailor-made interfaces / bridges for existing information exchange and harmonization;**
- **Respect for user rights and personal information.**

Concerning future opportunities, after a specific period of time has passed after the release of the system, the potential of enhancing the system and providing more solutions via its progression can be evaluated. These advantages should be weighed against any disadvantages. This would particularly imply further implementation and operation costs (see below).

In order to determine the need and viability of the system and to prove the potential opportunities, the **Business models** and **Operational procedures** will be studied, the **Technical approach** will be drafted and the **Impact** on business and human factors will be identified.

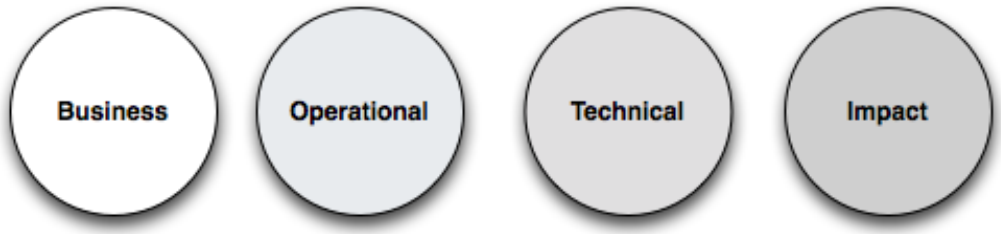


Figure 5: The four dimensions to consider

7 Technological considerations

In order to achieve the targets of the study according to the EC's directive namely to guarantee interoperability as well as immediate communication among all stakeholders, a high quality and sufficient standardization of actions would need to be set. Technologically advanced systems or standard approaches may exist or need to be developed and would also need customization in order to fit the needs as presented, especially to inform concretely the stakeholders for a specific information set.

7.1 Interoperability

Interoperability is a function in diverse type of domains of operational concepts and scenarios, policies, processes, and procedures. Organizations that manage data are autonomous regarding their adoption of architecture, design and communication technology. Autonomy in architecture and design gives leverage to adopting any of the designs suitable for holding the data. As for communication autonomy, it comes into existence when organizations are willing to share data with different vendors or solutions. For interoperability, the element of associative autonomy at different levels has to be under a controlled autonomy in order to share data across the organization through communication and exchanging of information. Interoperability is categorized into many different types.

The initiative to help interoperability is by Dublin Core[8] at a syntactical level and also to some extent at a semantic level. Various technologies are being used to achieve the interoperability at the syntactic level, such as Dublin Core, MODS, MARC (Machine Readable Catalogue), PICA, IAFA template (Internet Anonymous Ftp Archive), MDIS (Metadata Interchange Specifications) and TEI (Text Encoding Initiative).

As for interoperability or information at the semantic level, this deals with the meaning of the terms and expressions. This allows for the ability to automatically interpret the information exchanged in a meaningfully and accurate way in order to produce useful results defined by the end users of the two systems. To ensure that there is only relevant information, it is a must that semantic interoperability be exchanged or shared. This will allow for support of a higher level of contextual sensitive information requested over heterogeneous information resources and structures, as well as hiding system and syntax.

[8] Doublin Core Metadata initiative: http://dublincore.org

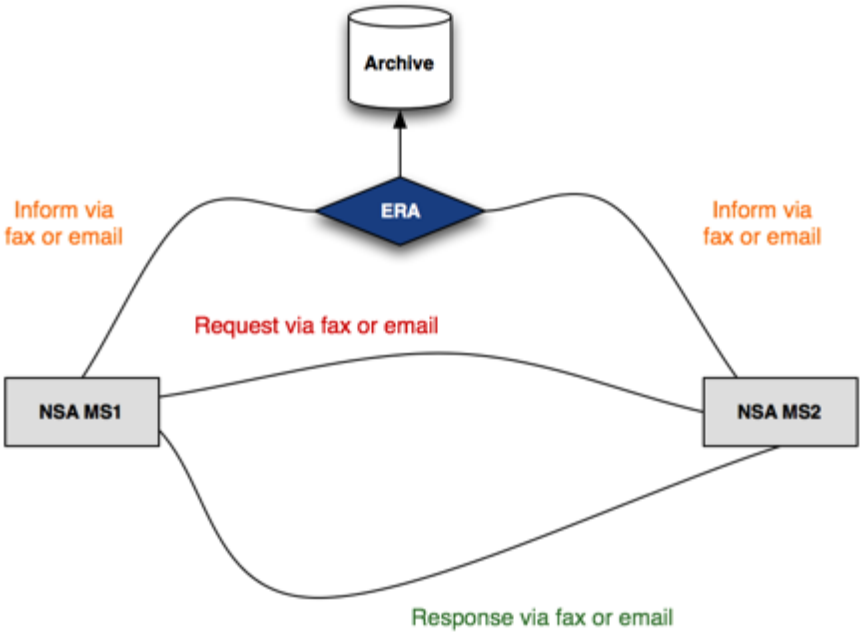
7.2 Advanced technology for information exchange

A system with advanced technological features with aim on improving communication will assist in bridging territorial distances and delays on responses, especially in situations that are highly important among various MS NSAs. Some of the key benefits are:

- information available non-stop (7-24) and respecting user credentials and workflows as well as logged in users may be able to access important details at any necessary time
- using internet technologies or 3G, communication is cheaper and all stakeholders do not need to be spending in other sources such as telephones or faxes
- less human-factor errors could appear especially under stress situations
- cross-European with capabilities to respond in own language solving any issues of translation or misinterpretation
- access to critical information, thus the results of exact or in an approximately high percentage of information that is requested, is more accurate than conventional means.

7.3 Establish technologically simplified workflows

In order to avoid the introduction of a new system to all MSs of a new system that might cause the need for training to some of the existing personnel and possible frustration, a workflow solution could be established, based on standard technological solutions such as emails, scanning and faxes. This possible workflow would be conducted as illustrated below.



In this simplified use-case scenario, the NSA from MS1 is requesting via fax or email from NSA MS2 a specific response via email. Synchronously ERA is informed about the event and archives

it as a fact. In turn, after investigation and necessary verifications, NSA MS2 is responding to NSA MS1 and informing ERA of the event. Informing ERA could succeed also at a later time segment, in a report form that both NSAs from MS1 and MS2 could verify and submit to ERA. Time response and verification issues are solely dependent on NSA MS2, which is responsible for providing the results on the specific request. The initial question though by NSA MS1 is also under quality challenge, since it might confuse NSA MS2 especially in terms of recognizing cultural and linguistic differences.

7.4 Data location and data exchange

There are three general, main directions to accomplish such a system, technologically advanced or not:

- keep records only in the NSA MS1 that the TD is registered and NSA MS2 would be only able to view the details but not store
- keep records in the NSA MS1 that TD is located and copy those records in the NSA MS2
- keep records in NSA MS1 and ERA after NSA MS2 request and it would be only available to view the details but not store

Eventually by exchanging information among NSAs of various MSs, there will be an issue of how to keep such data received from other Member States. Specific workflows and time keepings of the data storage should be considered. The third scenario by having all the information stored at ERA seems also interesting, but it has to be according to the National legislation as well as fulfilling legislation on data protection and data storage. In any case clear guidelines on when data should be exchanged and how it is then protected would be required.

7.5 Data protection

The most appropriate source for reassuring data protection on any system established in a MS in the EU is the **Directive 95/46/EC**[9]**,** on the protection of individuals with regard to the processing of personal data and free movement of such data. There might be specific legislation per MS that would be necessary to investigate upon the decision of implementing the system, although for this study, the main reference point will be the abovementioned Directive.

Principles for **data processing**, which means "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,*

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

blocking, erasure or destruction;" (art. 2 b) and **data supervision**, *"Each member state must set up a supervisory authority, an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated."* (art. 28):

- Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose and proportionality.
- Data may be processed only under the following circumstances (art. 7):
    - when the data subject has given his/her consent
    - when the processing is necessary for the performance of or the entering into a contract
    - when processing is necessary for compliance with a legal obligation
    - when processing is necessary in order to protect the vital interests of the data subject
    - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed
    - processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The data subject has the right to access all data processed about him/herself. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or is not being processed in compliance with the data protection rules. (art. 12)
- The controller must notify the supervisory authority before he/she starts to process data. The notification must contain at least the following information (art. 19):
    - the name and address of the controller and the representative, if any;
    - the purpose or purposes of the processing;
    - a description of the category or categories of data subject and of the data or categories of data relating to them;
    - the recipients or categories of recipient to whom the data might be disclosed;
    - proposed transfers of data to third countries;
    - a general description of the measures taken to ensure security of processing.
    - this information is kept in a public register.

Since there will be personal (even minimum) data exchange among MSs, the **Directive 2002/58/EC**[10] of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

sector (Directive on privacy and electronic communications) the provider of an electronic communications service must protect the security of its services by:

- ensuring personal data is accessed by authorised persons only;
- protecting personal data from being destroyed, lost or accidentally altered;
- ensuring the implementation of a security policy on the processing of personal data.

Annotation, concerning **Data retention**

The Directive determined that traffic data and location data must be erased or made anonymous when they are no longer required for the conveyance of a communication or for billing, except if the subscriber has given their consent for another use. On the sensitive issue of data retention, the Directive stipulates that Member States may withdraw the protection of data only to allow criminal investigations or to safeguard national security, defence and public security. Such action may be taken only where it constitutes a "necessary, appropriate and proportionate measure within a democratic society".

In order to ensure the availability of communication data for the purpose of investigation, detection and prosecution of criminal offences, the Directive laid down provisions for the retention of data.

8 Information Management

Information Management is the application of management techniques to collect information, communicate it within and outside an authority, and process it to enable stakeholders to be adequately informed or to assist them in taking decisions. The purpose of an information system would not only be to inform but also to retrieve critical information with a high percentage of accuracy.

Due to the fact of the complexity nature of the system in discussion, especially for the fact that information and data are not collected under the same storage location and interoperability or standardization has not yet been applied, the issues related to information management are:

- Large number of data information in various locations
- Little integration or coordination between information exchange
- Range of legacy systems requiring upgrading or replacement.
- No clear strategic direction for the overall technology environment.
- Poor quality of information, including lack of consistency, duplication, and out-of-date information.
- Lack of standardization policies
- Little recognition and support of information management by senior management.
- Limited resources for deploying, managing or improving information systems.
- Large number of diverse business needs and issues to be addressed.
- Lack of clarity around broader organisational strategies and directions.
- Difficulties in changing working practices and processes of staff.
- Internal, Regional or National politics impacting on the ability to coordinate activities enterprise-wide.

Principles that should be taken into consideration while drafting the information management policy should focus on:

- recognise and manage the complexity
- focus on adoption
- deliver tangible & visible benefits
- prioritise according to business needs
- provide strong leadership
- mitigate risks
- communicate extensively
- aim to deliver a seamless user experience
- thoughtful preparation of a pilot phase

9 Model approach

Having as basis the following principles:

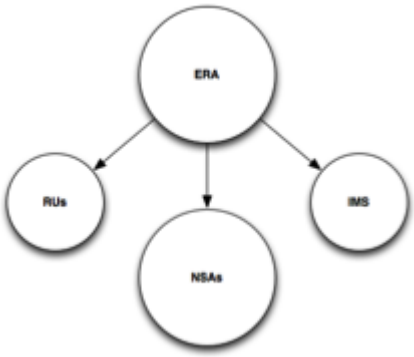
- **Achieve a high level of interoperability** and
- **Appropriate and non-complicated exchange of valid information**,
- Data security and information exchange should be according to the EC's directives respecting as well all national laws

In order to achieve this, the following models have been identified:

- **Model I**: system centralised at ERA (Annex 8.1)

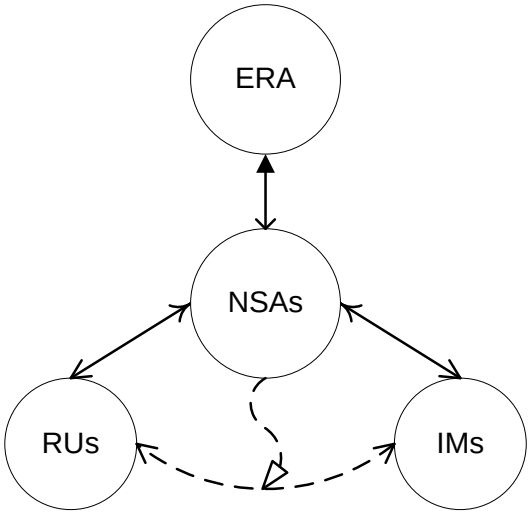
- Model II: hybrid system, interconnected by interface at ERA (Annex 8.2)

- Model III: system totally decentralized (Annex 8.3)

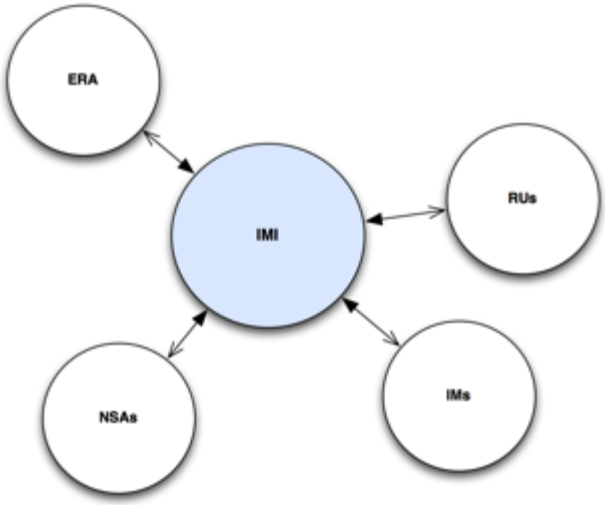


A further investigation provided us with two more models:

- Model IV is a distillation of Model I and II considering the interdependences of request-response-situations. (a) Information-exchange among NSAs is determined via the ERA; (b) information-exchange among NSAs and RUs/IMs presupposes a proceeding of verification and detailed authorisation of access-rights for each RU/IM; (c) information-exchange among RUs/IMs needs authorisations by the RUs/IMs themselves in any case; the NSAs announce therefore the responsible RU/IM here only. (Annex 10)



- Model IMI: model including IMI's messaging and information exchange system (Annex 9)



10 Cost model and assumptions for the implementing of a system for interoperability of registers

Cost model – Direct costs	Cost %	Involvement %
1. Direct costs: Pilot System implementation		
a. Implementation		
i. Technical study including use cases	20%	
ii. Development	40%	
iii. Debugging	15%	
iv. Pilot version 1.0	15%	
b. Costs on Technologies		
i. Technological background (.NET / MS SQL)	5%	
ii. System maintenance for one year	5%	
Total Cost of pilot phase	€200,000.00 (split in 2 years)	€200,000.00 (split in 2 years)
2. Human Resources allocation		
a. Project manager	1	20%
b. System analyst	1	100%
c. Database developer	1	50%
d. Application developer	1	100%
e. Network architect	1	50%
f. Expert in the field	1	20%
g. Representatives from NSAs, RUs and IMs	12	5% - 10%
Total human resources allocation Precise plan will be established in accordance to NSAs / RUs / IMs that will participate the pilot phase	6 ERA 18 total	

11 Risk allocation matrix concerning the implementation of a system for interoperability of registers

Risks / Gravity	Low	Moderate	High
1. Personal information storage and overall data protection			☑
2. Compliance with the national laws on data protection			☑
3. Quality and validity of information (Matching of information correctness)			☑
4. Time allocation for data exchange	☑		
5. Cases that the system is not necessary		☑	
6. Creation of an oversized system		☑	
7. Low frequency of requests that are necessary to be addressed	☑		
8. Costs that may apply per request for fee financed authorities (cases as DE, NL)	☑		
9. Impacts of non-implementing the system			☑
10. Unknown or unpredicted costs	☑		
11. Human factor		☑	
12. Security in terms of access information and network (in terms of people authorized to input and consult data within organizations)			☑

The risks as well as their severity definition were identified during the meeting processes with the TF and the NSAs, as well as the survey results. From those**, Risks numbered 1, 2, 3, 9 and 12** resulted in critical state and should be further investigated in the pilot phase with specific use cases that should then be developed as best practices.

It has to be mentioned that the more user categories the system should have the more complex its data security is becoming. Especially, adding drivers to the system to monitor their data increases the complexity of the system's security and therefore the costs incurred.

12 Impact Analysis

Information exchange and interoperability of registers of train driving licences (NLRs) and complementary certificates (CCRs)

Key impact assessment considerations for feasibility study

As part of the feasibility study examining suitable solutions to ensure the automated exchange of information among National Train Driving Licence Registers (NLRs) and Complementary Certificates Registers (CCRs) a high-level impact assessment has been undertaken in order to contribute to the decision-making basis regarding appropriate steps to be taken. The present note summarises the key impact assessment considerations and is structured in line with established Agency practice for impact assessment. In particular, it contains the following sections: (1) problem description; (2) identification of objectives; (3) development of options; (4) impact analysis; (5) follow-up activities. In the following each of these headers will be detailed out.

12.1 Problem description

In accordance with Directive 2007/59/EC the NSAs, as well as the RUs/IMs have to set up and keep relevant registers and are obliged to provide information (at least the minimum contained in the Directive 2007/59/EC and on the basis of access rights defined by the Decision 2010/17/EU). As such the stakeholders have to fulfil these requirements and one key consideration would be to ensure that these requirements are fulfilled in the most cost-effective manner.

Beyond fulfilling a legal requirement in the most cost-effective way it should be noted that the rationale for the requirement should be linked to needs of the railway sector in order to facilitate the safe and efficient functioning of a European railway system rather than 25+ national based systems.

The current context for information exchange between NSAs and between NSA and RU/IM is characterized by managing the tasks without harmonised procedures. This may create uncertainty among the stakeholders involved about how to deal with concrete requests and could lead to more resources required in comparison to a situation with harmonised procedures. As such this could also imply that the time taken for responding to requests is longer than with other possible systems.

On the basis of an Agency survey among the NSAs (undertaken in February 2012 with 21 of the NSAs responding) it appears that 85% of the authorities have electronic registers (though without guaranteeing interoperability between the registers). Some 60% of the NSAs have registers that are able to exchange information. As for the securing validity of information for 83% of the responding NSAs the method used for registering train driving licenses facilitate this.

It is also possible that the current approaches do not ensure the security of information exchanges in all possible cases.

The same survey also contains indications on current levels of information exchanges NSA to NSA and RU/IM to NSA. For the moment it is clear that there is a rather low level of information exchanges across Europe which should be taken into account in considering the possible solutions in order to ensure proportionality. This is particular relevant for the initial and transitionary phases following the entering into force of the Train Drivers Directive (2007/59/EC) and related legislation. It is noted that future levels of information exchanges may be higher as the importance of cross-border and international transport is expected to increase although taking a 5-10 year perspective assuming annual traffic growth of 2% would not result in substantial increases in the number of train drivers required over the next decade. This position is supported by published statistics on passenger and freight transport growth in recent years, see Tables 1 and 2.

Table 1 Passenger transport growth for EU27 (based on passenger-kilometres)

	Rail	Car	Total
1995 – 2010	15,2%	22,1%	21,0%
Per year	0,9%	1,3%	1,3%
2000 – 2010	8,9%	10,3%	9,5%
Per year	0,9%	1,0%	0,9%
2009 – 2010	0,3%	-1,3%	-1,0%

Source: DG MOVE (2012) EU Transport in figures, Statistical Pocketbook 2012

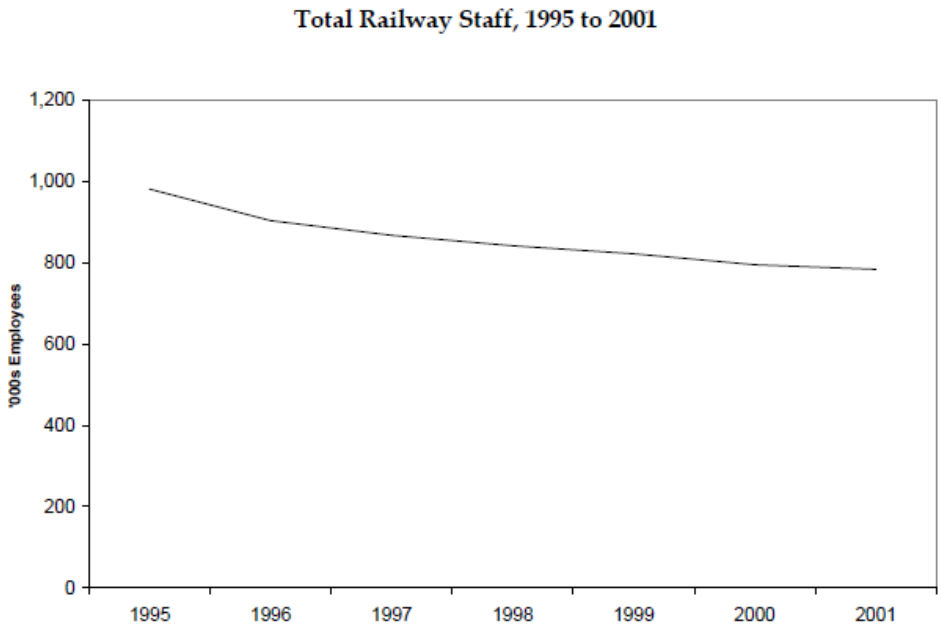
Table 2 Freight transport growth for EU27 (based on tonnes-kilometres)

	Rail	Car	Total
1995 – 2010 Per year	1,0% 0,1%	36,2% 2,1%	25,2% 1,5%
2000 – 2010 Per year	-3,4% -0,3%	15,6% 1,5%	9,5% 0,9%
2009 – 2010	8,0%	3,9%	5,3%

Source: DG MOVE (2012) EU Transport in figures, Statistical Pocketbook 2012

Further evidence supporting this view is provided from trends in employment in the railway sector in Europe, see Figure 6. The figure shows a declining trend for employment in the EU15 countries over the period 1995 to 2001. This pattern was a continuation from the period 1980 to 1995 where railway employment in the EU15 state railways fell by 35 per cent. Overall, this trend has continued in recent years such that the total railway staff in these countries in 2009 numbered 437 100 according to the latest statistics (DG MOVE, 2012). It should be noted that part of this decline is due to outsourcing and sale of peripheral businesses in the European railways.

Figure 6 Total Railway Staff EU15. 1995 to 2001



Source: NERA (2004) Study of the Financing of and Public Budget Contributions to Railways, Final Report prepared for the European Commission, DG TREN.

12.2 Identification of objectives

The key objective for this work is to identify frameworks for improved information exchange regarding train driver licenses and complementary certificates between the concerned stakeholders addressing their current and possible future needs. In particular, the objectives should work towards addressing the identified problems as outlined in the previous section.

As such relevant objectives to be considered in developing appropriate solutions for information exchange would then include:

- Cost-effective information exchange (taking into account both costs of proposed arrangements and actual needs)
- Usefulness and relevance of solutions for information exchange
- Security of access
- Data protection of personal data

It is noted that there may be conflicting objectives such that the proposed solution(s) needs to consider the various trade-offs. These objectives cover the key aspects

12.3 Development of options

The key principle of the impact assessments will be the comparison of the Do-nothing option with several Do-something options. The Do-nothing would be represented by current solutions used by the different stakeholders. This would cover a range of different solutions, e.g. fax, email, telephone and even automatic exchange via electronic registers (if any).

The different Do-something options examined as part of the feasibility study include:

- Dedicated models (I, II, III, IVa & IVb)
- Customisable existing solutions (IMI)
- Existing (similar) registers (ISA-TACHOnet)

Further details of these solutions are given elsewhere in the feasibility study.

It worth mentioning that for both the Do-nothing and Do-Something options information exchange will take place. This is important as this means the impact assessment should not address the issue of information exchange as such but only the most effective / efficient ways of

organising that information exchange. The options will vary in terms of costs and other properties / characteristics (e.g. speed, automatic interaction, security, validity of information, scalability with respect to information request volume, coverage).

12.4 Impact analysis

The impact analysis will consider how the different options compare in terms of key properties. In particular, this should take into account proportionality with respect to real needs and the costs incurred (as stated in Whereas (7) from Commission Decision 2010/17/EC).

A useful overview of the different options is set out in the following figure where the options are compared in terms of the key properties.

Figure 7 Comparison of identified options in terms of properties for information exchange

	Do-nothing (current approaches)	Dedicated systems	IMI	TACHOnet
Costs	Not clear (further data collection required here – important point is that a pragmatic solution may in fact introduce savings)	ECVVR estimates of development costs would be relevant 0,5 mln EUR (to be reviewed)	No costs incurred for the development, promotion, operation and maintenance	Cost figures available suggest that there could be costs of between 5 and 10 mln EUR
Speed	No not necessarily	Yes definitely	Yes, somewhat	To be considered
Automatic interaction,	No not necessarily	Yes definitely	No not real-time	To be considered
Security of access	Not necessarily guaranteed in all cases	Yes guaranteed	Yes guaranteed	Yes guaranteed

Validity of information	Not necessarily guaranteed in all cases	Yes definitely	Satisfactory	Yes definitely
Scalability	Yes somewhat (depends on what is currently in place)	No (the capacity cannot be adjusted according to volume, costs would broadly remain the same with low or high volume)	Scalability is not an issue given the zero costs	To be considered
Coverage	Yes, but possibly in a non-harmonised way	Yes definitely	Not fully – deals with NSA to NSA interactions but not NSA to RU / IM	To be considered

Note: ISA is not considered here as our information suggests that the system is still under development

As for the characteristics of the three do-something options the Figure indicates that TACHONet is performing worse than the other two options in terms of the high costs (and possibly also different focus than required re. train drivers' licences / certificates). A dedicated system (whether model I, II, III or IV) also entails costs and there may also be concerns regarding lack scalability with respect to actual volume. The option of IMI entails no costs for the development, promotion, operation and maintenance for the involved stakeholders. Two areas where IMI is disadvantaged: (1) not real-time information exchange; (2) covers NSA to NSA but not NSA to RU/IM. As for the first aspect we note that real-time information may be dispensable at this early moment of implementation of the EU train driver licence model and without having sufficient experience on the sector's need for immediate response to requests. For the second aspect we are aware that IMI is considering the possibility to add such linkages to the information exchange system. As part of a pilot / experience phase this dimension could be explored further.

Overall, our analyses suggest that there so far is rather limited information available about the frequency of requests (as well as other aspects of user needs), although indicative evidence (from ERA surveys) points towards a relative low level of transactions. Furthermore, there seem also to be relative low importance given to time critical information requests regarding train driver licences and complementary certificates with the exception of one very specific case.

As such the limited information available suggests that more time for data collection is required especially during a period outside the initial / transitionary phase in order to get an accurate picture of the actual level of transactions as well as other aspects of user needs. The need for more time would call for a pragmatic approach in order to ensure that appropriate solutions are adopted. Especially, a dedicated system may be too soon in this context.

The apparent low level of transactions at this point would point towards relative simple and light solutions with limited cost implications rather than more complex and expensive solutions which may not be justified in terms benefits.

Limited importance to time critical information would suggest that a solution involving automatic (real-time) response may not currently be in much demand.

As such it is also relevant to take into account the possible sunk costs related to stakeholders' investment in registers to date which would put importance to the most appropriate timing of more complex systems at the time of replacing / upgrading the existing systems.

The impact assessment therefore suggests that an appropriate step could be to explore the use of IMI in a pilot phase involving the NSAs.

12.5 Follow-up activities

On the basis of the findings of the high-level impact assessment a pragmatic and step-wise approach regarding proposals for improving information exchange is required. It is envisaged that further impact assessment will be required during the pilot / experience phase. In particular, this would involve consideration to the advantages / disadvantages of the pilot solution and analysis of further developments. It is expected that the proposed solution will contribute to the provision of information about frequency and type of requests. Indeed, this pilot solution would then work towards the aim behind Whereas (7) from Commission Decision 2010/17/EC: *'…a survey of the number of transactions is necessary to perform a cost benefit analysis and propose a feasible solution that does not impose administrative costs that might be disproportionate to real needs'*.

13 Conclusions & recommendations

As already mentioned this study is evaluating the feasibility of a computer-based application for exchange of information among NSAs, RUs and IMs and to provide a possible business model in order to comply with EU Decision Directive 2010/17/EC and allow the decision making foreseen by Article 3 therein.

The envisaged computer-based application consists of a web based tool. It enables the information-exchange on the base of the available data of all national registers (NLR) and includes the expectation to integrate the company registers (CCR) in future developments. This will improve the interoperability in the exchange of information, but with restrictions:

- in the cases of reasoned requests only;
- accompanied by a high-grade control of the access-rights for all data.

Finally, the selected approach could facilitate a solution, which can announce the assured current validity of the licences in special cases immediately.

In order to accomplish this study, the representatives of the stakeholders (Article 35 WG members and Task Force representatives) have provided to ERA all the necessary information and the point of view of users.

Initially three business models specifically designed on the basis of requirements in the Directive 2007/59/EC and Decision 2010/17/EU were investigated:

- Model I: system centralised at ERA (Chapter 8.1)
- Model II: hybrid system, interconnected by interface at ERA (Chapter 8.2)
- Model III: system totally decentralized (Chapter 8.3)

Discussions among the sector soon revealed that the proposed models seemed not able to overcome some very critical points. In fact the involved actors were not confident enough on:

- the assurance concerning data ownership and the security of data flow;
- the protection of personal data (including the level of application of national laws)
- the cost for ensuring the physical interconnection between National registers, which were not developed according to standardized processes, that may be disproportionate in relation to the number and to the type of information to be shared (not yet quantifiable due to the novelty of the overall legal framework).

It has to be considered that especially this last aspect of prematurity in the implementation of the registers and the diversity of existing national rules related to the procedure of information management and protection of personal data is expected to be at any time an obstacle to the development of a dedicated information system and have a very heavy impact on any decision.

Further investigations on the possibility to ensure the fulfillment of requirements and the confidence of the sector led to the evaluation of other dedicated models and to the review of

existing systems that could constitute a possible technical/organizational reference. In this stage two main models were evaluated:

- Model IV: process oriented modulations of Model I and Model II (Annex 10)
- Existing models as IMI, ISA and Tachonet (Annex): IMI was considered worthwhile deeper examination regarding the possibility for using its messaging and information exchange system between NSAs (in a first phase) (Annex 9)

Taking into consideration the evaluation of the models, all comments / remarks / proposals of representatives during meetings and incorporating results of a survey circulated among NSAs, **the study concludes that the most feasible solution at this stage is the adoption of the IMI System, for the following reasons:**

- **it ensures secure transactions, with log-in options and access rights that fulfills the requirements in the Directive 2007/59/EC and in the Decision 2010/17/EU;**
- **it covers all given prerequisites that were set by the EU for the exchange of information among competent authorities in the framework of professional qualification;**
- **it does not replace existing systems and registers, so it does not require any economic effort for design, implementation, maintenance or migration;**
- **it respect the current EU and national legislations concerning protection of personal data;**
- **It ensures validated translation of the information;**

The system is already in production mode and requires only a customization in order to start a pilot phase linking all the NSAs and ensure exchange of information between them.

From the technical point of view, the IMI model ensures high performance, quality and validity of information in terms of and specifically on:

- Interoperability;
- Immediate access to information on crucial cases (for authorized users);
- Standardized method;
- Computer based system;
- Data Security;
- Access Rights on information level with high level of security;
- Low cost for all involved stakeholders.

On the basis of the above listed conclusions, this study recommends that:

- Model IMI is adopted for the exchange of information among the NSAs.
- The exploration for a standardized computer based method in order to connect and ensure the exchange of information between NSAs and RUs/IMs is postponed to a later stage.

Way forward

The approval of this feasibility study by the members of the Article 35 WG will lead to the design of the pilot phase, which may start after necessary arrangements with DG Internal Market, IMI Project Manager, during the first half of 2013. The pilot phase will involve

representatives from the NSAs and the TF and development is then expected to start around the mid of 2013. The first phase of the Pilot with exchange of information may be split into four main parts:

- Development of technical specifications;
- Implementation of already defined use cases and user rights definition;
- Customization of IMI's system and add sub-systems for RUs/IMs;
- Testing and conclusion to version 1.0.

The second phase of the Pilot will include the data exchange among stakeholders.

The expected results and achievements of both pilot phases are:

- Gather a TF that along with ERA will ensure the correctness of the developments;
- create a workflow based on IMI's existing system that will comply with the needs;
- involve all NSAs for testing and securing the success of all processes and workflows of the first phase of the pilot;
- assure that IMI is able to provide what is necessary according to chapter 3.3 of this document;
- customization of IMI's templates according to the specifications and use-cases;
- translation of the templates and the standard questions in the system;
- standardization of all the workflows and processes according to the use-cases;
- define the second phase of the pilot system including the data exchange among the stakeholders;
- deliver a report to Art. 35 group on the achievements.

The specific strategy is suggested to cover not only current / immediate needs but also future. Its potential success and added value will be significant since it may advance the communication among all stakeholders of rail services across the EU. It is acknowledged that this is the first step towards interoperability among NSAs, RUs and IMs.

14 Annex 0: Definitions

Title	Acronyms and Definition
CA	Competent Authority is the National Safety Authority as defined in the Directive 2004/49/EC (Railway safety Directive)
CCRs	Register(s) of Complementary Certificates
IM	Infrastructure Manager
NLRs	National Register(s) of Train Driving Licences
NSA	National Safety Authority
RU	Railway Undertaking
Computer Based solution / System	*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.*
Interface / Bridge	A function that will unite and make information accessible between different systems.
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.
Access rights for NLRs	Specifically for the basic parameters of **NATIONAL REGISTERS OF TRAIN DRIVING LICENCES** (NLRS) Concerning the Access Rights as per the EC Decision (2010/17/EC) Annex 1 – Ch. 4: *Access to the information contained in the NLR shall be granted to the following interested parties for the following purposes:* • *to the competent authorities of the other Member States, upon reasoned request, for:* ▪ *controlling trains operating in their area of jurisdiction,* ▪ *making enquiries regarding compliance with Directive 2007/59/EC by all those active in their area of jurisdiction,* • *to the Agency, upon reasoned request, for evaluating the development*

	of train driver certification in accordance with Article 33 of Directive 2007/59/EC, in particular regarding the interconnection of registers, • *to any employer of drivers, for consulting the status of the licences in accordance with article 22(1)(b) of Directive 2007/59/EC,* • *to railway undertakings and infrastructure managers, employing or contracting train drivers, for consulting the status of licences, in accordance with Article 22(1)(b) of Directive 2007/59/EC,* • *to train drivers, upon request, for consulting the data concerning them,*
Data Exchange for NLRs	Concerning Data exchange as per EC Decision (2010/17/EC) Annex 1 – Ch. 5: *Access to relevant data shall be granted upon formal request. The competent authority shall provide the data, without delay, in a manner which ensures secure transmission of information and protection of personal data.* *Competent authorities may offer login facilities on their websites to all who have access rights, provided they ensure that the grounds for requests are checked.* *to the driver must be kept beyond the 10-year period if so required.*
Data Retention for NLRs	Concerning the Duration of data retention as per EC Decision (2010/17-/C) Annex 1 – Ch. 6: *All data in the NLR shall be kept for at least 10 years from the date of end of validity of the train driving licence. If at any time during the 10-year period an investigation involving the driver is started, data relating*
Data Exchange for CCRs	Specifically for the basic parameters of **TRAIN DRIVERS' COMPLEMENTARY CERTIFICATES (CCRS)** Concerning Data exchange as per EC Decision (2010/17/EC) Annex 2 – Ch. 5: *Access to the information contained in the CCR shall be granted to the following interested parties for the following purposes:* • *to the competent authority of the Member State in accordance with Article 22(2)(b) of Directive 2007/59/EC,* • *to competent authorities of the Member States in which the railway undertaking or infrastructure manager operates, and where the driver is authorised to drive on at least one line of the network:* ▪ *for their task of monitoring the development of certification, under Article 19(1)(g) and Article 26 of Directive 2007/59/EC,* ▪ *for their inspection tasks under Article 19(1)(h) and (2) and Article 29(1) of Directive 2007/59/EC (this task may be carried out by a delegated entity),* • *to train drivers, for the data concerning them, in accordance with Article*

	22(3) of Directive 2007/59/EC, • *to investigation bodies set up in accordance with Article 21 of Directive 2004/49/EC, for investigating accidents, in particular as stated in Article 20(e) and (g) of that Directive,* *Companies shall be free to grant access to other users, subject to personal data protection.*
Access rights for CCRs	Concerning Access Rights as per EC Decision (2010/17/EC) Annex 2 – Ch. 4: *In accordance with Directive 2007/59/EC, access to relevant data shall be granted:* *(a) to the competent authorities where the railway undertaking or infrastructure manager is domiciled, in accordance with Article 22(2)(b) of Directive 2007/59/EC,* *(b) to competent authorities of other Member States, upon request, in accordance with Article 22(2)(c) of Directive 2007/59/EC,* *(c) to drivers, upon request, in accordance with Article 22(3) of Directive 2007/59/EC.* *The railway undertaking, infrastructure manager or delegated entity shall provide the data, without delay, in a manner which ensures secure transmission of information and protection of personal data.* *Railway undertakings and infrastructure managers may offer login facilities on their websites to all who have access rights, provided they ensure that grounds for requests are checked.*
Data retention for CCRs	Concerning the Duration of data retention as per EC's Decision (2010/17-/C) Annex 2 – Ch. 6: *All data in the CCR shall be kept for at least 10 years from the last expiry date referred to on the certificate.* *If at any time during the 10-year period an investigation involving the driver is started, data relating to the driver must be kept beyond the 10-year period if so required.* *Any changes in the CCR shall be recorded.*

15 Annex 1: Glossary

The glossary below provides the reader with an overview of terms used throughout this study.

Term	Description
CEAF	The **C**ommission **E**nterprise **A**rchitecture **F**ramework. It shows from each stakeholder's perspective (business or IT) the blueprint of all aspects involved in constructing information systems and how they relate.
COTS	The term **C**ommercial **o**ff-**t**he-**s**helf product (hardware or software) refers to readily available products that can be acquired from the market (instead of being developed in-house).
CPO	The **C**orporate **P**roject **O**ffice – created by the Commission's decision SEC(2004)1267[11]. It is hosted by DIGIT and its duties concern horizontal activities related to information systems coordination in the Commission, including the preparation and presidency of the Methodology, Architecture and Portfolio management working group. Its mandate is detailed in Annex 1 of the SEC(2004)1267[12] communication.
CTI-IS	The **C**omité **T**echnique **I**nformatique-**I**nformation **S**ystems – created by the Commission's decision SEC (2004)1267[13]. The CTI-IS units all heads of information systems development in the DGs. The Committee assures the interservice coordination for all maters related to information systems in the Commission. Its mandate is detailed in the SEC(2004)1267[14] communication.

[11] See heading "20/10/2004 Memorandum to the Commission SEC(2004)1267" in the webpage below: http://myintracomm.ec.testa.eu/serv/en/digit/strategy_and_policy/it_governance/docs/Pages

[12] See heading "20/10/2004 Memorandum to the Commission SEC(2004)1267" in the webpage below: http://myintracomm.ec.testa.eu/serv/en/digit/strategy_and_policy/it_governance/docs/Pages

[13] See heading "20/10/2004 Memorandum to the Commission SEC(2004)1267" in the webpage below: http://myintracomm.ec.testa.eu/serv/en/digit/strategy_and_policy/it_governance/docs/Pages

[14] See heading "20/10/2004 Memorandum to the Commission SEC(2004)1267" in the webpage below: http://myintracomm.ec.testa.eu/serv/en/digit/strategy_and_policy/it_governance/docs/Pages

Term	Description
Data Centre	The Data Centre is often used to describe the services offered by Directorate C of DIGIT and concerns the provision of hosting facilities (infrastructure, hardware, software, network, etc.) to run and operate the information systems.
Document Management Officer (DMO)	The role of the Document Management Officer (DMO) is defined in the Decision 2002/47/CE, CECA, Euratom. Each DG has one or more DMO to ensure the application of the principles of a document management system. The DMO establishes a sound and reliable organisational structure for document management within each Directorate-General or equivalent department, at interdepartmental level and at Commission level. He or she is responsible for the establishment and the implementation of a filing plan associated with a common nomenclature for all the Commission's departments. This filing plan is employed to organise files and improve openness and access to documents. He or she organises, within the Directorate-General, training for the staff in charge of the implementation, control and monitoring of the management rules and ensures horizontal coordination between the document management centre(s) and other concerned departements.
Data Protection Co-ordinator (DPC)	The Data Protection Co-ordinator (DPC) is nominated by the DG and assures a coherent implementation of Regulation 45/2001 in the DG. He or she provides advice and assistance to all responsible persons and specifically assists Controllers in the DG in their Notifications to the Data Protection Officer (DPO). He or she sets up the inventory of applications for the processing of personal data in the DG, liaises and co-operates with the DPO. He or she also represents the DG in the network of co-ordinators which is chaired by the DPO.
Data Protection Officer (DPO)	Each institution has one or more Data Protection Officers (DPO) to ensure the application of the principles of personal data protection in the institution. Each DPO keeps a register of all personal data processing operations in his/her institution. He/she also provides advice and makes recommendations on rights and obligations. He/she notifies risky processing of personal data to the European Data Protection Supervisor and responds to requests from the European Data Protection Supervisor. In critical situations he/she may investigate matters and incidents on request or on his/her own initiative.

Term	Description
FTE	**F**ull-**T**ime **E**quivalent. One FTE indicates the equivalent work of one full-time person. A half FTE indicates the equivalent work of a half-time person, and so on.
GovIS	The Commissions IT **Gov**ernance **I**nformation **S**ystem. GovIS (http://applicationservers.cc.cec.eu.int/govisp/). It enables decentralised acquisition and sharing of data about the Commission's Information Systems and IT projects.
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
ISSP	The **I**nformation **S**ystem **S**ecurity **P**olicy developed by DG ADMIN/DS. The ISSP is a comprehensive security policy indicating which security measures should be taken into account when developing information systems.
MAP	The **M**ethodology, **A**rchitecture and **P**ortfolio management working group created by the Commission's decision SEC(2004)1267[15]. The MAP is a sub-group of the CTI-IS and aims to ensure the operational coordination of information system development in the Commission. It reports its activities to the CTI-IS. Its mandate is detailed in Annex 1 of the SEC(2004)1267[16] communication.
Programme	The term Programme often refers to the collection of projects aimed towards the same goal (e.g. the ABAC programme which comprised many projects to realise the introduction of an accrual based accounting in the Commission).

[15] See heading "20/10/2004 Memorandum to the Commission SEC(2004)1267" in the webpage below: http://myintracomm.ec.testa.eu/serv/en/digit/strategy_and_policy/it_governance/docs/Pages

[16] See heading "20/10/2004 Memorandum to the Commission SEC(2004)1267" in the webpage below: http://myintracomm.ec.testa.eu/serv/en/digit/strategy_and_policy/it_governance/docs/Pages

Term	Description
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.
TCO	**T**otal **C**ost of **O**wnership. The TCO of an information system defines the total estimated cost to develop the system, to put it into production, to operate it, to support it, to maintain it, to phase it out at the end, etc. The cost estimation is as comprehensive as possible and should include all costs from the very inception of the system until its phase out.

16 Annex 2: Acronyms and Abbreviations

Title	Description
CA	Competent Authority
CCRs	Register(s) of Complementary Certificates
IM	Infrastructure Manager
NLRs	National Register(s) of Train Driving Licences
NSA	National Safety Authority
RU	Railway Undertaking
EIN	European Identification Number

17 Annex 3: Existing practices

17.1.1 IMI

Internal Market Information System (IMI) is a secure online application that allows national, regional and local authorities to communicate quickly and easily with their counterparts abroad. IMI is accessible via the Internet without the need to install any additional software.

The development of IMI was funded under the IDABC programme (Interoperable Delivery of European eGovernment Services to public administrations, businesses and citizens) with a total budget of € 1,300,000 over a period of five years (2005-2009).

IMI helps users that are working for national, regional or local authorities in order to:

- find the right authority to contact in another country,
- communicate with them using pre-translated sets of standard questions and answers,
- reduce the response time, with a response period of two weeks for 60% of the requests,
- IMI offers a directory of registers held by authorities all over Europe, such as trade registers or registers of lawyers, with a multilingual search function. If a register is available online, IMI provides with the direct link to it

As IMI states, "*because Member States have been closely involved in devising the system, IMI offers uniform working methods agreed by every EU country*". However, should disputes arise, national or regional IMI coordinators can intervene. The European Commission runs a central IMI helpdesk.

IMI's basic characteristics:

- an authority can identify a partner authority in another country with the help of the IMI multilingual search function,
- create a request by selecting standard questions in your own language,
- users can also type in free text and attach documents,
- send the request to your partner authority,
- a partner authority receives the request in its own language,
- track the progress of your request,
- a partner authority replies to another country's authority in its own language,
- receive the reply in authority's local language.

Data Protection:

IMI has been developed with data protection in mind. It offers a much higher level of protection and security than traditional communication means, such as email or telephone. In particular:

- procedural and technical features help ensure that personal data is processed only for the purposes for which it is intended;
- restrictions are imposed to ensure that only people who need to see personal data related to a case have access to it; and
- after an agreed period following the closure of a case, personal data is automatically deleted from the system.

Benefits for NLR:

IMI and specifically the fact that it is a running and accepted system, assists on:

- using specific policies for exchanging information among various countries, respecting local but also EC's legislation
- respecting all of the Professional Qualifications Directive (2005/36/EC)[17] and Services Directive[18] data protection and data security issues covered
- already established and tested system, which will not need extra development or investigation

17.1.2 ISA

The goal of the project Interoperability Solutions of European Public Administrations (ISA)[19], is to provide a Trusted Document Exchange Platform that re-uses the existing e-PRIOR infrastructure and to proof the cross-sector re-usability of e-PRIOR. The main objective is to provide a set of integrated re-usable components designed within a coherent architecture that implements a technical platform able to support and secure a number of business document workflows between European Commission and national parliaments, permanent delegations, local governments, businesses, citizens and other EU institutions.

The intention of the project is to improve - in terms of reliability, security, efficiency and capacity - the communication between European Commission and administrations, businesses and citizens. The platform will guarantee equal treatment to all 3rd parties who need or want to exchange documents with the European Commission, and will replace, when needed and possible, notification by traditional means (via the post) with legally equivalent electronic interactions.

[17] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:255:0022:0142:EN:PDF

[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:EN:PDF

[19] http://ec.europa.eu/isa/index_en.htm

This action addresses the domain of Government-to-Government (G2G), Government-to-Business (G2B) and Business-to-Government (B2G) and is related to the following priority areas of the ISA programme:

- Interoperability Architecture – Building blocks
- Trust and Privacy

EXPECTED BENEFICIARIES AND ANTICIPATED BENEFITS

Beneficiaries	Anticipated benefits
Member States' public administrations and EU Institutions	Re-use of architectural aspects. In fact, the adoption of "Service Oriented Architecture" within which the various interactions between Commission systems (eg.: e-Greffe, ASAP, EDMA, State Aids management systems, e-Questionnaire), the e-PRIOR system and the "back office" of the public administration might be designed as invocation of services) Cost savings and improve efficiency, reduce time-to-market and ensure interoperability as handling legislative documents and follow up of legislative procedures can be automated (see business cases offered by e-Greffe and ASAP). Free-to-use open source tools for national parliaments and permanent representations to send and receive electronic legislative documents and metadata (see business cases offered by e-Greffe and ASAP). These tools can be used for exchanging other electronic business documents with other stakeholders (see business cases offered by DG COMP) Experience, lessons learnt, specifications, tools and components published as open source reusable by any Member State or EU Institution Replacement of notification by traditional means (via the regular mail) with legally equivalent electronic interactions, saving time, money and paper (green).
IT services in the Commission	The European Commission, because of its central position, is more and more called upon to develop distributed systems to coordinate political actions in various fields. If a generic system can be defined and later put in place, it will be a very big progress for the whole interoperability issue in Europe. This would of course also represent important cost savings since the infrastructure of such systems would then be reusable.
EU Tax payer	Given the potential economies of scale realised if such a generic system can be put in place, the indirect benefits for the EU Tax payer are obvious

Graphic: Expected stakeholders and anticipated benefits

Benefits for NLR:

ISA, which is under development, is already providing to NLR the understanding of complexities on data exchange and also data security, providing a solution to this issue as well, especially by being compliant with both national and EC rules. The proposed interoperability architecture is also interesting to the approach and verification of the current study especially Action 2.1

Towards a European Interoperability Architecture[20] and Action 2.2 Achieving a modern ICT standardisation policy[21].

17.1.3 TACHONET

The **Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards** (TACHONET) is assisting national administrations to keep roads safer across the European Union by sharing information on Smart Cards and the digital tachograph with each other.

TACHONET is a telematic network in operation across the EU. It acts as a central hub for the exchange of information between the national administrations responsible for issuing tachographs (in-vehicle recording equipment) to enforce rest periods and monitor the driving times of professional drivers.

In order to contribute to the successful implementation of new road regulations, a new electronic device called the digital tachograph is used in conjunction with smart cards. Tachographs are recording instruments that measure speed, miles travelled and the number and duration of stops.

TACHONET minimises duplication of work across the Member States and maximises efficient tracking of drivers.

TACHONET was created with two key objectives:

- To ensure fair competition between drivers, hauliers and other modes of transport;
- To enhance road safety by avoiding driver fatigue and controlling compliance with the legislation on speed limits.

The system is based on a system of message-exchanges between the EU Member States. The new system comprises a smart card and an electronic on-board tachograph. The digital tachograph guarantees better compliance with rules on driving times, rest periods and road safety and puts an end to the most common abuses of the present mechanical system (accident risk data demonstrates that after an 11-hour work span the risk of being involved in an accident doubles).

To take a concrete scenario: John is a long-distance lorry driver based in the UK. He regularly drives from Newcastle to Lyon in France. Although he is aware of the dangers of driving when fatigued, he decides to make an application for a tachograph and smart card both in the UK and

[20] http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-1action_en.htm

[21] http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-2action_en.htm

in France. In this way, he hopes to bypass the system and not be caught driving for too long periods without a rest.

- Member States are responsible for issuing the smart cards on time and in a reliable and secure manner. Therefore, when a driver goes to register in either France or the UK, the Administrator will automatically enter the request details into the card issuing software application developed by the UK/France.
- The local software application will in turn 'notify' the central TACHONET application which acts as a 'hub and spoke' for sending requests and receiving responses from other Member States.
- When the central TACHONET application receives a request from a the local software application in the UK/ France it will validate it, store it and return an acknowledgment of receipt to the original administrator dealing with John's request.
- It is also able to broadcast the request to all Member States, receive responses and provide a consolidated response to the original requester. The TACHONET system ensures that these transactions take place efficiently and securely. It is at this point that John's attempt to misuse the system will be detected. He cannot make more than one application within the EU.
- The Administrator will not only refuse his application, but will also follow proceeds against him for attempt to defraud the system. However, if John has only made one application, then he will be cleared to receive his card and tachograph.

It worth's mentioning that it is stated under EC's recommendations "*Member States should enable, encourage and support their national enforcement and control bodies to use TACHOnet and/or equivalent systems in order to facilitate effective checks of the validity, status and uniqueness of driver cards, notably either at the roadside, or at the premises of undertaking"*.

Benefits for NLR:

Besides its scope diversity, it is interesting validating further the standard process of recognition of each driver and additional details that exist on the tachograph / smart card, especially by the fact that is accepted by the EC and respects all data security and privacy issues. System's architecture, may also provide solutions for the information and messaging / communication bridges among NSAs from MSs.

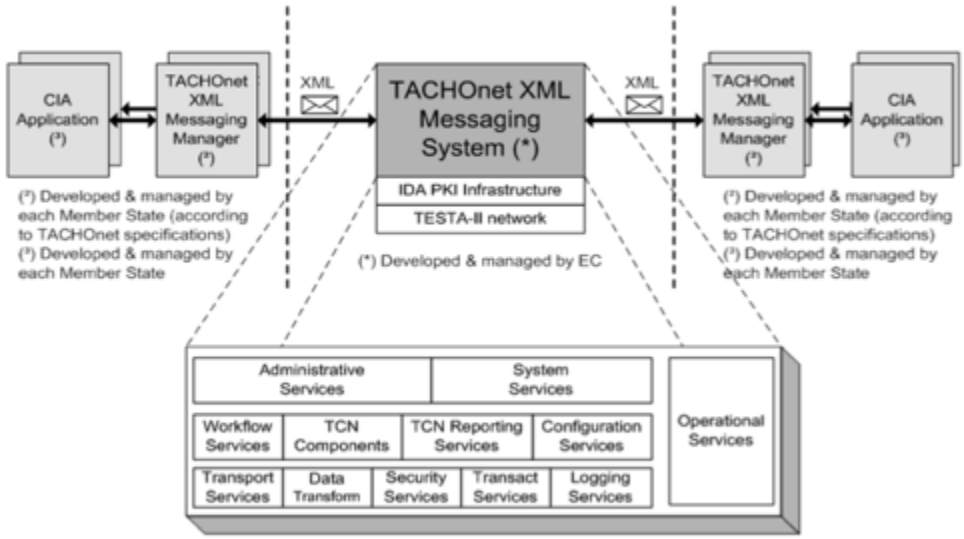


Figure: Tachonet Architecture

18 Annex 4: IMI's presentation

- File attached -

19 Annex 5: Mandatory requirements concerning registers and exchange of information

❶.1 Obligations concerning NLRs

ID	Legal reference	Legal requirement	Explanation (if required)	Could this action be pre-defined (structured)	Could IMI provide a support?
1.1	**Dir. 2007/59/EC *Article 22.1.(a)***	***Article 22*** ***Registers and exchange of information*** *1. The competent authorities **shall be required to:*** *a) **keep a register of all licences** issued, updated, renewed, amended, expired, suspended, withdrawn or reported lost, stolen or destroyed. This register shall contain the data prescribed in section 4 of Annex I for every licence, **which shall be accessible using the national number allocated to each driver. It shall be regularly updated;***	*A request to an NSA should be done using the national number for each driver (EIN).*	*Standardization of these processes is highly important. In any case of system or method chosen, in order to achieve high quality of results and performance there has to be a concrete methodology of information storage and exchange, with specific meta-data to allow interaction among competent authorities according to specific user credentials and security schema*	*NO - Storage of information would imply a centralized method that opposes NSA's wish based on potential security issues, national legislation and systems' interaction performance.* ***IMI cannot provide a technical solution to interconnect the National registers.***

1.2	Dir. 2007/59/EC *Article 22.1(b)* *+* EC Decision 2010/17/EU Annex I.4	*b) supply, upon reasoned request, information on the status of such licences to* ***….the competent authorities of the other Member States,*** Access to the information contained in the NLR shall be granted to the following interested parties for the following purposes: - *To the **competent authority of the other Member State**, upon reasoned request, for* - *Controlling train operating in their area of jurisdiction* - *Making enquiries regarding compliance with Directive 2007/59/EC by all those active in their jurisdiction*	*The request to an NSA should concern the status of the licence associated with an EIN.*	*By having an inter-connected method this can be standardized. Nevertheless these information should be according to national legislation and aligned to EC's principles* *The solution that will be selected should be fully adaptable according to user's credential nature and provide or not specific type of information*	*YES - Messaging is the strong point of IMI. Taking the applied method as best practice will resolve research time for ERA during the implementation process* *YES - IMI can support such a system's response* ***The IMI Information request module could be an efficient communication tool for the National authorities*** ***Partially – Through IMI National authority could request access to the national registers, or ask for information contained in them, however the access to such registers would have to be managed individually outside IMI.***

1.3	**Dir. 2007/59/EC *Article 22.1(b)*** ***+***	(b) supply, upon reasoned request, information on the status of such licences to **….. the Agency**	ERA is only entitled to information on the status of the license and informed of all transactions that would succeed	*Many cases of "Reasoned requests" may be reported and be used as templates. Practically it will imply the existence of predefined questions before submitting a request*	*Partially YES – Further investigation for action templates is necessary* ***further legal analysis would be required regarding the role of the Agency – to be seen in the context of the IMI regulation.*** ***ERA is able to use IMI, though all NSA's should agree on it. As it is stated in the ver. 2.0 of the feasibility EC's directives on data protection allow this.***

	EC Decision 2010/17/EU Annex I.4	Access to the information contained in the NLR shall be granted to the following interested parties for the following purposes: **To the Agency**, upon reasoned request, for evaluating the development of train driver certification in accordance with article 33 of Directive 2007/59/EC, in particular regarding the interconnection of registers,	ERA could be granted access to the total volume of licenses issued, suspended. etc. in total or, for instance, within certain periods of time , for monitoring purposes.	*In the case of emergency or predefined ready to grand access to information the solution should adapt. In case of emergency, basic on specific pre-sets, information should be able to be communicated with no further delay. Respecting always specific user credentials*	*Partially – Further investigation for action templates is necessary* ***further legal analysis would be required regarding the role of the Agency – to be seen in the context of the IMI regulation.***

ID	Legal ref.		Explanation (if required)	Can this action pre-defined (structured)	Could IMI provide a support?
1.4	Dir. 2007/59/EC Article 22.1(b) +	*b) supply, upon reasoned request, information on the status of* *such licences to* ***… or any employer of drivers.***		*Idem to 1.3 A clear role definition should be noted in order to avoid miscommunicating information to users that may not have access to it.*	*Idem to 1.3* *IMI is only for authorities – RU/IMs and other types of employers will be accepted as users of IMI after IMI's customization on the system* ***Potential development of the IMI public interface could allow employers to request information from NSAs. However such development would need to be further analysed.***

	EC Decision 2010/17/EU Annex I.4 EC Decision 2010/17/EU Annex I.4	*Access to the information contained in the NLR shall be granted to the following interested parties for the following purposes:* ***To any employer of drivers**, for consulting the status of the licence in accordance with article 22(1)(b) of Directive 2007/59/EC,* Access to the information contained in the NLR shall be granted to the following interested parties for the following purposes: **to railway undertakings and infrastructure managers, employing or contracting train drivers, for consulting the status of licences**, in accordance with Article 22(1)(b) of Directive 2007/59/EC,	*The decision to split in two employers of drivers and RUs/IMs (that can be also employers, of course) is motivated by the possibility that a train driver is employed by an entity that is not an RU/IM (e.g.: company leasing the drivers to RUs/IMs).*	*Security considerations may arise during this process. More connections equal more potential security threats.*	

1.5	Dir. 2007/59/EC Article 22.3	**Train drivers shall have access** to the data concerning them that is stored in the registers of competent authorities and of railway undertakings, and shall be provided with a copy of that data on request.		*Train drivers can access the solution by introducing their user credential and the solution will provide them only their own information. Type of information that may be available can be standardized and solution may respond to that*	*NO – In the case that data will be stored in NSA level* *YES – If data is stored at IMI's level* ***Potential development of the IMI public interface could allow employers to request information from NSAs. However such development would need to be further analysed.***

	EC Decision 2010/17/EU Annex I.4	*Access to information contained in the NLR shall be granted to the following interested parties for the following purposes:* ***to train drivers****, upon request, for consulting the data concerning them.*		*Requests may be identified and drafted with pre-defined selections. In case of non satisfactory reasons, train drivers should submit a request that will be evaluated by the CA and returned with an adequate explanation. Train drivers must always be granted full access to registrations/data concerning themselves. Authorities have no right to limit the access.*	*YES – In terms of messaging. IMI is strong in messaging among stakeholder members*
1.6	EC Decision 2010/17/EU Annex I.4	*Access to information contained in the NLR shall be granted to the following interested parties for the following purposes:* ***to investigation bodies*** *set up in accordance with Article 21 of Directive 2004/49/EC, for investigating accidents, in particular as stated in Article 20(2)(e) and (g) of that Directive;*		*An extra user access type should be defined. It is advisable that these bodies are well identified and introduced to the solution. Additionally the level of interaction should be also identified and specifically till which point without any authorisation by the NSAs' they could retrieve data The probality of*	*YES – In requesting* *NO – In data collection* ***Partially – If Investigation bodies act as competent authorities through IMI they could request access to the national registers, or ask for information contained in them. However the access to such registers would have to be managed individually***

				investigation bodies requesting data from a NLR in another MS seems very low. Defining such an access would not match the effort/costs due to increased complexity. If an investigation body from MS1 needs info from the NLR in MS2, the request should be handled by the NSA in MS1.	***outside IMI.***

ID	Legal ref.		Explanation (if required)	Can this action pre-defined (structured)	Could IMI provide a support?
1.7	**EC Decision 2010/17/EU Annex I.5**	**5. Data exchange** Access to relevant data shall be granted upon **formal request**. The competent authority shall provide the data, **without delay**, in a manner which ensures secure transmission of information and protection of personal data. Competent authorities may offer login facilities on their websites to all who have access rights, provided they ensure that the grounds for requests are checked.	**formal request:** *Every time a NSA requests an information, there must be a formalised request (whatever is the used medium, this is valid for all the request). The reason is that each request should be documented and traceable, to ensure that response is provided and also for monitoring purposes.* **without delay***: The statement is that the requested information is provided by the responding NSa(s) without delay: this does not mean that the response has to be in real time. Each single case has to be evaluated to assess time criticality.*	*The justifications could be agreed and a catalogue of reasoned requests could be created.*	*The list of agreed reasoned (justified) requests is already foreseen in IMI* ***(Information request module)***

❶.2 Obligations concerning CCRs

ID	Legal ref.		Explanation (if required)	Can this action pre-defined (structured)	Could IMI provide a support?
2.1	EC Decision 2010/17/EU Annex II.5	5.Data exchange (…) The railway undertaking, infrastructure manager or delegated entity shall provide the data, without delay, in a manner which ensures secure transmission of information and protection of personal data. Railway undertakings and infrastructure managers may offer login facilities on their websites to all who have access rights, provided they ensure that grounds for requests are checked.		*The standardization of this aspect is absolutely necessary in order to avoid any conflict, time or any other kind of delays on data retrieval.* *A centralized / standard authentication process will solute on not having a number of information access points.* A centralized portal that would fetch information from a specific source and not various websites existing for example in each MS.	*Partially It has be guaranteed that while it is according to EC data protection directives it is in accordance to each MS legislation. Additionally Data handling should be also been into consideration and data storage, and specifically to which extend should information should be kept at IMI's servers* ***Potential development of the IMI public interface could allow employers to request information from NSAs. However such development would need to be further analysed.***

2.2	Dir. 2007/59/EC *Article 22.2(a)*	*2. Each railway undertaking and infrastructure manager shall be required to:* *(a)* ***keep a register, or ensure that a register is kept****, of all certificates issued, updated, renewed, amended, expired, suspended, withdrawn or reported lost, stolen or destroyed. This register shall contain the data prescribed in section 4 of Annex I for every certificate, as well as data relating to the periodic checks provided for in Article 16. It shall be regularly updated;*		*Since this is an obligation and records should be stored upfront with specific meta-data information, information exchange on any level will be easily performed. Solution should be ready to index and/or be able to query information holders*	*NO – information is stored in RU / IM level and IMI cannot index other servers or information holders*

2.3	Dir. 2007/59/EC *Article 22.2(b)* *+*	*(b) cooperate with the competent authority of the Member State where they are domiciled in order to exchange information with the competent authority and give it access to data required;*		*Standardized method will ensure high performance*	*YES* ***Potential development of the IMI public interface could allow employers to request information from NSAs. However such development would need to be further analysed.***
	EC Decision 2010/17/EU Annex II.4 +	4. Access rights Access to the information contained in the CCR shall be granted to the following interested parties for the following purposes: **to the competent authority** of the Member State in accordance with Article 22(2)(b) of Directive 2007/59/EC,		*Authentication and standardized reasoning of requests will verify the workflo*	*YES*
	EC Decision 2010/17/EU Annex II.5	5. Data exchange In accordance with Directive 2007/59/EC, access to relevant data shall be granted: (a) **to the competent authorities where the railway undertaking or infrastructure manager is domiciled**, in accordance with Article 22(2)(b) of Directive 2007/59/EC,		*In the case all prerequisites are met, a complete response will be provided automatically, unless extra investigation is necessary*	*NO – data exchanged in non centralized environment is not possible*

ID	Legal ref.		Explanation (if required)	Can this action pre-defined (structured)	Could IMI provide a support?
2.4	Dir. 2007/59/EC *Article 22.2(c)* *+*	*(c) supply information on the content of such certificates to **the competent authorities of the other Member States upon their request**, when this is required as a consequence of their transnational activities.*		*This is possible to be standardized though it will imply a common line among all MSs'. Theoretically it exists for being compliant to EC's directives. A by locale adaptation of the solution might be necessary.*	*YES with the condition that there is a standardized method for all MSs. See 2.1*
	EC Decision 2010/17/EU Annex II.4 (Access rights) +	*Access to the information contained in the CCR shall be granted to the following interested parties for the following purposes:* - ***to competent authorities of the Member States in which the railway undertaking or infrastructure manager operates**, and where the driver is authorised to drive on at least one line of the network:* – *for their task of monitoring the development of certification, under Article 19(1)(g) and Article 26 of Directive 2007/59/EC,* – *for their inspection tasks under Article 19(1)(h) and (2) and Article 29(1) of Directive 2007/59/EC (this task may be carried out by a delegated entity),*		*For both monitoring and inspection processes workflows can be set for informing their status, validity and alters*	
	EC Decision 2010/17/EU Annex II.5	*In accordance with Directive 2007/59/EC, access to relevant data shall be granted:* *(b) **to competent authorities of other Member States**, upon*		*Depending the authenticated type of user solution should*	*YES*

	(Data exchange)	*request, in accordance with Article 22.2(c) of Directive 2007/59/EC*		*respond promptly*	

2.5	Dir. 2007/59/EC *Article 2.3* *+* EC Decision 2010/17/EU Annex II.4 (Access rights) + EC Decision 2010/17/EU Annex II.5 (Data exchange)	**Train drivers shall have access** to the data concerning them which is stored in the registers of competent authorities and of railway undertakings, and shall be provided with a copy of that data on request. Access to the information contained in the CCR shall be granted to the following interested parties for the following purposes: **to train drivers**, for data concerning them, in accordance with Article 22(3) of Directive 2007/59/EC In accordance with Directive 2007/59/EC, access to relevant data shall be granted: (c) **to drivers**, upon request, in accordance with Article 22(3) of Directive 2007/59/EC.		*Idem 1.5*	*Idem 1.5*

2.6	EC Decision 2010/17/EU Annex II.4 (Access rights)	Access to the information contained in the CCR shall be granted to the following interested parties for the following purposes: **to investigation bodies** set up in accordance with Article 21 of Directive 2004/49/EC, for investigating accidents, in particular as stated in Article 20(e) and (g) of that Directive,		*With the condition that CA will be introduced in the system as also their level of access, it is possible to standardize this process*	*YES in messaging processes* ***The role of investigation bodies to be clarified furtner***

❶.3 Requirements concerning the controls by the competent authorities

ID	Legal reference	Legal requirement	Explanation (if required)	Can this action pre-defined (structured)	Could IMI provide a support?
3.1	**Dir. 2007/59/EC Article 29.1**	*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**.*	*Only possession is mentioned – not the validity of the documents*	*This will require prior standardization of access levels, information flow, types of information to be accessed, cases that information will be provided automatically or with a specific request*	*Partially – needs to be tested. Since no direct access to NLR is possible through IMI, IMI could only be used for post-inspection validation of the license/(certificate) validity. This should happen only if information is stored at IMI's level as well*
3.2	**Dir. 2007/59/EC Article 29.2**	*Notwithstanding verification as provided for in paragraph 1, in the event of negligence at the workplace the competent authority may **verify if the driver in question complies with the requirements set out in Article 13.***	*Not relevant for the TF. Driver negligence reported to/detected by a NSA implicates the following actions:* *1. Suspension (and reporting another NSA, if TDL is foreign)* *2. Suspension and actions to taken by NSA and employing RU/IM.* *It's not a question of verification of the license/certificate, but of the competences = different approach, and not within our scope.*	*This is a part of the general standardized workflow and dependant on all elements as in 3.1*	*YES*

3.3	**Dir. 2007/59/EC Article 29.3**	*The competent authority may carry out **enquiries regarding compliance with this Directive by drivers,** railway undertakings, infrastructure managers, examiners and training centres pursuing their activities in its area of jurisdiction.*		*It is necessary establishing a specific request / respond method*	*YES*

3.4	**Dir. 2007/59/EC Article 29.4 (a)**	*If the competent authority finds that a driver no longer satisfies* *one or more required conditions, it shall take the following* *measures:* *(a) if it concerns a **licence issued by the competent authority**, the competent authority shall suspend the licence. The suspension* *shall be temporary or permanent depending on the scale* *of the problems created for rail safety. **It shall immediately*** ***inform the driver concerned and his employer of its reasoned decision,** without prejudice to the right of review provided for in Article 21. It shall indicate the procedure to be followed for recovering the licence;*	*Seldom, and could be organised more dynamically without a specific it-solution.*	*Reports are a key point to the solution. An extract of the information workflow and involved parties. National legislation and EC's directives should be taken into account. These reports will be specified in the pilot phase*	*Adaptation is necessary* ***Potential use of the IMI Notification workflow (available Q2 2013***

3.5	**Dir. 2007/59/EC Article 29.4**	*(b) if it concerns a **licence issued by a competent authority in another Member State**, the competent authority shall*		*Since the interaction of more than one location is necessary, a centralized but also*	*Adaptation is necessary when sending out the notification to all other NSAs*

	(b)	*approach that authority and* ***provide a reasoned request*** ***either that a further inspection be carried out or that the*** ***licence be suspended. The requesting competent authority*** ***shall inform the Commission and the other competent*** ***authorities of its request.*** *The authority that issued the licence in question shall examine the request within four weeks and* ***notify the other authority of its decision****. The authority that issued the licence* ***shall also inform the Commission and the other competent authorities of the decision.*** *Any competent authority may prohibit train drivers from operating in its area of jurisdiction pending notification of the issuing authority's decision;*		*standardized verification on the reasoning should be implemented. All involved members, reasons and information type should be observed and recorded. Cases of high importance that will demand storing as well of information might exist.*	***Potential use of the IMI Notification workflow (available Q2 2013***
3.6	**Dir. 2007/59/EC Article 29.4 (c)**	*(c) if it concerns a certificate, the competent authority shall approach the issuing body and request either that a further* *inspection be carried out or that the certificate be suspended.* *The issuing body shall take appropriate measures and report* *back to the competent authority within a period of four* *weeks. The competent authority may prohibit train drivers*		*Idem 3.5* *Clarification on the type of information is always necessary to be noted*	*No; only authorities* ***IMI could support the communication between the authorities, the role of the issuing body would need to analysed further***

		from operating in its area of jurisdiction pending the report *of the issuing body, and shall inform the Commission and* *the other competent authorities thereof.*			
3.7	**Dir. 2007/59/EC Article 29.4**	*(….) At all events, if the competent authority considers that a particular driver creates a serious threat to the safety of the railways, it shall immediately take the necessary action, such as asking the infrastructure manager to stop the train and prohibiting the driver from operating in its area of jurisdiction for as long as necessary.* ***It shall inform the Commission and the other competent authorities*** *of any such decision.*		*Incident report system will resolve these situations, registering all related information and involved members. This could be an automatic process*	*YES* ***Potential use of the IMI Notification workflow (available Q2 2013***

❶.4 Obligations concerning interoperability of NLRs/CCRs

ID	Legal reference	Legal requirement	Explanation (if required)	Can this action pre-defined (structured)	Could IMI provide a support?
4.1	Dir. 2007/59/EC *Article 2.4*	The competent authorities shall cooperate with the Agency in order to ensure the **interoperability** of the registers provided for in paragraphs 1 and 2.	*This is the general obligation/requirement for the MS, and cannot be specified at this level*		*Not necessary – Communication could be successful with simplified methods*

4.2	EC Decision 2010/17/EU Article 3	*Within 24 months from the taking effect of this Decision, the European Railway Agency (hereinafter 'the Agency') shall carry out a feasibility study for a* ***computer-based application fulfilling the basic parameters for the NLR and CCR and facilitating the exchange of information among competent authorities, railway undertakings and infrastructure managers.***		*Specific timeframe should be drafted in order to accomplish this target. This should be also communicated to all stakeholders.*	-

20 Annex 6: Questionnaire on interoperability of NLRs/CCRs

- **File attached -**

21 Annex 7: Survey to NSAs on Interoperability of NLRs – CCRs (FEB 2012)

ERA circulated a questionnaire to NSA's the 3rd of February, 2012 (Annex 3). On February 7th ERA has collected 21 results

Respondents: UK, NO, DE, BE, NL, FI, DK, AT, SE, LV, IT, FR, LT, RO, EE, CZ, BG, PL, SK, HU, IE

Questions on the current state of your NLR	Average %
3. Does your NSA have a standardized method for registering train driving licenses according to Decision 2010/17/EU (either electronic or paper-based)?	**100%**
4. Is this an **electronic system**	**85.71%**
a. **YES**:	
i. Is it accessible via browser	**64.29%**
ii. Is it able to exchange information	**60.00%**
b. **NO**: In a scale from 0 to 5, how would you evaluate its importance? (0 = not important at all, 5 = very important)	
5. Does the method you currently apply assist interoperability with other stakeholders (including NSAs, RUs, IMs, etc.)? Why not? How?	**30.00%**
6. Is the method you currently apply securing validity of information?	**83.33%**
7. How many incoming transactions would you estimate to happen per year from other NSAs?	**< 50**
8. How many outgoing transactions addressed to other NSAs would you estimate to happen per year?	**< 50**
9. How many incoming transactions would you estimate to happen per year from other RUs/IMs?	**< 200**
10. How many outgoing transactions addressed to other RUs/IMs would you estimate to happen per year?	**< 200**
11. What is the maximum time span you would allow between sending a request and receiving an answer?	**2 weeks**
12. What is the maximum time span you would allow between receiving a request and providing an answer?	**2 weeks**

Of the twenty country responses, most of all stated that their respective NSA has a standardised method for registering train driving licenses according to Decision 2010/17/EU, while some (10%) are in process of developing such method. For 85% of them this is an electronic system that is accessible via browser and/or able to exchange information for two thirds of them. However, the majority (70%) of NSAs answered that their current method does not assist interoperability with other stakeholders whilst most national methods apply securing validity of the information (83%). The range of incoming and outgoing transactions to/from other NSA's varies widely amongst countries with an average of 200 transactions per year. The same is true

for transactions from and to RUs/IMs ranging between 5 and 2,000, and again an average of 200. The maximum time span for receiving/giving an answer ranges between 0 days and 1 month, probably depending on the type of request, with a medium of 2 weeks.

Interestingly, most respondents chose to indicate the same number of incoming and outgoing transactions for NSAs and RUs/IMs. In sum, as incoming and outgoing would have to add up, the questionnaire results seem strange unless there are pairs of countries who typically communicate with each other. Possibly, these results indicate the importance of perception affecting issues in this feasibility study in general.

Also, when indicating the time span for receiving and giving answers is consistent for each country (the expectations for receiving and giving are the same) apart from The Netherlands whose NSA would only wait 1 week for a response but allows itself up to 8 weeks to send responses as per their national legislation status. Yet, the expectations vary widely amongst countries from as little as one day in Finland to up to one month in Germany, Latvia and France (except The Netherlands for sending responses). This could also mean that the NL respondent read Q9 as min and Q10 as max.

From your point of view as an NSA, on a scale from 0 to 5, please rate the importance of the following interoperability measures concerning registers:	Average
11. Adoption of harmonized processes and of a common policy throughout the EU (fits with overall interoperable and harmonized framework for railway sector and promote removal of barriers)	**3**
12. The design of the system involving all actors so that the output reflects all needs (NSAs, RUs, IMs, NIBs, drivers)	**3**
13. The interoperability supports the monitoring of the system (through functions including reports, statistics, frequencies, etc.)	**2**
14. The system undergoes maintenance and periodical reviews to implement corrective action(s), if necessary.	**3**
15. A possibility to include new functions based on emerging demands of the sectors.	**3**
16. The security of transactions based on roles and access rights.	**4**
17. It contains automatic checks for duplicate information (to facilitate detection of abuses) in all databases and relevant notification to the identified stakeholders.	**4**
18. Automatic notifications in case that pending expiration dates are identified by the system.	**4**

It is obvious that most NSAs are increasing the level of compliance in terms of interoperability according to EU's decision. It is important to highlight the fact that there is a concern in terms of security as also duplication of information while there has to be a raise on applications related

to awareness factors, which should be taken into consideration during the potential design and implementation of the system.

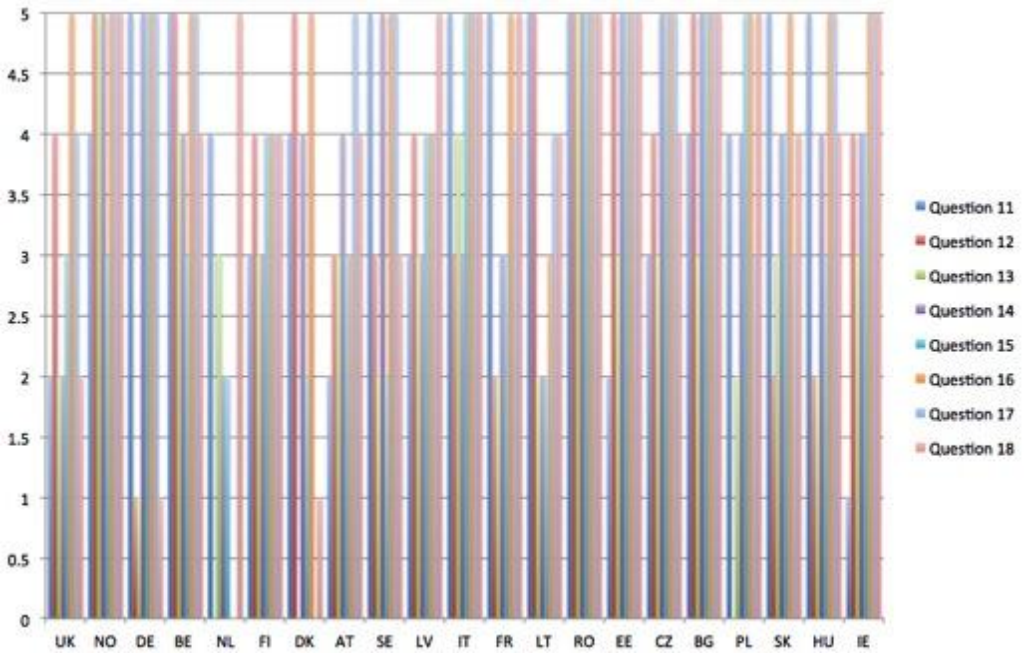


Figure 3: Results on Questions 11 – 18

On a scale from 0-5, please rate the importance of the following system's concepts concerning the interoperability of registers	Average
19. Availability of a common framework (based on Decision 2010/17/EU) or possibility to connect with existing registers through a system	**4**
20. Quick response to needs	
a. Exchange of information in real time amongst NSAs	**3**
b. Exchange of information in real time between NSAs and RUs/IMs when employing or contracting drivers	**3**
21. Improved quality of communication:	
a. Standardized language in order to facilitate easy understanding	**3**
b. Automatic translation in order to overcome language barriers	**2**
22. Automated acceptance of requests	
a. Adoption of approved catalogue of reasoned requests	**3**
b. Possibility to include unidentified reasons (first using an open field, then with advanced criteria)	**2**
23. Controlled access to information according to rights	**4**
24. Freedom for NSAs to include other actors by creating a login for them (or requesting login information from ERA)	**2**

25. Alert of duplicate information in one database to send relevant notification to identified stakeholders	**3**
26. Automatic notifications in case of expiry dates	**3**

We can observe that the communication between NSAs as also an NSA and its regionally dependent RUs and IMs, is not adequately rapid. Additionally at this stage a standardised method in terms of communication is not yet established, which may bring more accurate and faster communication results. Special caution should be taken to access rights and to the roles that actors may have in the system. Since personal information is dealt security should be handled with high standards.

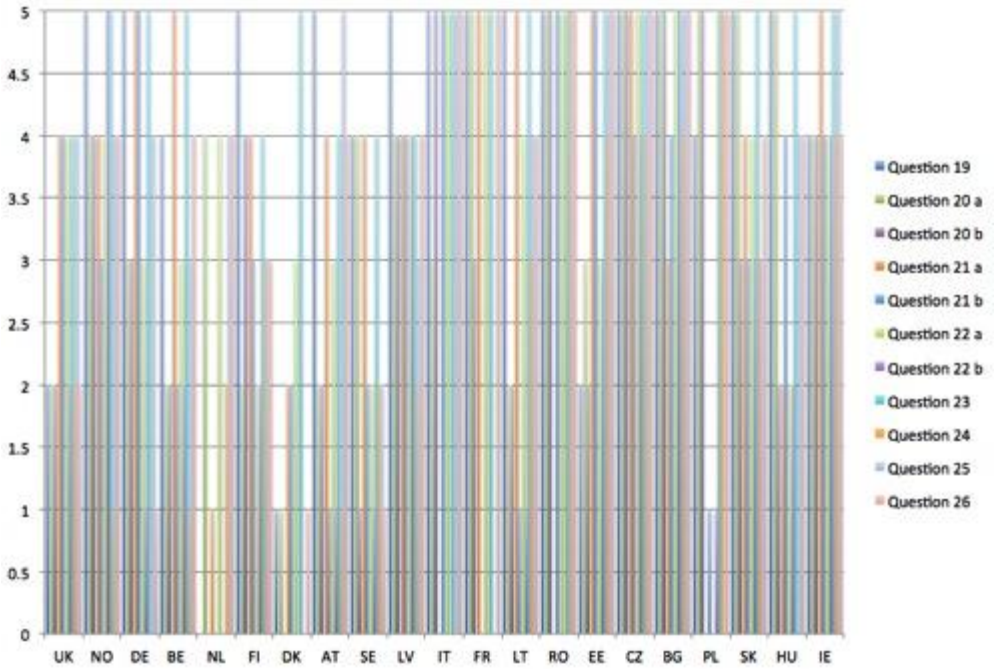


Figure 4: Results on Questions 19 – 26

21.1 Survey on Interoperability of NLRs – CCRs results

According to the Survey on Interoperability of NLRs – CCRs, conducted by ERA[22] in February - March 2012 and addressed to all NSAs, with 90% of respondents coming from the 25 NSAs (plus Norway), the following conclusions can be made (full results in Annex 3 – Document attached):

Question	Answer	Result
6	Has the Directive 2007/29/EC been transposed in your National legal framework?	**Yes 82%**
7	Please provide the date of entry into force of the National provisions for the transposition of the Directive 2007/59/EC	**All after mid-2011**
12	Could the similarities of the IT application for interconnecting the registers with the Virtual Vehicle Register (ECCVR) be of help for your NSA?	**Yes 86%**
13	Should ERA have a role of general coordination and maintenance of the IT application for inter-connecting the registers, after the (eventual) approval of the feasibility study?	**Yes 80%**
14	Please mark the case indicating the importance for your NSA of the following characteristics of the IT application for interconnecting the registers.	**Ease of use 55%** **Adaptability 70%** **Internet based 60%** **Login to NSAs/RUs 45%**

These requirements do not assure the technical interoperability of registers. Therefore, in order to meet the EC Decision 2007 Article 3, a feasibility study has to be carried out.

[22] http://extranet.era.europa.eu/Interop/NSAexp_art35/Lists/Survey%20on%20Interoperability%20of%20NLRs%20%20CCRs/overview.aspx

22 Annex 8: Business models supporting interoperable information exchange

After considering suggestions of approach and the necessities, there is a strong emphasis on establishing a technological solution using a system that will be able to serve as specified. For the implementation of the NLR-CCR project, three main ways have been identified:

22.1 Model I

1. ERA will be the central point for collecting information:

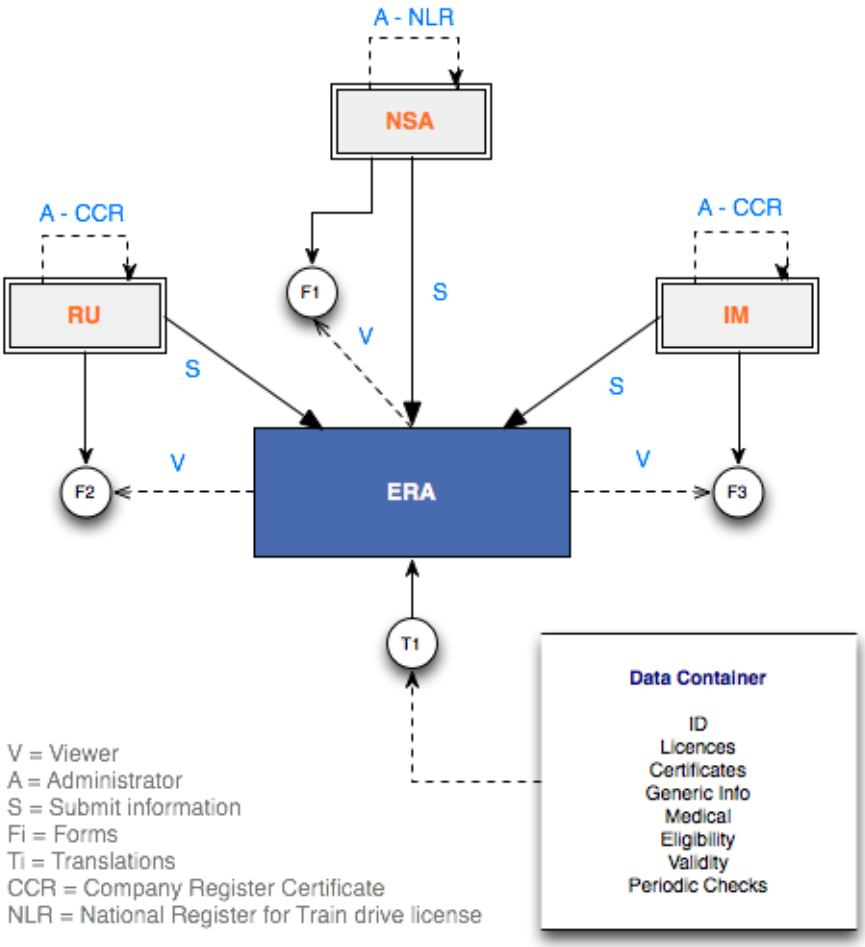


Figure 8: Model I

Model I proposes a centralized solution where ERA will collect all data information in a data pool, and will distribute them according to specific user privileges.

The system will be hosted in ERA's server cloud, and therefore be compatible with all EC regulation concerning data protection, personal information, high access levels as well as

network security, high performance on availability, respecting accessibility standards, respecting access rights and high data storage and back-up capacity.

Involved actors (apart from ERA) will be in the position to enter and retrieve all relevant information to and from the system according to the already defined access rights by the EC decision. Specific procedures will be in force to request the access to information.

It is important to point out that there will be specific standardized interfaces / bridges that will be responsible for the **data import and data collection** from all authorities. Those will be developed and executed for the initial import, but would also be set to proceed with comparing and updating data and information periodically (recommended once per day). Historic information of all such transactions (information, introduction and updates) should be recorded.

Information Items:

- Creators C_m able to input / manage information – NSA_{25} / RUs / IMs
- Delegator ERA responsible for delegating information
- Forms F_I forms that stakeholders will to submit in order to retrieve info
- Submit S_I forms in order to store information in the server
- Information I_I information stored ERA – needs local server
- Viewer V_n Involved actors will be able to view information

22.2 Model II – Hybrid

2. ERA will be the central point for disseminating information:

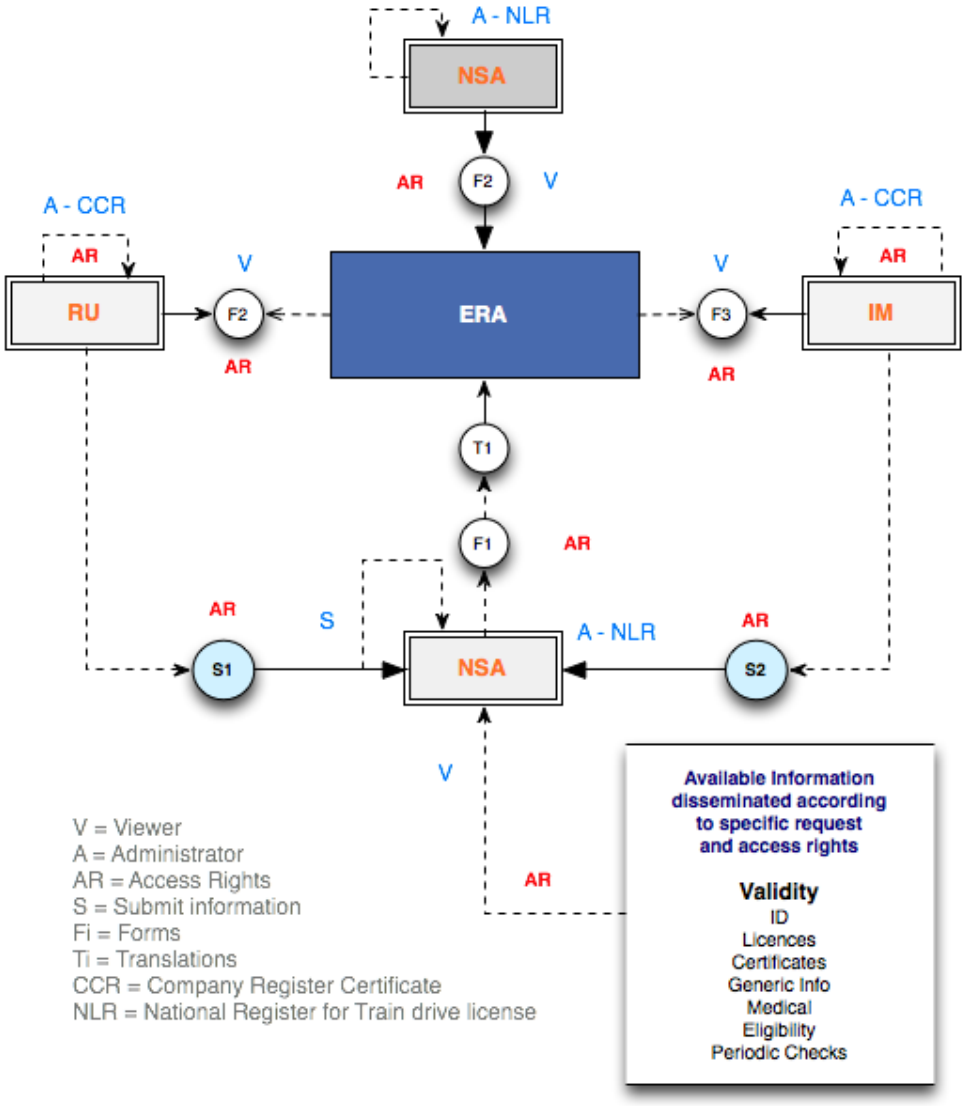


Figure 9: Model II Hybrid

Model II Hybrid represents a hybrid solution where each NSA will be deliverer of the incoming requests and the outgoing information concerning the national catchment area. Per case the NSAs will decide the distribution according to specific data-locations. Users' privileges and adequate reasons of the request arise from the roles, given by the ERA to each questioner. Additionally there will be no further need for RUs or IMs to have a computer-based data-base by developing communication Bridges or providing tools for adequate and interoperable communication. All transactions and access rights will be provided by ERA. This model signifies the need of increasing data and network security for each key point and its importance should be given to the system's availability and response time.

The following points for this model are of most importance:

- The system will be served as web-based platform;
- Specific access rights and users groups / roles will be secured for accurate information handling and access. For this process ERA will be the responsible authority;
- All information requests are handled via the ERA: (a) managing responsibly the roles for the information requests (b) arranging the information requests of questioners to the NSAs.
- Automatic triggers will be developed for disseminating responses of immediately high-importance or curtail information. Those will respect all access rights plus will be reasoned specifically;
- RUs and IMs may directly use the system provided by the NSA they belong to and will have direct access rights only to specific information owned and submitted by themselves;
- In the case that an RU or IM would have their own system, then they will be bridged to the NSA that they belong in terms of their region;
- In the case that an NSA will already have a system, a bridge between ERA and NSA will be implemented to assist and monitor the queries;
- In the case that RUs or IMs may not be able to have access to an advanced system, the web-based platform will provide them all the necessary means to provide information or respond to queries, such as built-in-email to their NSA or the rest of the stakeholders, with messaging and uploading of documents possibilities. Replies may be accessed by the system as also will be sent to their already registered email address. That process may also succeed with PDF online. Method with most advantages will be accurately determined in the pilot phase;
- In the case that RUs / IMs wish to have their data in such a system hosted by NSAs, the respective NSAs according to their decision, may grant them access to it. In the opposite scenario, RUs / IMs, their information will be held or easily transformed in electronic format, and will be under a specific standard in order to secure interoperability and ease of dissemination. Therefore, it will be provided the possibility to allow the RUs / IMs to choose the location of keeping their own data (NSA Level/Their Own System) and also allow them to simply exchange the information with the NSA without storing Data in the NSA server in a standardized way. The NSAs are able to decide, whether they store in addition to the NLR the data of the CCRs of the national RUs and IMs in their system, too – or not;
- There will be no specific data container but a harmonization process should be followed in order to develop the specific bridges for the queries handling.

ERA will host a system in its servers which will serve the handling queries arriving from NSAs / RUs / IMs and provide an information path to the NSA that keeps the record respecting all access rights and allow reports for statistical purposes. No information will be kept at ERA servers and no direct access will ERA have to any other stakeholder unless written authorization.

Information Items

- Creator NSA_{25} able to manage information and attached documents
- Information I_I information stored at NSAs – need of local server & client
- Delegator ERA responsible for delegating information
- Forms F_I forms that stakeholders will to submit in order to retrieve info
- Submit S_I forms in order to store information in the server
- Viewer V_n all will be able to view information

22.3 Model III

3. Each of the NSA's / RU's / IM's will be a concrete point for collecting information:

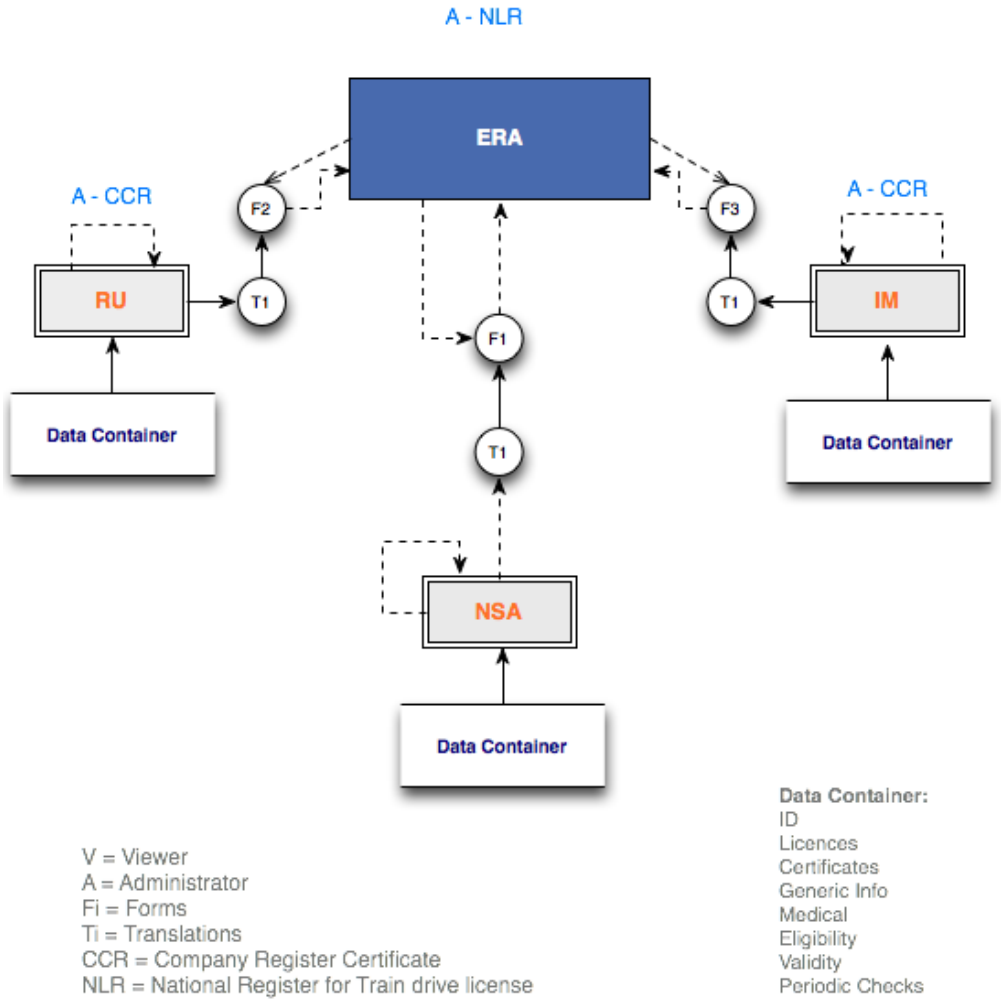


Figure 10: Model III

Model III is a decentralized solution where all information is kept by the different national actors and shared through a system with all other actors with access according to specific user privileges.

It is obvious that, in this model, a lot of attention should be considered to network security and data protection issues, since all information will not be hosted in a specific but a sum of specific servers. As in Model II, ERA will be hosting the system's interface to connect with all involved parties per request, and provide them with the path on finding the specific information.

Information Items

- Creator NSA_{25} able to manage information and attached documents
- Creator RU_m able to manage information and attached documents
- Creator IM_k able to manage information and attached documents
- Information I_l information stored local – need of local server & client

- Delegator ERA responsible for delegating information
- Viewer V_n all will be able to view information

22.4 Methods' key concept

All above-mentioned methods follow the principle of:

High performance vs. low cost

This means that the initial investment and the additional cost specific to all NSAs, RUs and IMs should be kept at a minimum. For that, the solution should be:

- Having established standardized methods for information flows;
- Accessed by commonly spread web browsers;
- Free from client installation necessity;
- Easy to use without any specialised IT-knowledge as a prerequisite for information input, retrieval and request;
- Having simple and concise processes concerning the Information request forms;
- Notifying users properly according to access rights and events of the information flow;
- Easy to use when accepting or refusing requests.

23 Annex 9: Business model with secure information exchange

Having as an accepted working model by the EC, IMI, as stated above is a IMI is a multilingual IT tool for exchange of information between Competent Authorities throughout the European Economic Area. The system is developed by the European Commission in partnership with EU Member States and it facilitates communication between public administrations at national, regional and local level.

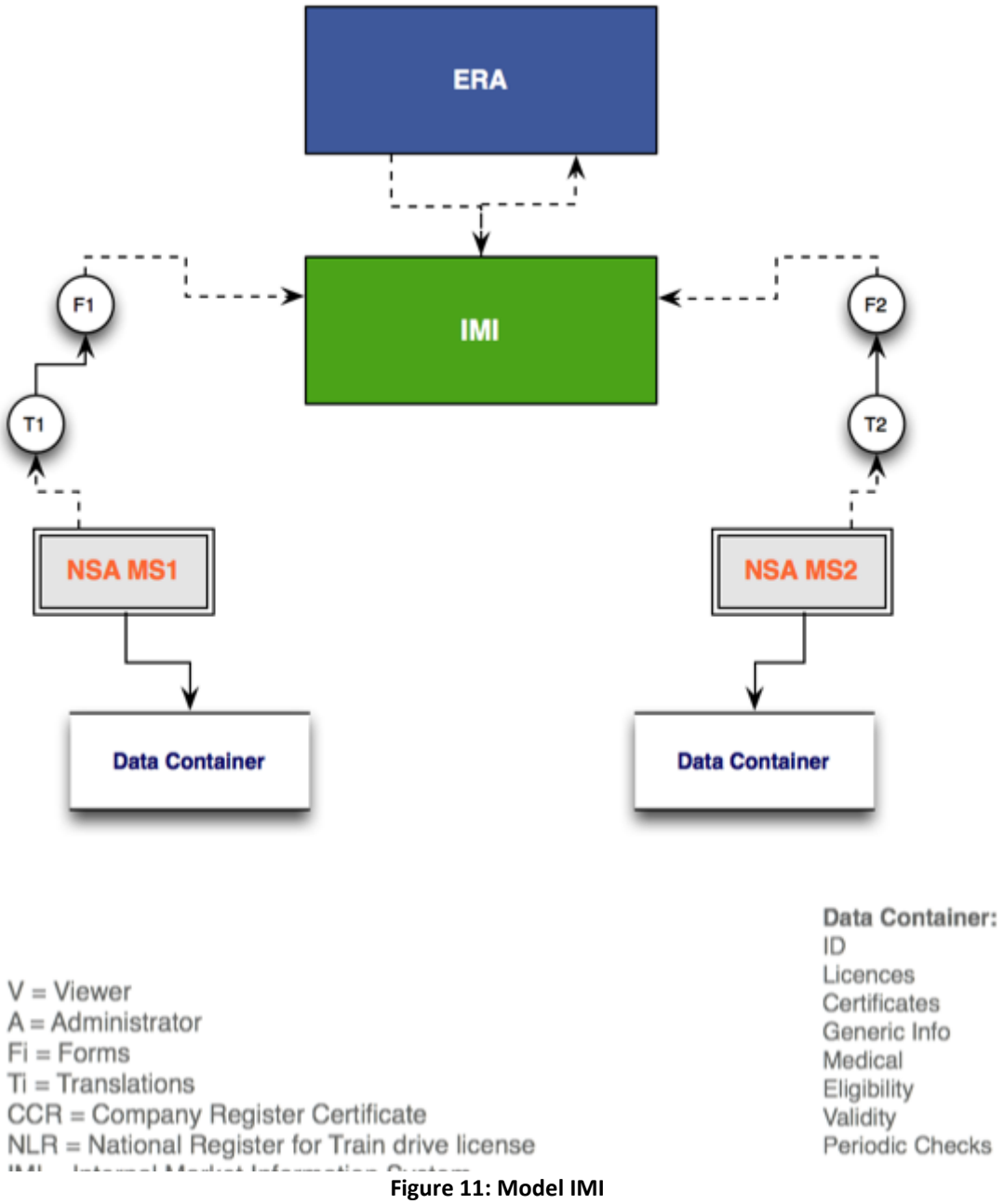


Figure 11: Model IMI

In the specific model NSA from MS1 requests information from NSA MS2. Matching process succeeds via IMI and ERA is informed of the process. Data transaction may succeed from NSA MS1 to NSA MS2 directly without any interval.

With this basis we can assume that IMI will:

- Reassure information exchange among designated stakeholders in short period of time after original request;
- By using IMI there will be the opportunity to monitor the type and number of transactions that will succeed in a specific time range;
- ERA will be able to have access to reports and be informed of the types of the transactions but not to any personal information. For example, ERA will be informed that NSA from MS1 did a query to NSA MS2 for a specific type of request;
- The Railway Sector will be able to use the system without any disruptions and access specific information during their complete life-cycle (from about seven to ten years);
- Consequent a complete interoperable system solution that will be implemented based on the results of using IMI's product. Outcomes could be made after five years in order to assist taking a decision.

Important Notes:

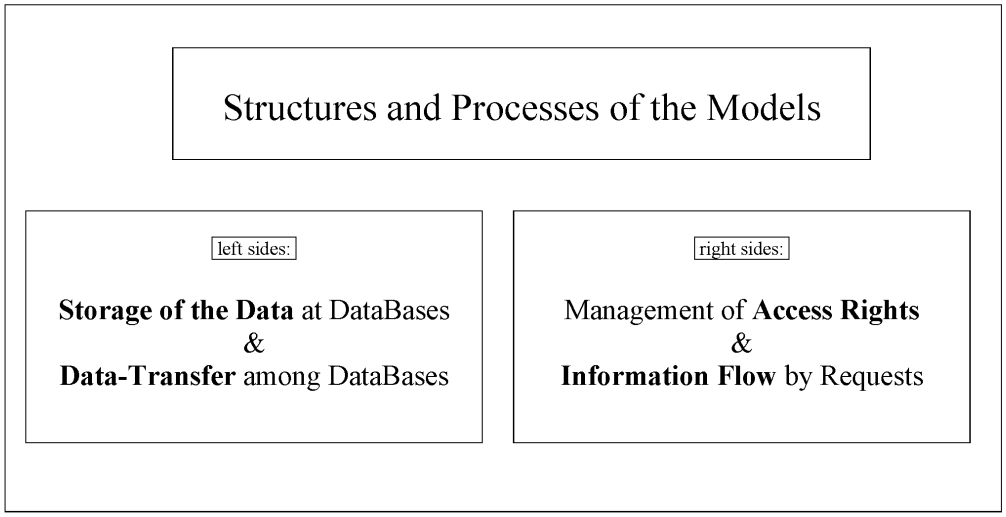
1. It is necessary to evaluate the data exchange process. Although IMI and ERA are respecting data security and personal information according to the directives given by the EC, it might be necessary according to national or regional legislation that data should not be stored in any other intermediate authority, therefore they should be transmitted to the requested authority without as attachments or reference to a secure link or FTP but not storing them in either IMI's or ERA's servers. This is a matter of further investigation.
2. There has to be an additional investigation on how the specific model could guarantee interoperability especially by storing data only in the original source and the requesting authority.
3. In relation to the last point the "time critical" events should be also been treated in a way that the interacting authorities will be able to react and provide immediately results. While IMI will be matching and sending immediately the request, the data transfer might be lengthy as a process.
4. Most operations will succeed via standard forms and in the language of each stakeholder. This will enhance but also reassure the level of interoperability of the solution. Those forms will allow the auto-filing of general information of each NSA but also the issuer of the request.
5. In addition, the forms, may also have standard questions that will be checked by issuer in order to secure the reasoned requests and combine it with the legal basis and the time criticality of the event. Additionally there has to be also the opportunity to add free text for further explanation if necessary.
6. For the case adding sub-system to assist the communication with RUs and IMs, IMI responded positively for a specific customization to secure this. NSAs will not be necessary accessing a different environment, but would be informed automatically of a

request. Depending the legal basis, RUs / IMs may use the NSA of the MS that they belong and that will extend the request to the appropriate NSA of another MS or directly post the request to the NSA of the MS that keeps the record of the driver.

7. There will be no installation of third party software and there will be no need but conventional methods of Internet browsing and access. Therefore, the system will stand as independent solution for information exchange.
8. Concerning the data exchange there could be a solution based on meta-data and use of XML combined with IMI's system, but needs to be double-checked with IMI.

24 Annex 10: Process oriented model IV

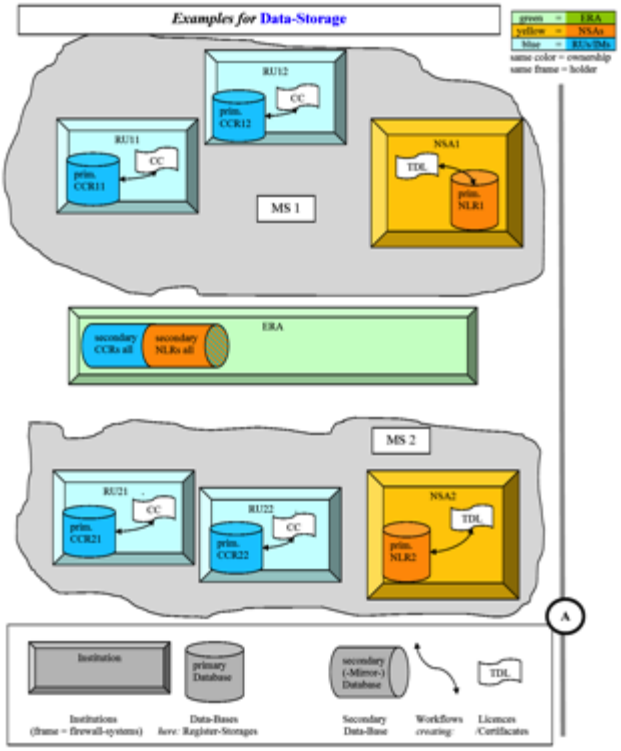
Model IV is a process-oriented model, combining structures of the models I and II. Therefore in the following the structures and processes of the previous models I, II and III are sketched first, to develop in a second step the work-flows in model IV adjusted for discussed use-cases.

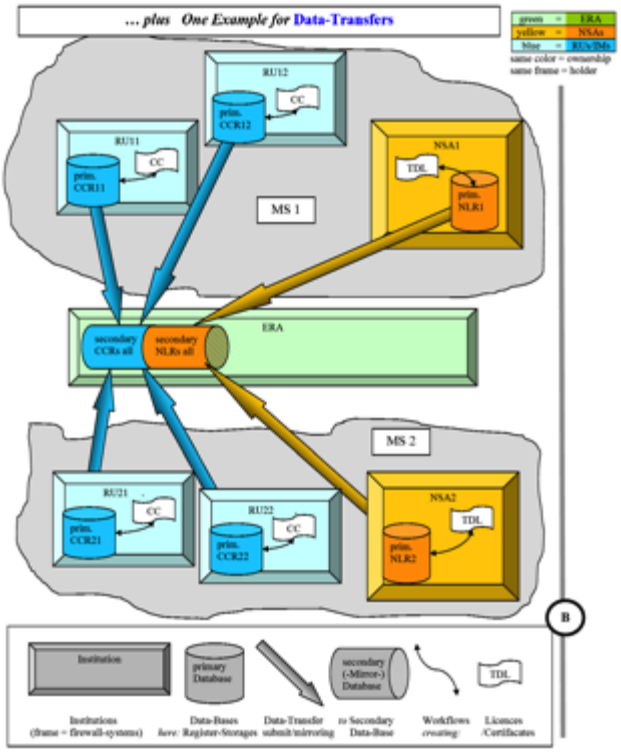


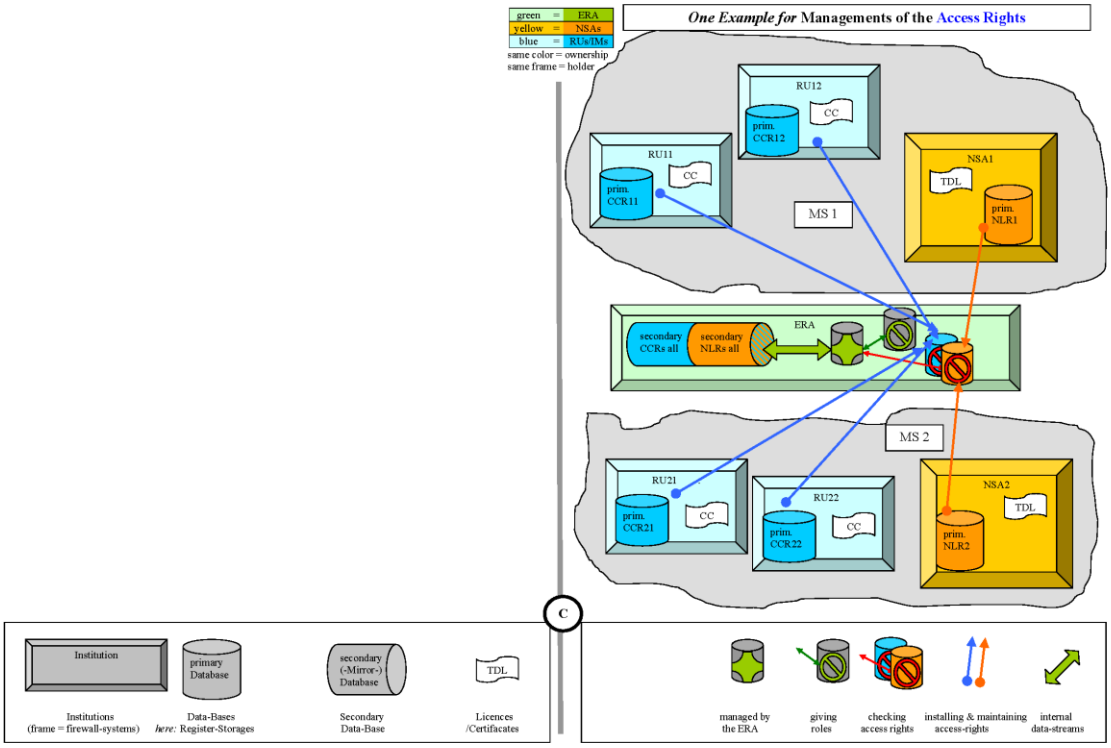
The following pages show all models, differentiated according to their structures (left sides) and processes (right sides):

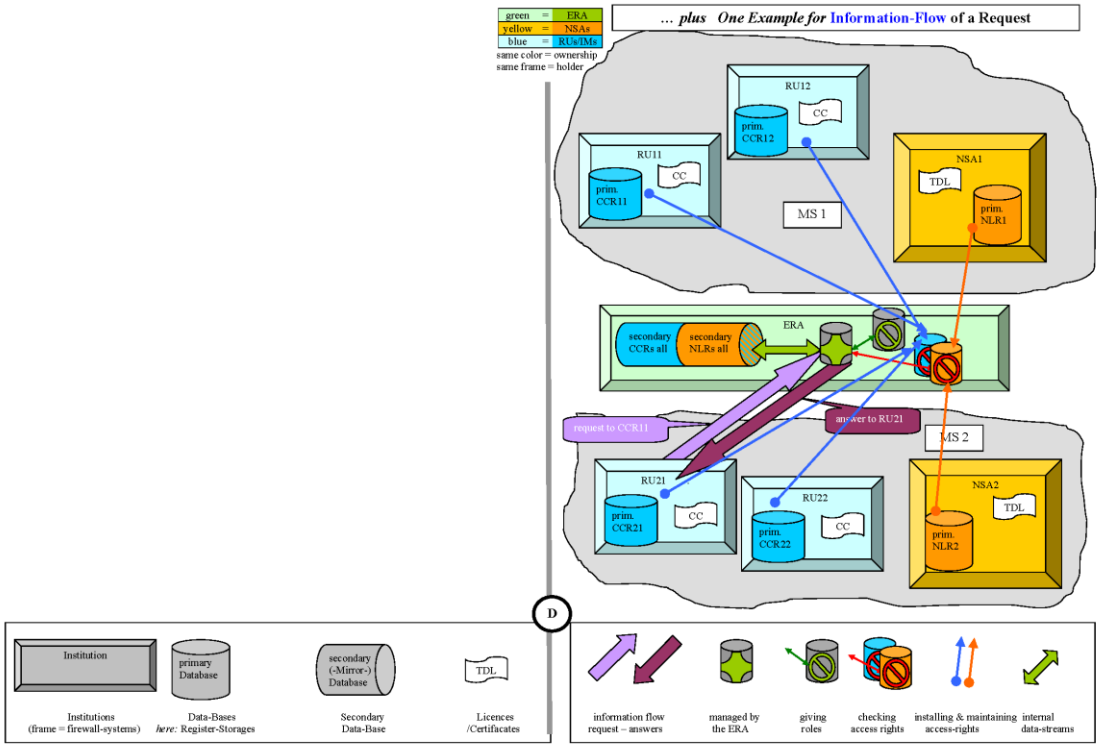
a. explaining the four considered aspects: data-storage, data-transfer, management of access-rights, information-flow;
b. for the Models I, II Hybrid and III
c. supplemented by the process-orientated Model IV, combining structures of the model I and model II. Two variations are discussed here: with or without a small central core-database.

Note: In the following illustrations the symbol of “RU” stands for RUs and IMs.


Examples for Data-Storage
green = ERA
yellow = NSAs
blue = RUs/IMs
same color = ownership
same frame = holder
RU12
CC
prim. CCR12
RU11
CC
prim. CCR11
MS 1
NSA1
TDL
prim. NLR1
ERA
secondary CCRs all
secondary NLRs all
MS 2
RU21
CC
prim. CCR21
RU22
CC
prim. CCR22
NSA2
TDL
prim. NLR2
A
Institution
primary Database
secondary (-Mirror-) Database
TDL
Institutions (frame = firewall-systems)
Data-Bases here: Register-Storages
Secondary Data-Base
Workflows creating:
Licences /Certificates

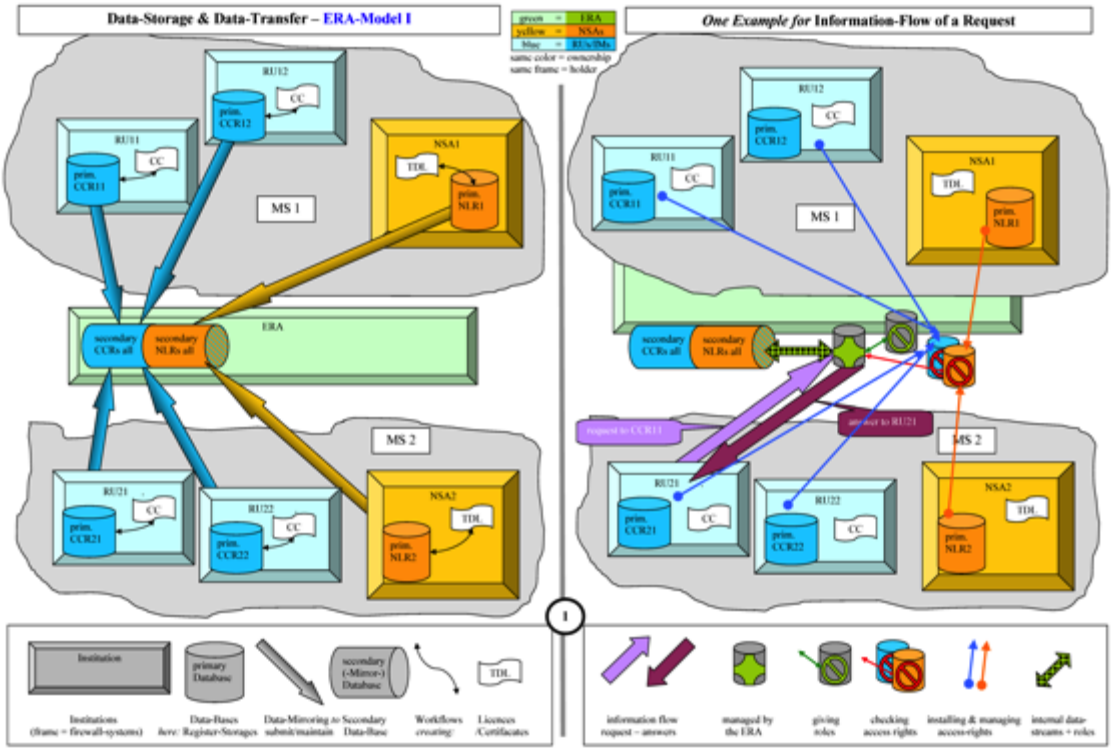

... plus One Example for Data-Transfers
green = ERA
yellow = NSAs
blue = RUs/IMs
same color = ownership
same frame = holder
RU12
CC
prim. CCR12
RU11
CC
prim. CCR11
MS 1
NSA1
TDL
prim. NLR1
ERA
secondary CCRs all
secondary NLRs all
MS 2
RU21
CC
prim. CCR21
RU22
CC
prim. CCR22
NSA2
TDL
prim. NLR2
B
Institution
primary Database
secondary (-Mirror-) Database
TDL
Institutions (frame = firewall-systems)
Data-Bases here: Register-Storages
Data-Transfer submit/mirroring
to Secondary Data-Base
Workflows creating:
Licences /Certificates

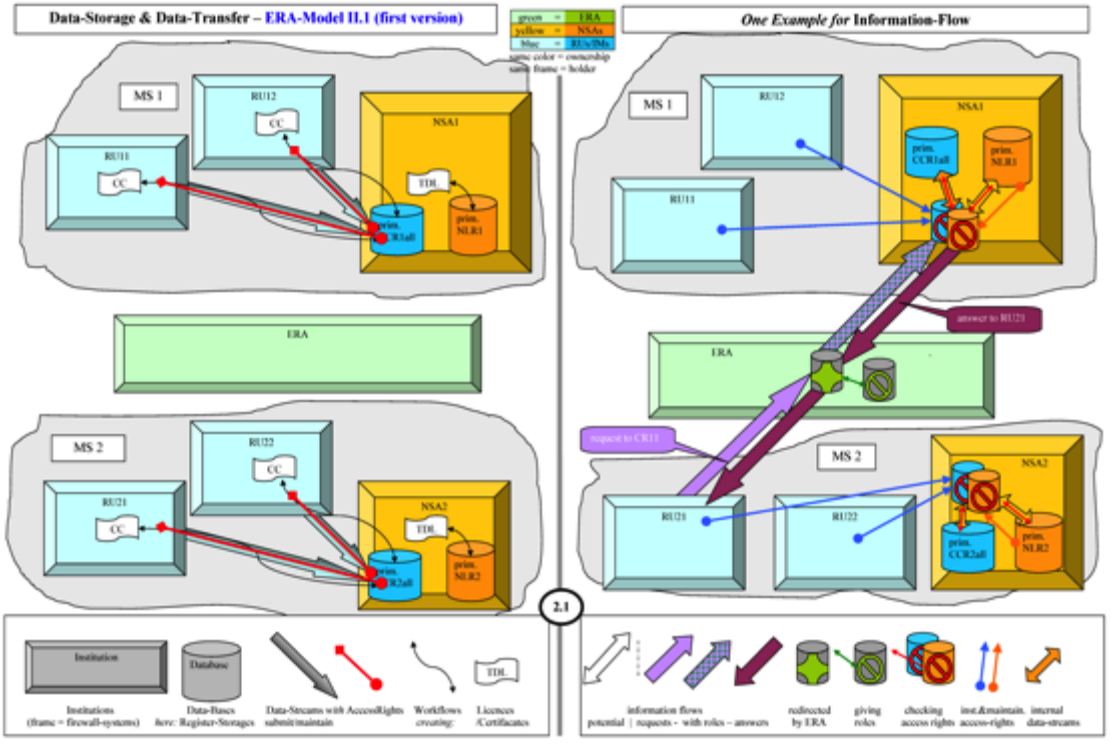

green = ERA
yellow = NSAs
blue = RUs/IMs
same color = ownership
same frame = holder
One Example for Managements of the Access Rights
RU12
CC
prim. CCR12
RU11
CC
prim. CCR11
NSA1
TDL
prim. NLR1
MS 1
secondary CCRs all
secondary NLRs all
ERA
MS 2
RU21
CC
prim. CCR21
RU22
CC
prim. CCR22
NSA2
TDL
prim. NLR2
C
Institution
primary Database
secondary (-Mirror-) Database
TDL
Institutions (frame = firewall-systems)
Data-Bases here: Register-Storages
Secondary Data-Base
Licences /Certifacates
managed by the ERA
giving roles
checking access rights
installing & maintaining access-rights
internal data-streams

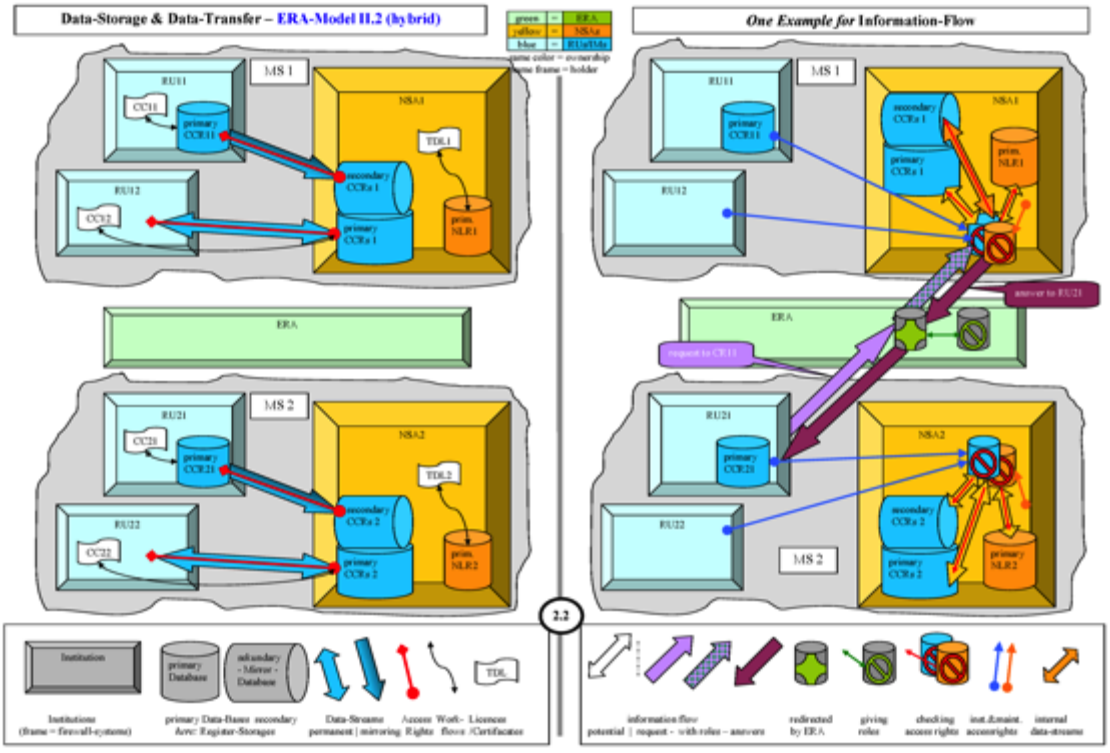

green = ERA
yellow = NSAs
blue = RUs/IMs
same color = ownership
same frame = holder
... plus One Example for Information-Flow of a Request
RU12
CC
prim. CCR12
RU11
CC
prim. CCR11
NSA1
TDL
prim. NLR1
MS 1
secondary CCRs all
secondary NLRs all
ERA
request to CCR11
answer to RU21
MS 2
RU21
CC
prim. CCR21
RU22
CC
prim. CCR22
NSA2
TDL
prim. NLR2
D
Institution
primary Database
secondary (-Mirror-) Database
TDL
Institutions (frame = firewall-systems)
Data-Bases here: Register-Storages
Secondary Data-Base
Licences /Certifacates
information flow request – answers
managed by the ERA
giving roles
checking access rights
installing & maintaining access-rights
internal data-streams

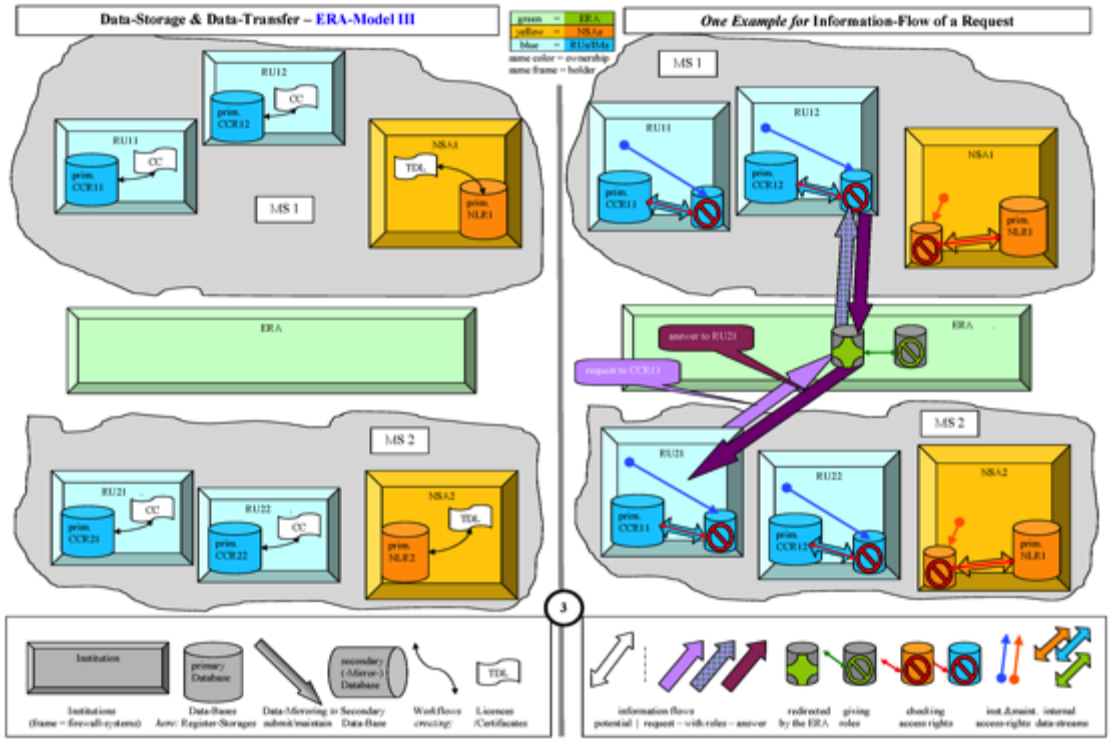
Models I, II, III

Model I.	**ERA** as central point for **collecting** information
Model II.1	**NSAs** as central points for **collecting** information
Model II.2/Hybrid	**ERA** as central point for **disseminating** information
Model III.	**Each NSA/RU/IM** as concrete point for **collecting** information


Data-Storage & Data-Transfer – ERA-Model I
One Example for Information-Flow of a Request
MS 1
MS 2
ERA
NSA1
NSA2
RU11
RU12
RU21
RU22
CC
TDL
1


Data-Storage & Data-Transfer – ERA-Model II.1 (first version)
One Example for Information-Flow
MS 1
MS 2
ERA
NSA1
NSA2
RU11
RU12
RU21
RU22
CC
TDL
2.1


Data-Storage & Data-Transfer – ERA-Model II.2 (hybrid)
One Example for Information-Flow
MS 1
MS 2
ERA
RU11
RU12
RU21
RU22
NSA1
NSA2
2.2

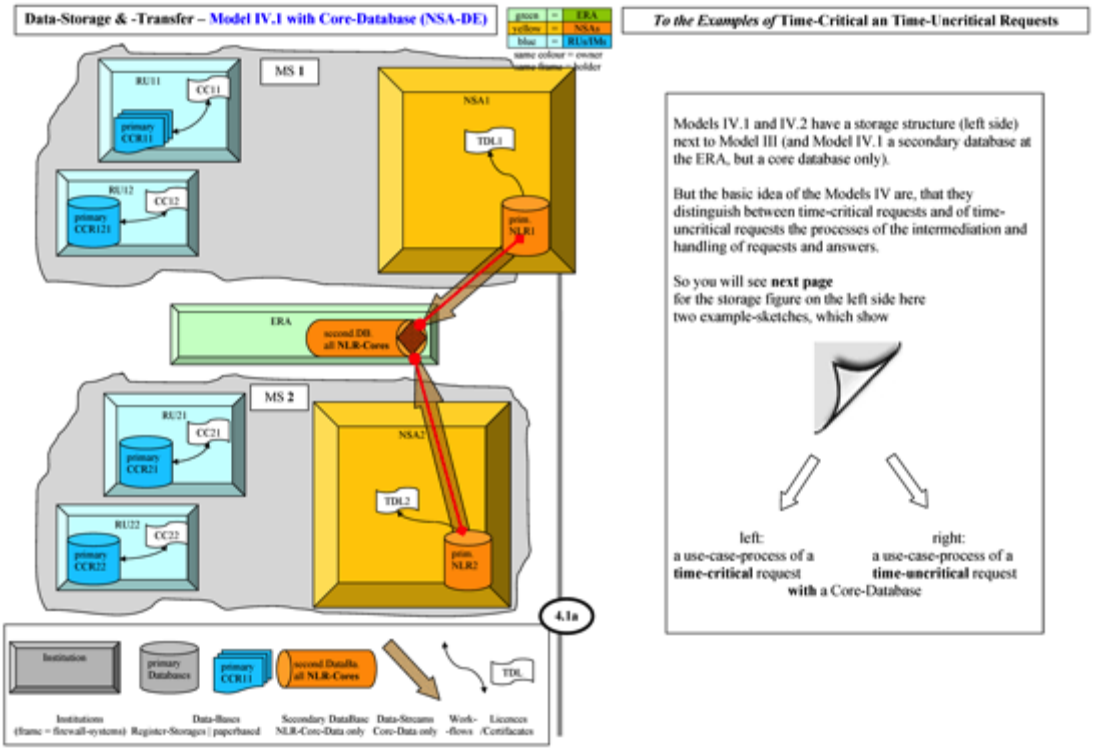

Data-Storage & Data-Transfer – ERA-Model III
One Example for Information-Flow of a Request
MS 1
MS 2
ERA
RU11
RU12
RU21
RU22
NSA1
NSA2
3

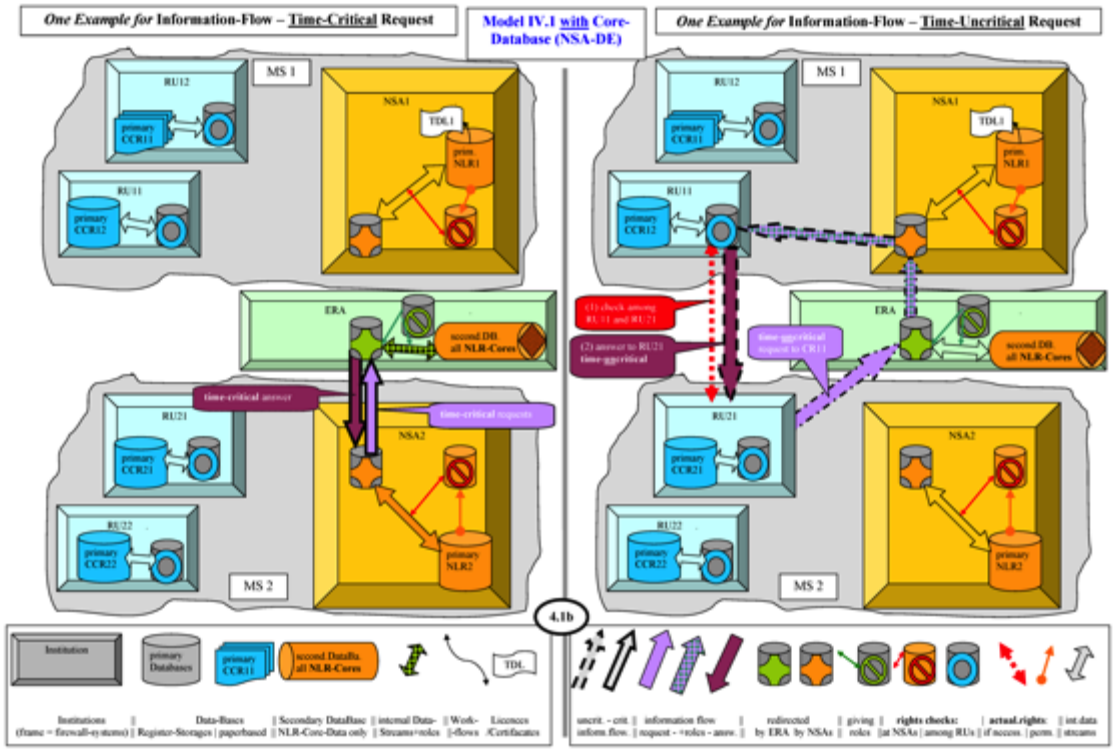
Model IV

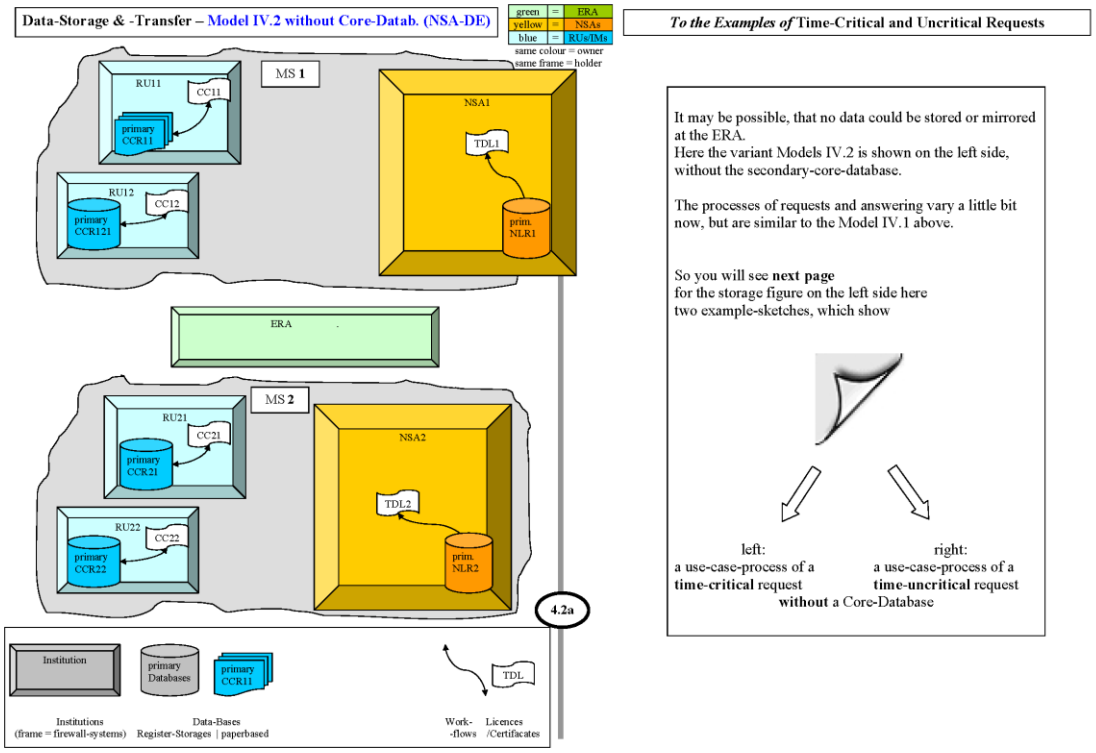
Version: IV.1 **with** a small **ERA-Core-Database**
Version: IV.2 **without** an **ERA-Core-Database**

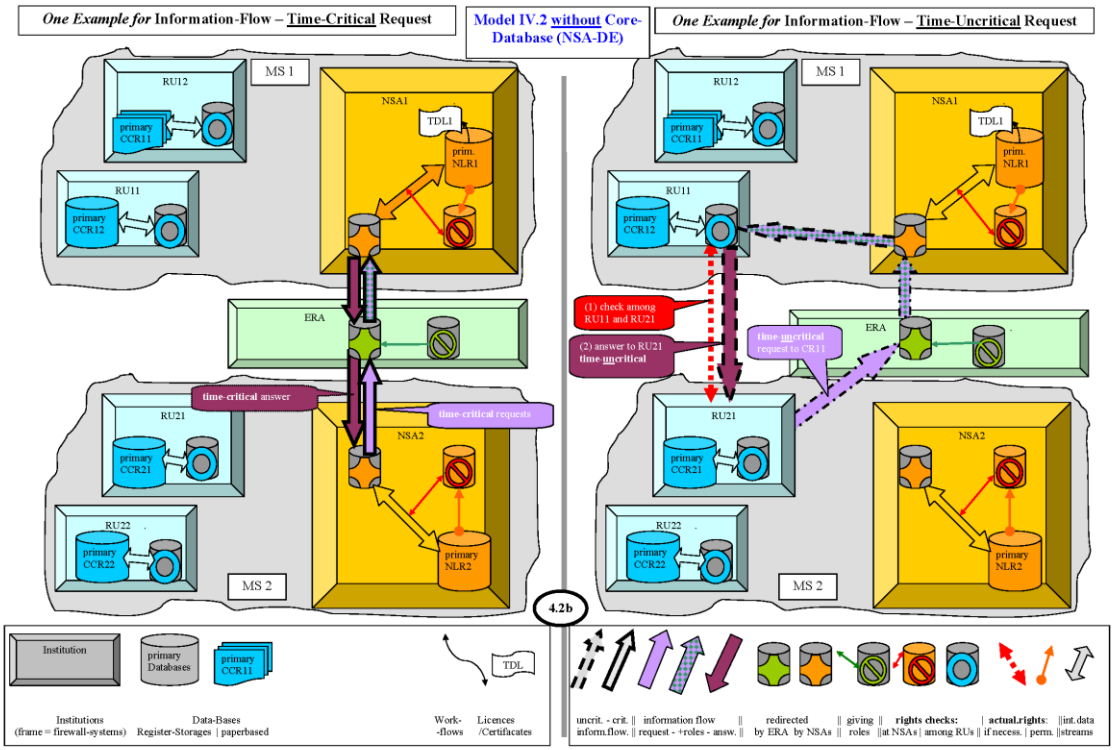
basing on the distinction of use-cases with …

- **time-critical** requests
  → **automatical** information-processes for immediate answers
- **time-uncritical** requests
  → **specific** information-processes for a answers in a period of max. 4 weeks


Data-Storage & -Transfer – Model IV.1 with Core-Database (NSA-DE)
To the Examples of Time-Critical an Time-Uncritical Requests
MS 1
MS 2
RU11
RU12
RU21
RU22
NSA1
NSA2
TDL1
TDL2
ERA
second DB all NLR-Cores
4.1a
Models IV.1 and IV.2 have a storage structure (left side) next to Model III (and Model IV.1 a secondary database at the ERA, but a core database only).
But the basic idea of the Models IV are, that they distinguish between time-critical requests and of time-uncritical requests the processes of the intermediation and handling of requests and answers.
So you will see next page for the storage figure on the left side here two example-sketches, which show
left:
a use-case-process of a time-critical request
right:
a use-case-process of a time-uncritical request
with a Core-Database


One Example for Information-Flow – Time-Critical Request
Model IV.1 with Core-Database (NSA-DE)
One Example for Information-Flow – Time-Uncritical Request
MS 1
MS 2
RU11
RU12
RU21
RU22
NSA1
NSA2
TDL1
ERA
4.1b


Data-Storage & -Transfer – Model IV.2 without Core-Datab. (NSA-DE)
green = ERA
yellow = NSAs
blue = RUs/IMs
same colour = owner
same frame = holder
MS 1
RU11
CC11
primary CCR11
RU12
CC12
primary CCR121
NSA1
TDL1
prim. NLR1
ERA
MS 2
RU21
CC21
primary CCR21
RU22
CC22
primary CCR22
NSA2
TDL2
prim. NLR2
4.2a
Institution
primary Databases
primary CCR11
TDL
Institutions (frame = firewall-systems)
Data-Bases Register-Storages | paperbased
Work- -flows
Licences /Certificates
To the Examples of Time-Critical and Uncritical Requests
It may be possible, that no data could be stored or mirrored at the ERA.
Here the variant Models IV.2 is shown on the left side, without the secondary-core-database.
The processes of requests and answering vary a little bit now, but are similar to the Model IV.1 above.
So you will see next page
for the storage figure on the left side here
two example-sketches, which show
left:
a use-case-process of a time-critical request
right:
a use-case-process of a time-uncritical request
without a Core-Database


One Example for Information-Flow – Time-Critical Request
Model IV.2 without Core-Database (NSA-DE)
One Example for Information-Flow – Time-Uncritical Request
MS 1
RU12
primary CCR11
RU11
primary CCR12
NSA1
TDL1
prim. NLR1
ERA
time-critical answer
time-critical requests
MS 2
RU21
primary CCR21
RU22
primary CCR22
NSA2
primary NLR2
(1) check among RU11 and RU21
(2) answer to RU21 time uncritical
time uncritical request to CR11
4.2b
Institution
primary Databases
primary CCR11
TDL
Institutions (frame = firewall-systems)
Data-Bases Register-Storages | paperbased
Work- -flows
Licences /Certificates
uncrit. - crit. || inform.flow. || information flow || request - +roles - answ. || redirected by ERA by NSAs || giving roles || rights checks: || at NSAs | among RUs || actual.rights: if necess. | perm. || int.data streams

List of Symbols

	The left sides:	Illustrated are the physical locations of the data, the storage of the data, and data-streams signifying the transport of data from one place to an other one.	
1		These boxes show the different institutions: ERA (green), NSAs (yellow), RUs/IMs (blue). Note: the frame of these boxes shall remember, that each institution will have a firewall-construction, which is to consider for the installation of the network connections.	
2		Member state area with a MS-number	
3		Primary Databases. – This shape marks the fundamental databases: NLRs (yellow) at the NSAs (yellow) or CCRs (blue) at the RUs/IMs (blue). The colour marks the owner of the data in this secondary base.	
4		by-the-way: if an RU or IM may have a paper-based database, it will be signed in this way	
5		Secondary Databases stock data, which are repeated stored or mirrored at another place as answer-base for the information system. The data will be mirrored from the primary database or online input. So, for example, the hybrid version of Model II allows, to store the data of the RUs/IMs primary at the RUs/IMs, but mirroring these data at the NSAs in a secondary storage. The colour marks the owner of the data in this secondary base.	
6		… So it may happen, that a NSA, which allows both ways, could have a hybrid database with a primary and a secondary part.	
7		A special Secondary Database would be applied in Model I, where the ERA (green) would store the mirror of the databases of all other institutions: the NSAs (yellow) and RUs/IMs (blue).	
8		The wide, shaded arrows mark the data-streams of mirroring among the institutions or the primary databases and the secondary databases, every night for example. The colour of the arrows marks the responsibility (submitting, maintaining, controlling) of these data.	
9		It is one act, to mirror data in a foreign IT-system. It is another act, to work in a duplex operation in a foreign system. Therefore the necessary of full access-rights of a data-owner, operating in the IT-system of a foreign data-holder is signified with this symbol.	
10		The symbols for the Train-Driver Licences and the Complementary Certificates …	
11		Marks the connection, needed for the creation of the licences/certificates	
12		A special case will occur in Model IV (first version), where only core-data of the NLRs are mirrowed to the ERA, the variation of a smart version of Model I.	
13		… and accordingly the arrows for mirrow-streams of core-data (see below).	

	The right sides:	Here the occurring information-flows are illustrated. Additionally to the previous signs you find here:	
14		These cylinders mark electronic-founded distribution-systems, which redirect requests out of an institution to the competent answerer. With a green cross for the ERA, yellow cross for the NSAs. In the here presented models no RU/IM needs such a distribution cylinder. But …	
15		… a special case will occur (see Model IV and the Inter-MS-Problem), when RUs/IMs contact other RUs/IMs to interchange information or data. To prefigure, that RUs/IMs are allowed to cooperate in their own manner, this sign is used.	
16		One important aspect of the ERA-models is to equip the requests with roles, symbolized with this sign.	
17		But also important become the control of the request with access rights. For these procedures databases for a right-management are needed. Note: Access-rights are guaranteed by the owners of the correspondent data. So these owners have to arrange and maintain their access-right-data: marked with the colour (yellow by the NSAs, blue by the RUs/IMs), even if the access-right-database is stored in another institution. The small red arrow symbolized the given access rights to the internal data-request for a foreign requester.	
18		So if the data of NSAs and RUs/IMs are stored at the ERA, a double database had to control the access rights – maintained by those NSAs and RUs/IMs.	
19		The small wide arrows mark internal data-exchanges or data-streams in an institution (normal = active, pallish = inactive in the examples) …	
20		… with the carried access-rights	
		Data-streams within the ERA with roles	
21		If data of the access-right-database correspond with the primary database it is signed by this arrow.	
	Information-Flows (on the right sides)	The wide arrows mark on the right side of the pages information-flows. To see: potential flows (white) and one example per page (coloured).	
22		Symbol for a one- or two directed information-flow. White arrows mean only potential streams.	
23		In the presented examples the colours will say: request to the ERA – equipped with roles by the ERA – answer	
24		When use-cases will be studied, the frame of the arrows shows: • continuous frame = time-critical procedure (immeditially) • broken frame = time-uncritical procedure (up to 4 weeks)	
25		The red-dotted arrow (pure or in a white arrow) marks the time-uncritical possibility, to clarify access-rights in an un-critical way among the information-partners.	

25 Annex 11: Business models of Interoperability evaluation (Models I, II & III)

	Model I			Model II Hybrid			Model III		
	ERA	NSA	RU / IM	ERA	NSA	RU / IM	ERA	NSA	RU / IM
Server hardware cost	5	0	0	2	5	0	2	5	5
Programming cost	5	0	0	4	2	0	4	2	2
Maintenance cost	4	0	0	3	2	0	2	2	2
Server Installation cost	4	0	0	2	4	0	2	4	4
Client installation cost	0	0	0	0	0	0	0	0	0
Aggregate:	**4**	**0**	**0**	**3**	**3**	**0**	**2**	**3**	**3**
Security factor	**5**	**2**	**2**	**4**	**4**	**2**	**4**	**4**	**2**
Human factor (HR Requirements)	5	3	0	4	3	3	4	3	4
Political implications	5	0	0	0	5	5	0	5	4
Aggregate:	**5**	**2**	**0**	**2**	**4**	**4**	**2**	**4**	**4**

Table I: Summary figures of Models' Necessary Budget Evaluation

Note: Factors are representing cost measures rather than financial values, therefore lower figures suggest the better approach.

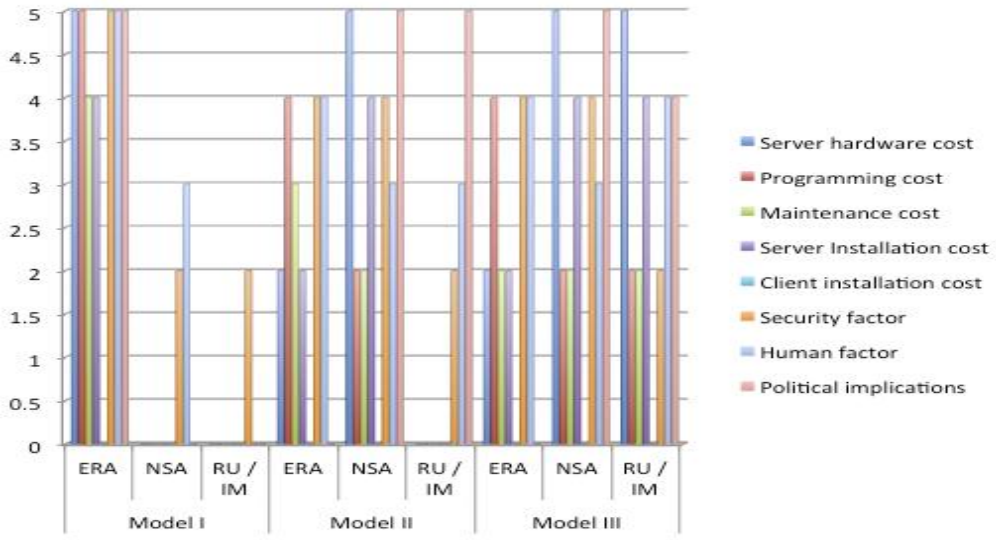


Figure 11: Cost measures

There are three important groups of factors: the **Technological**, **Human** and **Political.** They need to be evaluated for each model in order to choose the condition that is most suitable to ensure the project's success.

25.1 Technological factor

- Model I: It is important to highlight that the cost factor remains at the minimum level since analysts, developers, network engineers, security experts and help desk experts, on the one side, but also servers and hardware, on the other side, are centralized at ERA. Therefore, NSAs, RUs and IMs will only be querying with specific criteria in order to retrieve information and collect it according to their user credentials. They will be able to further manage information that is owned by them, not being able to interfere with others. Having a centralized software production team always has more profits in terms of quality and time performance. A solution will be provided to NSAs for introducing existing registered information/data by developing specific or generic bridges to import them in the new system. The specific model is not applicable specifically on the decision that ERA should not maintain the data storage.

- Model II - Hybrid: The cost of implementation will remain almost equal for ERA as it will be the main responsible organization for the delivery of the solution, additional costs will be incurred by NSAs since there will be local servers (twenty-five in total – currently) in order to manage and delegate information, so the need for developers and network engineers will become of high importance. Model II is gathering all elements described in Model I. One benefit is, if politically feasible, the possibility to concentrate data at few places (namely from the RUs and IMs at the NSAs) In these cases critical information is not spread at various locations, an the latency issues as well as increasing security risks (as in Model I) can be minimized; therefore a specific technical study should be assessed. In the case that an NSA would already have a system, specific bridges will be implemented in order to assist the workflow of information retrieval.
  On the other hand – and this is its hybrid character of this model – it allows each NSA of each MS to decide:
  - whether it collects all data of their national catchment area – viz. the CCR of all RUs and IMs in their country in addition to the NLR – in their data-base-system, and to answers so all request out of their system; optimizing the data import procedures concretely;
  - or it operates as a delivering system, which received the incoming requests, finds out the competent information-location, redirects the request to this place (to the NLR at the NSA itself or to a CCR of a RU/IM), and return the answers to the questioner via the ERA; optimizing the data transmission procedures concretely.

  As in all models the information access based on a cooperation of the role allocations by the ERA, the personal access rights given by the data owners, and the codification of the data themselves (such as UID, s. p. 51). But in the Hybrid Model the RUs and IMs of a

country can make an agreement with their NSA, whether they will manage the access permission itself or delegate to the NSA.

- Model III: In this case, the cost will also extend to the RUs and IMs and the need for additional engineers will increase for them. Additionally, there will be a serious multiplication increment in security risks despite the fact that ERA will provide the specifications on server and router installations.

- **Result**: **Model II Hybrid** is apparently the best practice as for the technological aspect, minimizing cost, human resources allocation and security issues. Additionally, the implementation cost will seize after product delivery. Thus, only the maintenance and help desk cost will continue running unlike in the other two cases. In fact, in Model II and III, the costs do not remain stable as expected and unforeseen costs may arise such as the purchase of equipment and the establishment of a network connection for the servers, network implications or increasing firewalls security.

- Unexpected factors: While unexpected, unforeseen factors or acts of God may always occur, a specific solid backup plan for only one location is more feasible than a series of plans. A possible solution is that a mirror server is kept in a third commonly agreed location that will continue to operate in case of a disaster.

25.2 Human factor

- Model I: A technical team will be needed at ERA's premises including

Optimal	Minimal	Time
1 Project manager	1 Project manager	100%
1 System analyst	1 System analyst – Technical writer	20%
1 Senior Database architect	1 Senior Database architect	20%
2 Database developers	1 Database developers	50%
1 Network architect	1 Network architect	20%
2 Software engineers	1 Software engineers	100%
1 Security expert	1 Security expert	20%
1 GUI expert		10%
1 Graphic designer	1 GUI - Graphic designer	10%
1 Technical writer		10%
1 Translator	1 Translator	5%
15 team members	**10 team members**	**Avg: 33%**

The above-mentioned team will be contracted or assigned for the lifecycle of the project implementation, which is estimated to be one year. This will cover the needs for developing the project, shortly after that, for its dissemination and then may be allocated to other projects. Additional staff will of course be necessary as:

Optimal	Minimal	Time
1 Software maintenance engineer	1 Software maintenance engineer	30%
1 Helpdesk	1 Helpdesk	100%
2 members per ERA	**2 members per ERA**	**Avg: 65%**
2 team members	**2 team members**	

Optimal	Minimal	Time
1 NSA Representative	1 NSA Representative	30%
2 Trainers on National level	1 Trainer on National level	10%
3 members per NSA	**2 members per NSA**	**Avg: 20%**
Sum with ERA of 81	**Sum with of 54**	

- Model II: With this model, the above-mentioned human resources will be needed for each NSA, and the costs displayed in the following have to be added:

Optimal	Minimal	Time
1 Network engineer	1 Network – Security specialist	25%
1 Database administrator	1 Database – Software specialist	20%
1 Security specialist		10%
1 Helpdesk support	1 Helpdesk support	30%
4 members per NSA	**3 members per NSA**	**Avg: 21%**
Sum with ERA of 180	**Sum with ERA of 85**	

Note: NSA employees will have a part-time role to the percentage that it is displayed.

- Model III: On top of all of the necessary human resource units for Model I and Model II, Model III requires the HR effort (minimum numbers):

Optimal	Minimal	Time
1 Network engineer	1 Network – Security specialist	25%
1 Database administrator	1 Database – Software specialist	20%
1 Security specialist		10%
3 members per Entity	**2 members per Entity**	**Avg: 18%**
Sum with ERA - N/A	**Sum with ERA - N/A**	

- **Staff allocation**: It is necessary to highlight that most of the staff members by all involved parties will already be existing in Model I, and can be partially used for the implementation of the project, while in Model II and III, there is a high probability of requiring the recruitment of additional resources.

- **Result**: The project will take a major proportion in terms of human resources moving from Model I towards Model III. The only difference between Model I and Model II is the additional effort in maintenance that should be necessary in terms of number of staff required by the NSAs. It needs to be highlighted that the more human interactions are involved, the higher the likelihood of issues that can arise, especially when managing various locations as in Model III.

25.3 Political Sensitivity

- Scope: Understanding the political sensitivity of this system, a strategic alignment should be achieved, in order to preserve political support. Although, at a theoretical level, on the basis of the EC legislative framework, there should not be any specific issues to consider, we understand that decentralization on a national level may trigger certain uncertainties derived from cultural and personal concerns.

- Model I: In the **ERA Insourcing** model, all information will be hosted at ERA and none at a National level, which means that there will have to be certain and secure workflows

that are related to information delegation and interoperability. Those that should be taken into consideration are specific user rights and privileges for each transaction.

- Model II: This is a **hybrid - moderate decentralized model**, which has the **main privilege of having information managed by the NSAs and at least each NSA's proprietary information would be delegated faster at a local scale**. That is necessary since specific National Legislations are in force, and even though according to the EC's decisions, this is not necessary, in order to avoid copyright issues, these models lead to maximum results in this aspect.

- Model III: This **decentralised model** implies that the existing players would remain in control of collecting information and would therefore imply the lowest risk of political uncertainties or resistance.

- **Result**: Model II, is securing data information storage and will not imply any issue regarding keeping records of personal information. The changes need to be presented and communicated in the correct way to assure collaboration from the relevant political authorities ahead of time. Also, the potential advantages for job seekers and employers in this sector need to be highlighted.

25.4 Business Models Comparisons and Understandings

	Model I	Model II	Model III
Overall Performance	**High**	**Moderate**	**Poor**
Availability	**High**	**High**	**Moderate**
Technology	**High**	**High**	**Poor**
Security	**High**	**High**	**Poor**
Governance	**Moderate**	**High**	**Poor**
Process issues	**Moderate**	**High**	**Poor**
EC Policy Compliance	**High**	**High**	**High**
Scalability and Elasticity	**High**	**High**	**Poor**
Human Resources	**High**	**Moderate**	**Poor**
Green IT	**High**	**Moderate**	**Poor**
Political Impact and Sensitivity	**Poor**	**High**	**Poor**
Costs and Funding	**High**	**High**	**Poor**

Table II: Summary of Performance based on findings – Values measuring Performance

Observing the result figures, it becomes evident that **Model II** would be the optimal scenario in the case of deciding in favour of developing the system.

Observations:

- As an expected result of systems that need to be centralized, there needs to be a specific point of reference for data collection, in order to establish high quality of information delegation and retrieval, while data and network security will be maintained at high levels and budget will stay at the minimum expenditure levels.

- It is clear that since NSAs, RUs and IMs will be involved not only in retrieving information but also in feeding them to the system, their resources should be allocated in such operations instead of creating additional needs for system monitoring, security and networking. Additionally, having various points of reference as per Model II and III, network performance issues may arise and increase risk levels in terms of security, response and data loss. A potential failure in such issues may cost trust among the involved parties and decrease confidence in the system and the motivation to use it.

- In addition, it is important to highlight that the system under discussion, according to the EC Directive, must be accessible and open to all stakeholders (respecting their individual access rights) and serve the mentioned purposes. Compromising with a sum of factors would risk the overall performance and lead to dubious results.

26 Annex 12: Actors' involvement

In the case of proving the feasibility of the system, in order to secure its success there has to be specific involvement of all actors at the **Technological, HR** and **Information Dissemination** levels.

Note: For the tables below, the measurement to be followed is:

✓100% involvement	✓50% involvement	✓25% involvement	✓0% involvement

Figure 6: Explanation of involvement measures

26.1 Technological aspect

Implementation Steps	Description	ERA	NSA	RUs	Ims
PHASE I					
Requirements & Specifications	• Define Project Scope • Content definition and data migration • Interview Authorities • Inspect Conditions • Define Deliverables • Prepare Project Budget • Determine Technologies • Create Functional Technical Analysis Document • Determine Use Needs • Determine Users and rights • Define Use Cases	☑	☑	☑	☑
PHASE II					
System Design & Development	• Verify Specifications • Prepare Project Plan • Determine Code Compliance Needs • Database architecture • Administrators Environment • Design front-end and back-end interface (GUI) • Bridges Development • Testing • Develop draft version 1.0	☑			

PHASE III					
System Adaptation	• Document Messages and Translate into EU Languages • System Security • Plan system backups	☑			
PHASE IV					
Production Release	• Final testing • Perform Installation in all designated locations • Security verification • Inspect Installation • Release version 1.0	☑	☑	☑	☑
PHASE V					
Maintenance and Support	• Corrective maintenance • Adaptive maintenance • User support • Authorities support • System updates • System security • System 24/365 availability • System back-ups	☑			

Table II: Technological actors' involvement

Even though most of the staff allocation will take place in Phase II, special attention should be given to Phase I, since that will be the keystone for the success of the system. **Use Cases** and **Information Flow Scenarios** will provide the understanding for architects and developers in order to create the system according to the EC's Decision prerequisites. For Phase V, it is also important to highlight that hosting the know-how and the help desk in-house, higher efficiency of query responses by all involved parties can be offered.

26.2 Human Resources aspect

Implementation Steps	Description	ERA	NSA	RUs	IMs
PHASE I					
Technical Specification	• Technical Writer • Project Manager • Analyst Programmer • Database Architect • Network Architect • Graphical User Interface (GUI) Designer	☑	☑	☑	☑
PHASE II					
Implementation (Design - Development)	• Project manager • Database developers • Analyst Developers • Network Developer • GUI Designer • Testers	☑	☑		
PHASE III					
Dissemination	• Project Manager • Analyst Developer • Technical Writer • Tester	☑	☑	☑	☑
PHASE IV					
Maintenance	• Analyst Developer • Helpdesk	☑			

Table III: HR actors' involvement

As expected, the first two phases - primarily the second one - will use the majority of the allocated staff resources. Also, apart from the first and the third phase, NSAs, RUs and IMs will not need to provide any staff resources. In fact, their involvement will be minimal but essential for the success of the project. It needs to be highlighted that the majority of the staff necessary for the development is already in force and will be allocated to this project by ERA, while the necessities of the rest of the actors will be minimal and covered by their existing staff.

26.3 Information Dissemination

Assuming the insourcing Model II, the higher the quality and impact level of dissemination, the higher the expected involvement of the relevant parties is. A specific dissemination plan should be devised in case the system is created. This should be based on the further technical study of how information is reviewed, in order to preserve interoperability. It is likely that different actors require different types of dissemination. Whilst public servants can most likely be reached with newsletters by email, train drivers and related staff tend to be moving, therefore might be more interested in reading flyers and receiving information at the different train stations (posters, leaflets, etc.).

ERA will provide training, training material, manuals of use for both users and administrators organize meetings and presentations, whilst the introduction and validity of data will be a responsibility by the rest of the involved actors.

27 Annex 13: Technical approach

The approach follows specific principles, such as **low cost for all stakeholders**, **high level of interoperability**, **immediate response** and **high level of security standards**. All these four elements are specifically designed to meet the criteria of EU's decision.

27.1 Information flowchart

There are two main processes to describe concerning the **information flow**, that apply to Model II, which has been proven to be more suitable for the specific needs. It is to differ: data are the single items in a database. A dataset are the combined data of a topic. Information is the combination of datasets delivered in a process of enquiry:

- **Information storage process**:
  - All information will be managed / delivered / redirected and answered by NSA's servers;
  - All information will be ready to be queried by ERA's interface;
  - NSAs, RUs, IMs, will be legitimate and/or physical owners of each of their information item
  - Information are maintenance and as the case may be submitted or updated by NSAs, RUs, IMs themselves;
  - Access rights will be respected while introducing or updating information;
  - If Information is be stored or updated via a browser environment, no additional is needed for client installation at the local NSA, by the NSA or RU/IM that regionally belongs to it;
  - Users' authentication forms will be in place before accessing the administrative part of the system to secure access only to authenticated users;
  - Information should be stored in one or more databases;
  - Each information item is to discuss to have a specific Unique Identifier (UID);
  - Each information item will have the reference of the authority that submits it;
  - Each information item will have the authorised person's ID that commits the transaction;
  - All physical documents will be stored and linked with a specific information item plus its author/owner;
  - All items will only be able to be altered by their owners;
  - A chronological record of updates (versions) will be kept per each item;
  - All network transactions will succeed under secure network protocols.
  - But there will be a problem of cross-storing of personal data, which is not yet solved and will be shown here:

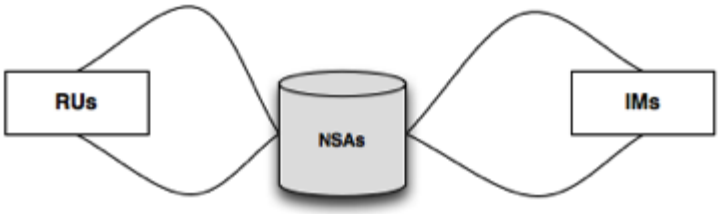


Figure 12: Information storage process

- **Request and retrieve information process**:
  - In Hybrid-Model IIa (Data Collecting Variation) there are six equal, in terms of data flow cases, on how information may be sought by the stakeholders:
    1. **NSA** seeks information submitted by RU/IM
    2. NSA seeks information submitted by NSA other
    3. NSA seeks information submitted by NSA self
    4. **RU/IM** seeks information submitted by NSA
    5. RU/IM seeks information submitted by IM/RU other
    6. RU/IM seeks information submitted by RU/IM self

    Annotation:

    (a) what is meant above: data-flow-cases or information-flow-cases or both? – The following considerations mean information-flow-cases.

    (b) Question: Are six cases enough, to describe all information-flows? Because:

    Requester can be:
    7. all NSAs
    8. all RUs/IMs
    9. other authorities
    10. train-drivers themselves
    11. ERA

    Answerer can be:
    12. each NSAs
    13. each NSA

    Conditions can be:
    14. answer in a state
    15. answer to another member state

    So as combinations can occur:
    16. NSA to itself
    17. NSA to other NSA (or ERA)
    18. NSA to RU/IM in the same member state
    19. NSA to RU/IM in another member state
    20. NSA to an authority in the same member state
    21. NSA to an authority in another member state

22. NSA to a Train Driver
23. RU/IM to itself
24. RU/IM to other RU/IM in the same member state
25. RU/IM to other RU/IM in another member state
26. RU/IM to NSA in the same member state
27. RU/IM to NSA in another member state (or ERA)
28. RU/IM to an authority in the same member state
29. RU/IM to an authority in another member state
30. RU/IM to a Train Driver

In this considerations are not regarded the cases of redirected requests among NSAs and/or RUs/IMs. This will occur, if train driver's CC is not registered in the same state as his TDL.

- As for the EU's decision, access to information will be granted to the stakeholders by reasoned request, therefore, specific **forms** will be implemented that will forward the request to the appropriate authority according to the six potential processes as described above;
- **Forms will associate**:
  - Authority that request information;
    - Person from the specific authority that seeks information;
  - Authority that has originally submitted the specific information;
    - Person in charge who will reply to the request;
- Users will be able to use forms and the environment after login with their personal user credentials;
- All transactions will succeed under specific user rights;
- Reasons of the transactions, along with their report of acceptance or rejection will be recorded automatically in the database (IMI's in the selected case scenario);
- Response of the system on retrieving information after the acceptance should be immediate;
- Notifications for acceptance or rejection on providing information should exist;
- All transactions will be monitored and stored at ERA's servers;
- High network security standards should be met.

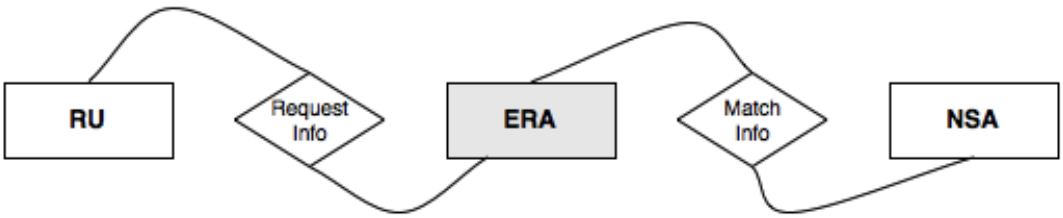


Figure 13: Example 4/6 case > Information requested by an NSA that was submitted by an RU

27.2 Information kept for drivers for NLRS and CCRS

As per Decision EC/17/2010 Information that should be kept by all stakeholders concerning:

- **National registers of train driving licences (NLRS)** are:
  - **Section 1: Current state of the license**
    - **Licence number**
      - Number of the licence
    - **Current state of the licence**
      - Evidence of the current state of the licence.
        - Valid,
        - Suspended (decision pending),
        - Withdrawn,
      - Reason for suspension or withdrawal
  - **Section 2: Information on the current licence issued, in accordance with Annex I, Section 2, of Directive 2007/59/EC**
    - **Surname(s) of the holder**
      - Surname(s) displayed on passport or national identity card or other recognised document proving identity. More than one surnames are allowed, depending on national custom
    - **Name(s) of the holder**
      - Name(s) displayed in passport or national identity card or other recognised document proving identity. More names are allowed, depending on national custom
    - **Date of birth of the holder**
      - Date of birth of the holder
    - **Place of birth of the holder**
      - Place of birth of the holder
      - Nationality
    - **Date of issue of the licence**
      - Display of the current date of issue of the licence
    - **Date of expiry of the licence**
      - Date of the expected formal expiry of the valid licence
    - **Name of issuing authority**
      - Name of the authority issuing the licence (competent authority, delegated entity, railway undertaking, infrastructure manager)
    - **Name(s) of the undertakings, employing the TD**
    - **Address(es) of the authorities**
    - **Reference number assigned to the employee by the employer**
      - Company reference for the train driver
    - **Photograph of the holder**
      - Photograph
    - **Signature of the holder**
      - Signature

- **Permanent place of residence or postal address of the holder**
  - Address of the holder
  - Street and number
  - Town
  - Country
  - Postcode
  - Telephone number
  - e-mail address
- **Additional information**
  - Information imposed by a competent authority in accordance with Annex II of Directive 2007/59/EC
  - Field 9.a.1 — Native language(s) of the driver
  - Field 9.a.2 — Space reserved for entries by the Member State which issues the licence, for information that may be necessary under national legislation
- **Medical restriction**
  - Information imposed by a competent authority in accordance with Annex II of Directive 2007/59/EC
  - Mandatory use of glasses/lenses
  - Mandatory use of hearing aid(s)

- **Section 3: Records information on the status of the licence and the results of periodic checks**
  - **Date of first issues**
    - Date of first issue
  - **Date of expiry**
    - Date of expiry (and of expected formal renewal)
  - Update(s) (Several records are possible)
    - Date of update
    - Reason for update
  - **Amendment(s) (Several records are possible)**
    - Date of amendment
    - Reason of amendment
    - 13.1.2010 EN Official Journal of the European Union L 8/21
  - **Suspension(s) (Several records are possible)**
    - Length of period of suspension
    - Reason for suspension
  - **Withdrawal(s) (Several records are possible)**
    - Date of withdrawal
    - Reason for withdrawal
  - **Licence reported lost**
    - Date of communication
    - Date of any duplicate issued
  - **Licence reported stolen**
    - Date of communication
    - Date of any duplicate issued

- **Licence reported destroyed**
  - Date of communication
  - Date of any duplicate issued

- **<u>Section 4: Information on the basic requirements for issuing a licence and results of periodic checks</u>**
  - **Education**
    - Basic requirement
    - Highest level of certification
  - **Physical fitness**
    - Basic requirement
    - Statement on fulfilment of criteria in Directive 2007/59/EC, Annex II (Sections 1.1, 1.2, 1.3 and 2.1)
    - Date of check
    - Subsequent periodic check
    - Date of last check
    - Next check
    - Notes
      - Normal schedule,
      - Anticipated schedule (according to doctor's certificate),
      - Change in information (code 9.a.2) if necessary,
      - Change in restriction code,
      - Other + field to specify,
  - **Occupational psychological fitness**
    - Basic requirement (Statement on fulfilment of criteria in Annex II of Directive 2007/59/EC (Section 2.2)
    - Date of check
    - Following check(s)
    - Date of any subsequent
  - **General professional knowledge**
    - Basic requirement - Statement on fulfilment of criteria in Annex IV o Directive 2007/59/EC
    - Date of check
    - Subsequent check (only if required at national level)

II. Part of the CCR-Database

- Details of **Complementary Certificates for train drivers (CCRS)** are:
  - **<u>Section 1: Reference to the licence</u>**
    - **Licence number**
      - Number of the licence, giving access to data in the national register (13.1.2010 EN Official Journal of the European Union L 8/25)
    - **Current state of the licence**
      - Evidence of the current state of the licence
        - Valid
        - Suspended

- Withdrawn

- **<u>Section 2: Information about the current complementary certificate issued, as listed in Annex I, Section 3, of Directive 2007/59/EC</u>**
  - According to the ***Section 2: Information on the current licence issued, in accordance with Annex I, Section 2, of Directive 2007/59/EC***
  - **Address of the railway undertaking or infrastructure manager for which the driver is authorised to drive**
    - Address of the RU/IM (Street and number)
    - Town
    - Country
    - Postcode
    - Contact person
    - Telephone number
    - Fax number
    - email address
  - **Category in which the driver is authorised to drive**
    - Relevant code(s)
  - **Rolling stock which the driver is authorised to drive**
    - (list, record to be repeated)
    - For each item the date of the next expected check shall be added
  - **Infrastructure on which the driver is authorised to drive**
    - (list, record to be repeated)
    - For each item the date of the next expected check shall be added (13.1.2010 EN Official Journal of the European Union L 8/27)
  - **Language skills**
    - (list, record to be repeated)
    - For each item the date of the next expected check shall be added
  - **Additional information**
    - (list, record to be repeated)
  - **Additional restrictions**
    - (list, record to be repeated)
- **<u>Section 3: Records on the status of the complementary certificate</u>**
  - **Date of first issue**
    - Date of first issue of the certificate
  - **Update(s) (Several records are possible)**
    - Date of update
  - **Details of and reason for update (correction of one or more data displayed on the complementary certificate, e.g. personal address of the driver)**
  - **Amendment(s) (Several records are possible)**
    - **Date of amendment**
    - **Reason for amendments, referring to specific parts of the certificate:**
      - amendments in field 3 'Categories of driving'
      - amendments in field 4 'Additional Information'
      - amendments in field 5: new linguistics knowledge

- acquired or knowledge periodically checked
- amendments in field 6 'Restrictions'
- amendments in column 7: new rolling stock knowledge acquired or knowledge periodically checked
- amendments in column 8: new infrastructure knowledge acquired or knowledge periodically checked

- **Suspension(s) (Several records are possible)**
  - Length of period of suspension
  - Reason for suspension (L 8/28 EN Official Journal of the European Union 13.1.2010)
- **Withdrawal(s) (Several records are possible)**
  - Date of withdrawal
  - Reason for withdrawal
- **Certificate reported lost**
  - Date of communication
  - If yes, date of issued duplicate
- **Certificate reported stolen**
  - Date of communication
  - Date of any duplicate issued
- **Certificate reported destroyed**
  - Date of communication
  - Date of any duplicate issued

- **Section 4: Historical records in connection with the basic requirements for issuing a complementary certificate and the results of periodic checks**
  - **Linguistic competence**
    - Basic requirement (Working language(s) for which a statement that the criteria set out in Annex VI(8) of Directive 2007/59/EC had been fulfilled was issued)
    - Periodic check (Date of certified knowledge (exam passed) for each language)
  - **Rolling stock knowledge**
    - Basic requirement (Rolling stock for which a statement that the criteria set out in Annex V of Directive 2007/59/EC had been fulfilled was issued)
    - Periodic check (13.1.2010 EN Official Journal of the European Union L 8/29)
  - **Infrastructure knowledge**
    - **Basic requirement** (Infrastructure for which a statement that the criteria set out in Annex VI of Directive 2007/59/EC had been fulfilled was issued)
    - Periodic check

27.3 Information owner

It is important to highlight that the owner is responsible for each information item, plus the

physical documents (files) that accompany them, exist in the system, remains the specific **NSA**, **RU** or **IM** that submits and that only has privileges on updating it. ERA is not responsible for the content and will not be able to access such information for any reason, unless a written authorization by the owner is made and access from distant or local at NSA will be required. Despite the fact that information will be stored at NSA's database servers, only those that are in accordance to the EU Decision, regarding the user rights, will be able to access those information items or the attached physical documents to them. All information stored will be encrypted in a database and a high level of security standards will be established, only permitting access to owners and to those that owners will provide with specific access upon reasoned request. All requests and their reasons will be stored at ERA's servers.

27.4 Description of user functionalities

There are three main functionalities that we need to describe at this point:

- **Information Input by a stakeholder**
  - Verify that information exists at stakeholder's facilities in **electronic format**;
  - Stakeholder **logs-in** the system
    - **Access specific URL** established by NSA pointing to specific server;
    - Provide with **user credentials** (username / password);
    - Only employees of the NSA or RUs / IMs that belong to it may access the system;
  - **Automatic verification of access rights** according to EC's decision;
  - Access system page and select to **add information**;
    - Fill in specific form;
    - Attach file documents that accompany the information item;
    - Verify the validity of content;
    - Submit information;
  - Information stored at NSA's servers successfully

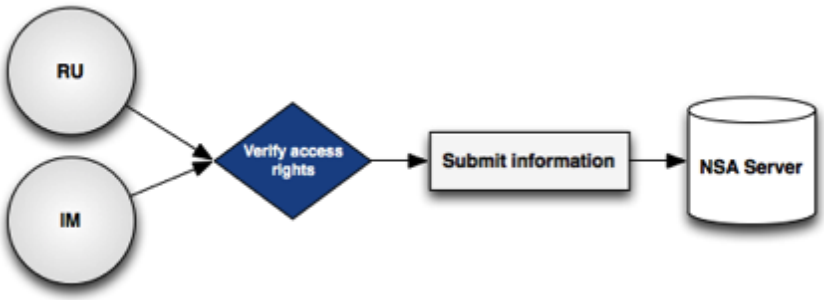


Figure 14: Example case > Information submitted by an RU/IM to NSA

- **Information updated by a stakeholder**
  - Stakeholder **logs-in** the system
    - **Access specific URL** the **matching system**, established by ERA pointing to the specific server;
    - Provide **user credentials** (username / password);

- **Automatic verification of access rights** according to EC's decision;
- Access system page and select **edit information**;
  - Access specific item that has to be updated and Fill in the specific form;
  - Attach updated file documents that accompany the information item;
  - Verify the validity of content;
  - Submit information;
- Information stored at ERA's servers successfully

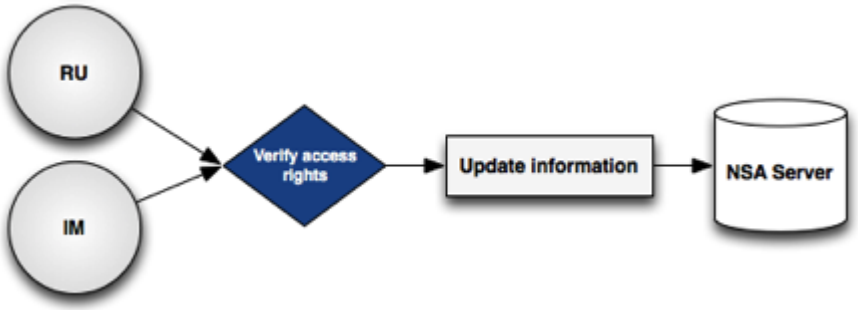


Figure 15: Example case > Information updated by an RU/IM to an NSA

- **Information requested by another stakeholder**
  - Stakeholder **logs-in** the system
    - **Access specific URL** established by NSA pointing to the specific server;
    - Provide **user credentials** (username / password);
  - **Automatic verification of access rights** according to EC's decision;
  - Access system page and select **search information**;
  - **Retrieve specific information item**
    - Fill in the specific form in order to provide an adequate reason for the owner of the specific item;
    - **Owner**
      - retrieves a notification that another stakeholder seeks a specific record and the reason for such a request
      - accepts the reason and allows specific information of the record to be displayed to the ?
      - declines the request and provides a significant reason
      - Verify the validity of the specific action;
    - **Stakeholder**
      - retrieves a notification for the state of his application
      - accesses information after acceptance
      - cannot access information after rejection
  - **All history of transactions is stored at ERA Servers.**

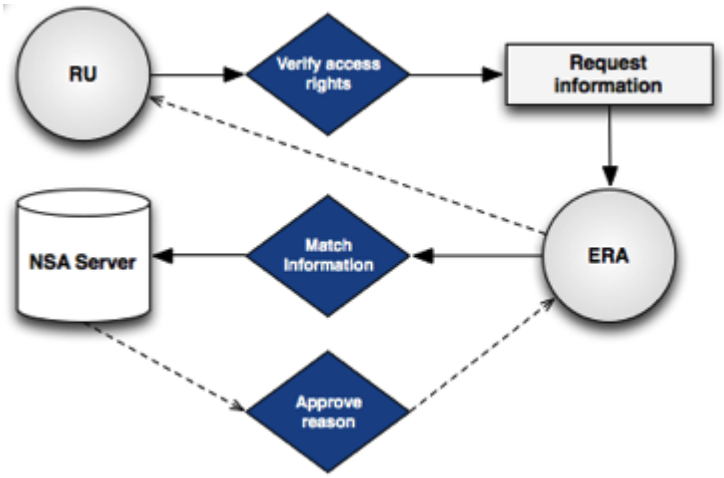


Figure 16: Example 4/6 case > Information submitted by an NSA and requested by an RU

27.5 Communication bridges and information retrieval

Since a significant number of NSAs are already developing such a system, it may not by any means imposed, using the new system for the registers, though specific communication bridges that will allow the secure interoperability and exchange of information upon reasoned request:

There are two cases:

- **a NSA has a system**: since according to the highest in performance proposed model (Model II) ERA will only be serving for the recording of requests and redirecting to the appropriate NSA, ERA's matching system will be querying each NSAs' system in order to redirect the query to the correct NSA. Of course, there will be detailed search forms, that ERA's matching system will be able to predetermine to a high percentage, the NSA that should redirect a specific query. (i.e. Driver nationality DK > NSA DK). For that **specific information bridges** will be installed that will most likely use **XML technology**, that is cross platform, in order to fetch the appropriate results.
- **a NSA does not have a system**: ERA will develop and install at NSA level the system in subject, and will respect all user rights and security issues. The abovementioned process will be added to this one.

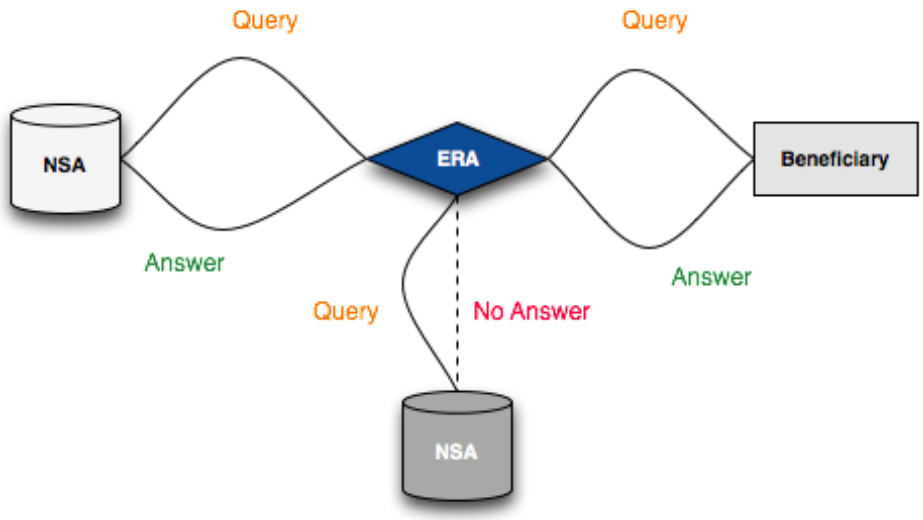


Figure 17: Example of querying 2 NSAs and bringing result to a stakeholder

27.6 Databases entity diagrams

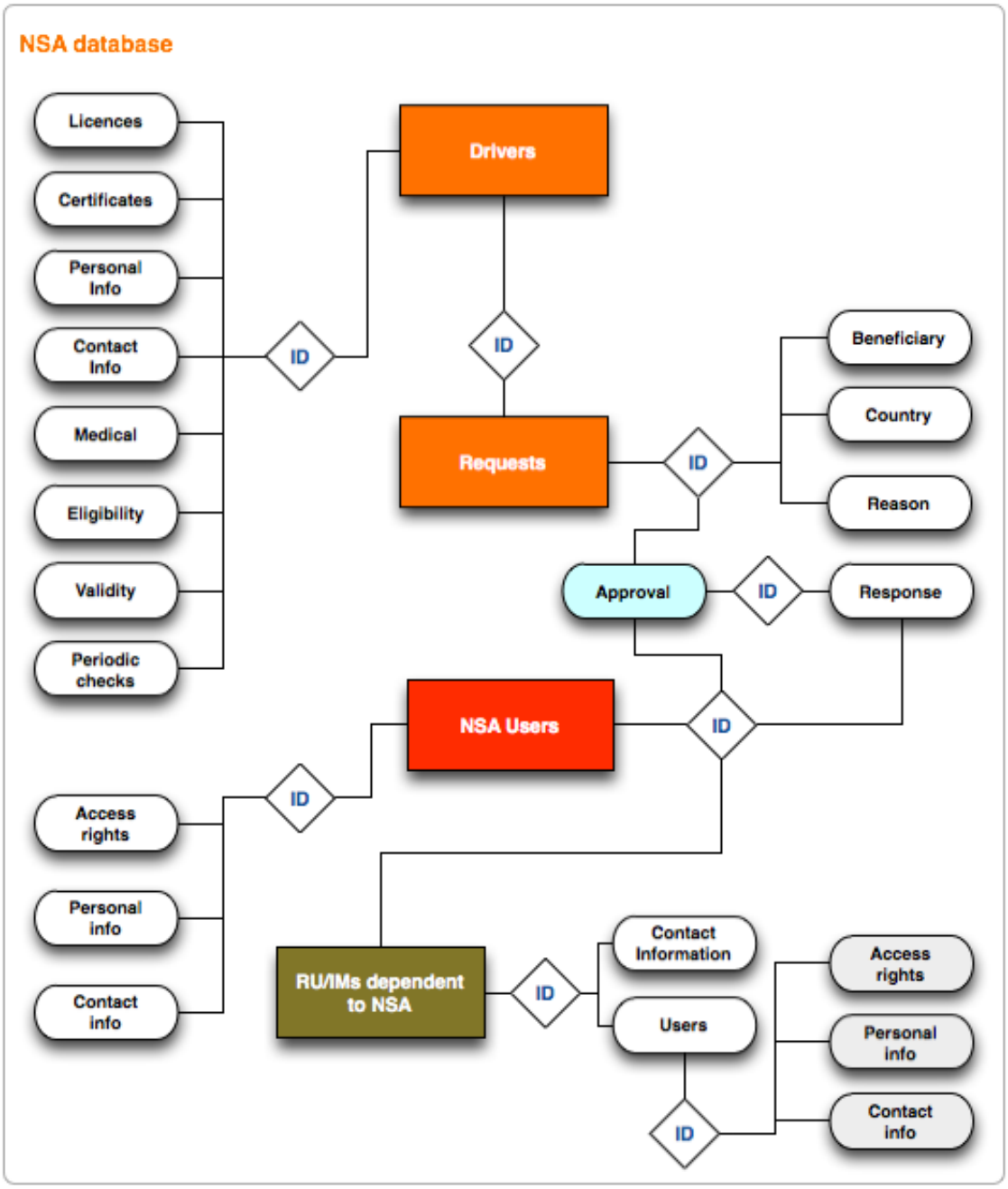


Figure 18: Database scheme of an NSA database

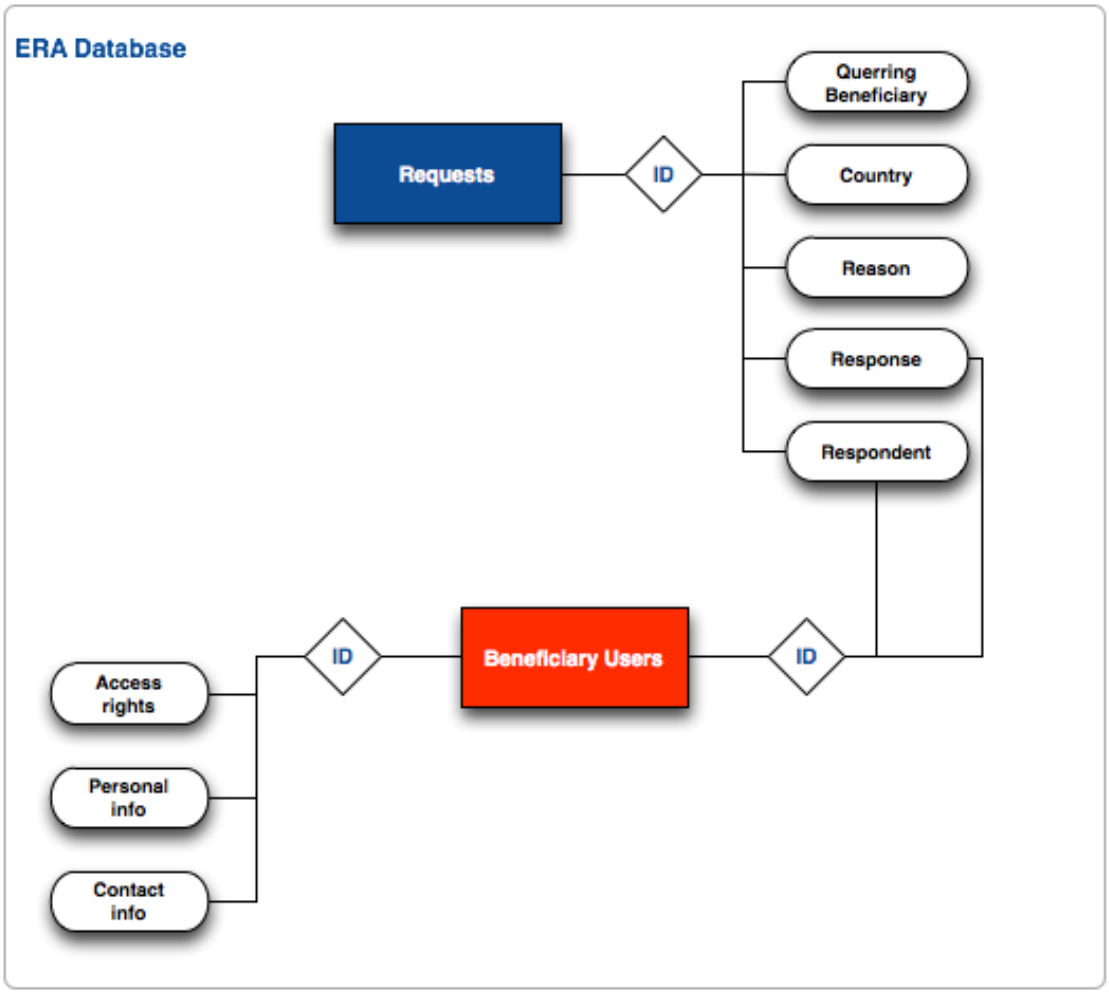


Figure 19: Database scheme of ERA database

Please note that detailed database diagram along with the entities will be necessary for the development of the pilot system.

27.7 Security observations

One of the most important factors in a high-quality system are the security characteristics. The system and server should adapt the following characteristics:

- **Captcha:** a type of challenge-response test used in computing to determine that the response is not generated by a computer
- **Content Approval:** a workflow to secure published on web information
- **Email Verification:** in order to avoid SPAM emails, an email filtering technique is checking both subject plus email content and sender address validity
- **POP3** / **SMPT** / **IMAP:** security on how to send, receive and post emails with NOTLS
- **Kerberos Authentication:** in order to allow individuals to communicate over a non-secure network to prove their identity to one another in a secure manner
- **Login History:** in order to keep a record of users transactions
- **Problem Notification** a system that reports any potential or existing issue
- **Session Management:** a process of keeping track of a user's activity during each session and interaction with the computer system;
- **Secure Shell or SSH & SSH 2:** a network protocol that allows data to be exchanged using a secure channel between two computers. Encryption provides confidentiality and integrity of data over a insecure network, such as the internet;
- **Versioning:** a process of assigning either unique version names or unique version numbers to unique states of computer software.

At this point, we would like to highlight that **NSA's servers and their collaboration with ERA servers should be proven to be trustworthy and secure**, because various information transactions will succeed. ERA's major responsibility lies in securing confidentiality of personal information and access to restricted information that will be hosted at NSAs' servers.

The following represent the required **enterprise operational standards**:

1. **Application Security** – the system along with its bridges will allow for **folder** and **function access** controlled through **NSA's and ERA** as defined by the standard permissions functionality. It has to be highlighted that **there will be no extra login screen**, but after the primary and only authentication the user may access easily the functions of the system.
2. **Application Services Security** – the document management application will support system administration functions to manage four major software functions:
    a. *Storage Manager* – functions which manage the document files stored in a repository(ies) and the media associated with the application

b. *Security Functions* – functions that support application level controlled access to the files and system level security functions (system administration tools for managing resources, users, documents, databases, workflow, forms, backup and recovery)
c. *Activity/Audit Log* – functions that manage the history of activity against documents in the repository and manage changes to documents (plus system maintained audit trails)
d. *Information Access* – functions which support searching for documents in the repository and controlling access to the documents through the document management application or through network security.

3. **Network Security** – equipped with appropriate tools installed in the server, we are in the position to identify any malicious attempts by human or machine. Allowing only necessary communication protocol active and securing them we guarantee the well assurance of stored information and system's performance.

4. **Access on Information Security** – there is a main concern on Privacy Law related to the data introduced in the system. The major issue derives from the fact that each Member State has a different Law and Regulation on Privacy. In respect to this, access rights on information should be established while respecting EU's as also national level directives or laws.
   a. Roles:
      i. Administrators ERA level
      ii. Administrators NSA Level
      iii. Supervisors
      iv. Representatives
      v. Users
      vi. Viewers
      vii. No access
   b. User access provided to ERA's server:
      i. ERA — access only to transactions, responsible for maintenance
      ii. NSAs — definition of key administrators and representatives
      iii. RUs/IMs — definition of representatives
   c. System owner:
      i. ERA — queries handling and transaction record keeping
      ii. NSAs — managers of their own system
      iii. RUs/IMs — managing their own system or having a partition at their NSA
   d. Information owner:
      i. ERA — no access to information apart from the queries
      ii. NSAs — owners to their information stored at their servers
      iii. RUs/IMs — owners to their information stored at their premises

28 Annex 14: Use-Cases

A use case is a description of how users will perform tasks on your Web site.

A use case includes two main parts:

- the steps a user will take to accomplish a particular task on your site
- the way the Web site should respond to a user's actions

A use case begins with a user's goal and ends when that goal is fulfilled. Each use case captures:

- The actor (who is using the system?)
- The interaction (what does the user want to do?)
- The goal (what is the user's goal?)

The steps we will follow to conduct the use cases are[23]:

- Identify who is going to be using the system,
- Pick one of those actors,
- Define what that actor wants to do on the system. Each thing the actor does on the system becomes a use case,
- For each use case, decide on the normal course of events when that actor is using the system,
- Describe the basic course in the description for the use case. Describe it in terms of what the actor does and what the system does in response that the actor should be aware of,
- When the basic course is described, consider alternate courses of events and add those to "extend" the use case,
- Look for commonalities among the use cases. Extract these and note them as common course use cases,
- Repeat the steps 2 through 7 for all other actors.

28.1 Use-cases methodology

The Criteria that are necessary considering for building the methodology of the Use-Cases are:

- **Information**
    - Requested content
        - TDL-Basics

[23] Kenworthy, E. (1997). Use case modelling: Capturing user requirements.

        - NLD-Data
        - NLR-Specifics
        - CCR-Data
        - CCR-Specifics
    - Use Cases
        - Unified / Consistent
        - Non Consistent
    - Extension of Response
        - Small
        - Middle
        - Differing
        - Large
    - Frequency
        - Seldom
        - Middle
        - Often
    - Required / Useful
    - Time critical
        - High
        - Middle
        - Low
    - Efforts for (prior) authorization
        - Very small
        - Small
        - Middle
        - Large
        - Very Large
    - Permission of requests
        - Total
        - Partial
        - Problematic
- **Paths**
    - Reduced Request
        - NSA1 > NLR2
        - NSA > CCR
        - NSA1 > [NSA] > CCR2
        - TD > NLR
        - TD > CCR
    - Reduced Answer
        - NLR2 > NSA1
        - CCR > NSA
        - NLR > TD
        - CCR > TD
        - NLR > SecF
    - Path Automation

- **Effort**
  - Verification
  - Identification
  - Authentication
  - (Sum) Authorization
  - Maintenance
  - Data rights
  - Permission for requests

The Use-Cases appear having many similarities and can be classified according to their nature but also the information exchange pattern according to the criteria and values that are characterizing them. According to the following figure, we can trace the use-case lifecycle and perform its analysis involving all necessary values. (Figures 6-8 are not readable! Flowcharts should be repeated in appropriate size as study annex.)

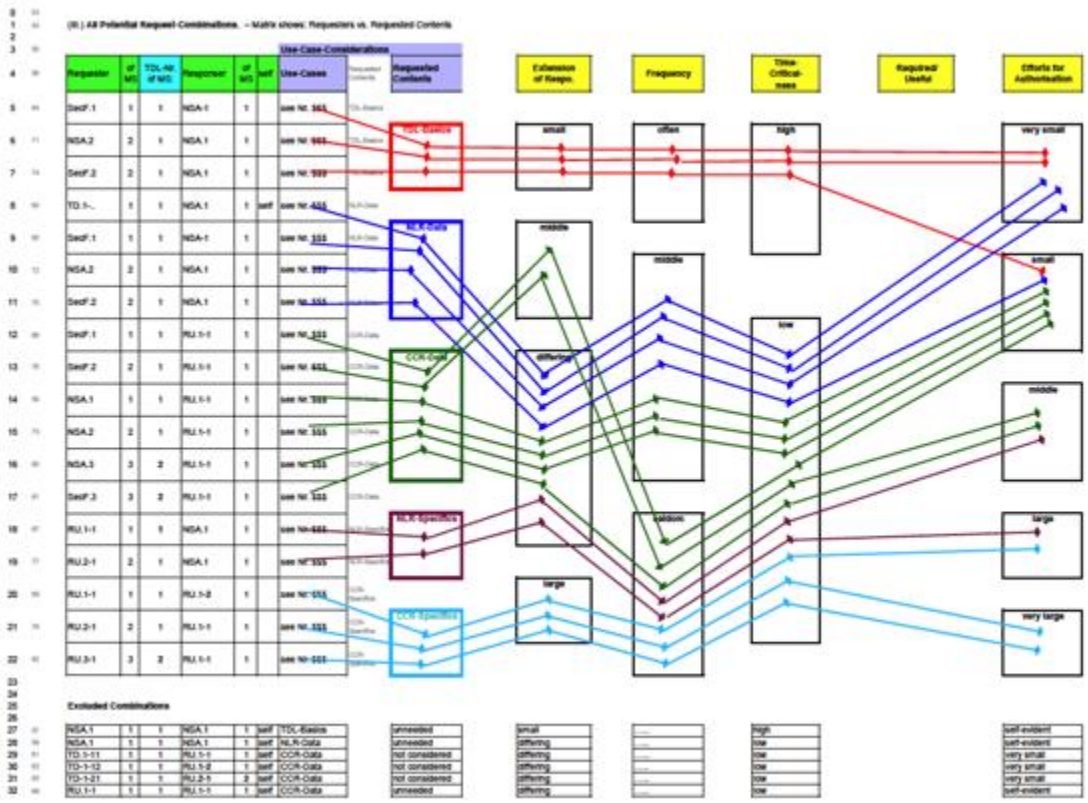


Figure 6: Trace Lines of Use-Cases

In the following figure, is displaying also the following information:

- Sum of paths
- Sum of authorizations
- Effort maintenance
- Effort data-rights
- Permission of request

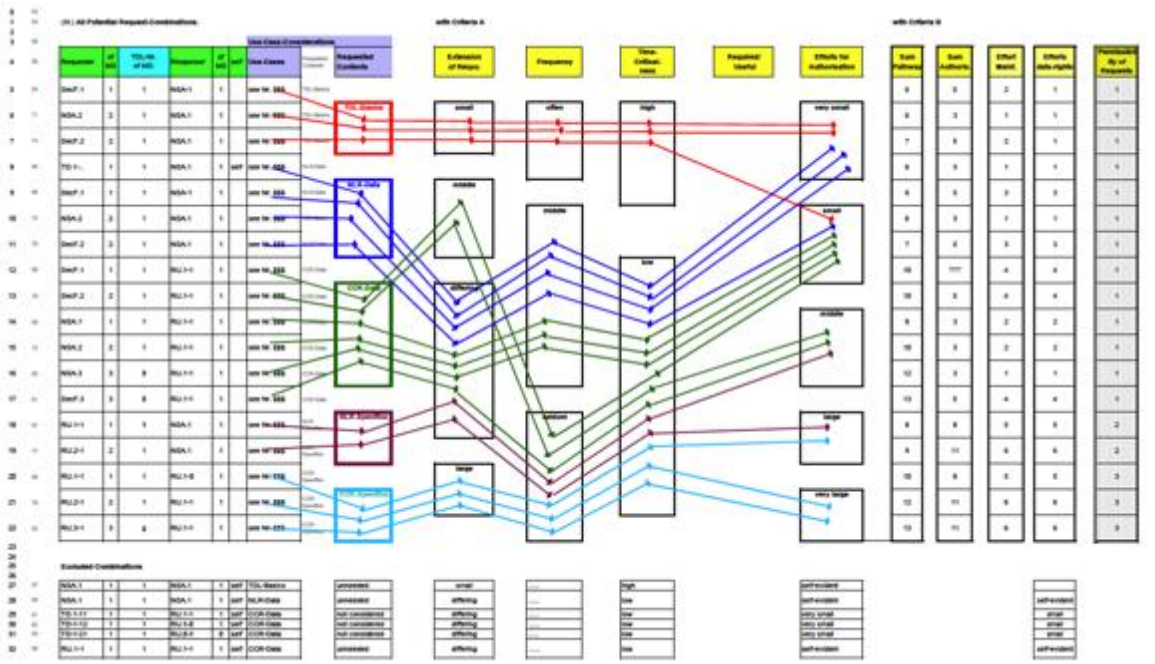


Figure 7: Display of all criteria for the Use-Cases

In the following graphic we can observe how all kind of use-cases are covered by the proposed business models as also how the existing solutions are providing solutions in our case.

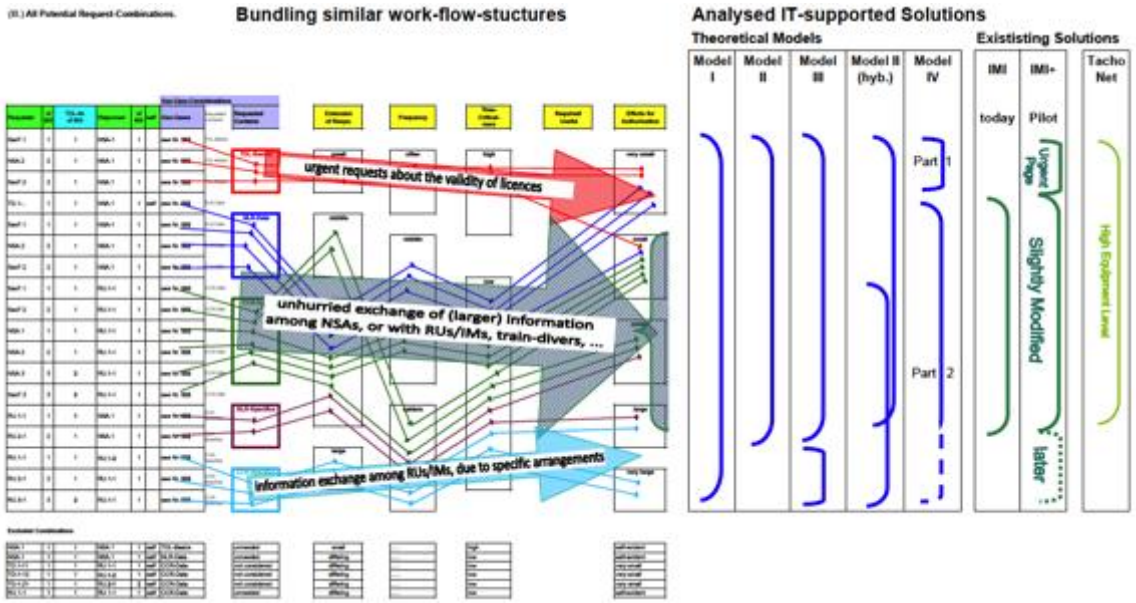


Figure 8: Display of all criteria for the Use-Cases

28.2 Use-cases examples on classification

We need to highlight at this point, that the use-cases are following the following principles:

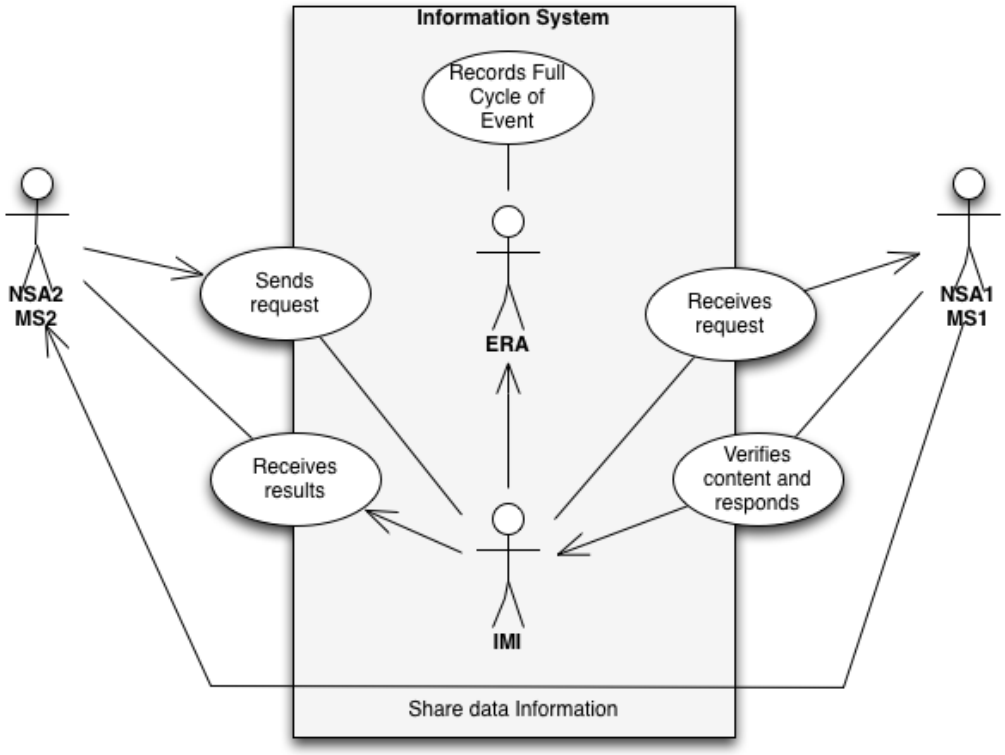
- ERA is informed of the nature of transactions and the result, but not the data of the information itself
- Involved parties will be hosting their data and communicate them to the requesting authority
- Data storage implies respect of the privacy policies according to EC's directives
- Messaging / Exchanging from an authority to another, of information involves an electronic system
- All users of the system are having specific credentials to access any part of it
- The Model of Use-Cases' transaction is alike to all classes since the actors remain the same as also the nature of requests

Use-Case Example Class #1

Use Case Class #1
Scenario: NSA2 of MS2 requests information from NSA1 of MS2

Actors Involved:
- NSA1 MS1
- NSA2 MS2
- IMI
- ERA

Criteria:
- Requests content : TDL-Basics
- Extension of response : Small
- Frequency : Often
- Time Critical : High
- Effort Authorization : Small



Use-Case Example Class #2

Use Case Class #2
Scenario: SecF1 of MS1 requests information from NSA1 of MS1

Actors Involved:
- NSA1 MS1
- SecF1 MS1
- IMI
- ERA

Criteria:
- Requests content : NLR-Data
- Extension of response : Differing
- Frequency : Middle
- Time Critical : Low
- Effort Authorization : Very Small

Use-Case Example Class #3

Use Case Class #3
Scenario: SecF1 of MS1 requests information from RU1-1 of MS1

Actors Involved:
- RU1-1 MS1
- SecF1 MS1
- IMI
- ERA

Criteria:
- Requests content : CCR-Data
- Extension of response : Middle
- Frequency : Seldom
- Time Critical : Low
- Effort Authorization : Small

Use-Case Example Class #4

Use Case Class #4
Scenario: RU1-1 of MS1 requests information from NSA1 of MS1

Actors Involved:
- RU1-1 MS1
- NSA MS1
- IMI
- ERA

Criteria:
- Requests content : NLR-Specifics
- Extension of response : Differing
- Frequency : Seldom
- Time Critical : Low
- Effort Authorization : Middle

Use-Case Example Class #5

Use Case Class #5
Scenario: RU2-1 of MS1 requests information from NSA1 of MS1

Actors Involved:
- RU2-1 MS1
- NSA MS1
- IMI
- ERA

Criteria:
- Requests content : CCR-Specifics
- Extension of response : Large
- Frequency : Seldom
- Time Critical : Low
- Effort Authorization : Large

28.3 Use cases analysis

Operational situations concerning the consultation of National Train Driving Licences Register (NLR)

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
1.	**NSA (NSA1) seeks information submitted by another NSA (NSA 2), with as minimum: status of the licence, in the following cases:**	**TDD, Article 22.1(b) DEC17/2010, Annex I.4**	**NSA > NSA**	**RR**	**X**						
1.1	In case of accident	***TF***			**X**						
	In case of incident, near-miss or other dangerous occurrence (e.g.: SPAD)	***TF***			**X**						
1.3	In case of inspections (on sight / on site)1 : Inspection of validity	**TDD Art 29.1**			**X**						
	In case of inspections (on sight / on site)2: Check of having a license	**TDD Art 29.1**			**X**						
	In case of check (“double-give-out”)	***TF***			**X**						
	In case of audit	***TF***			**X**						

Use Case #1

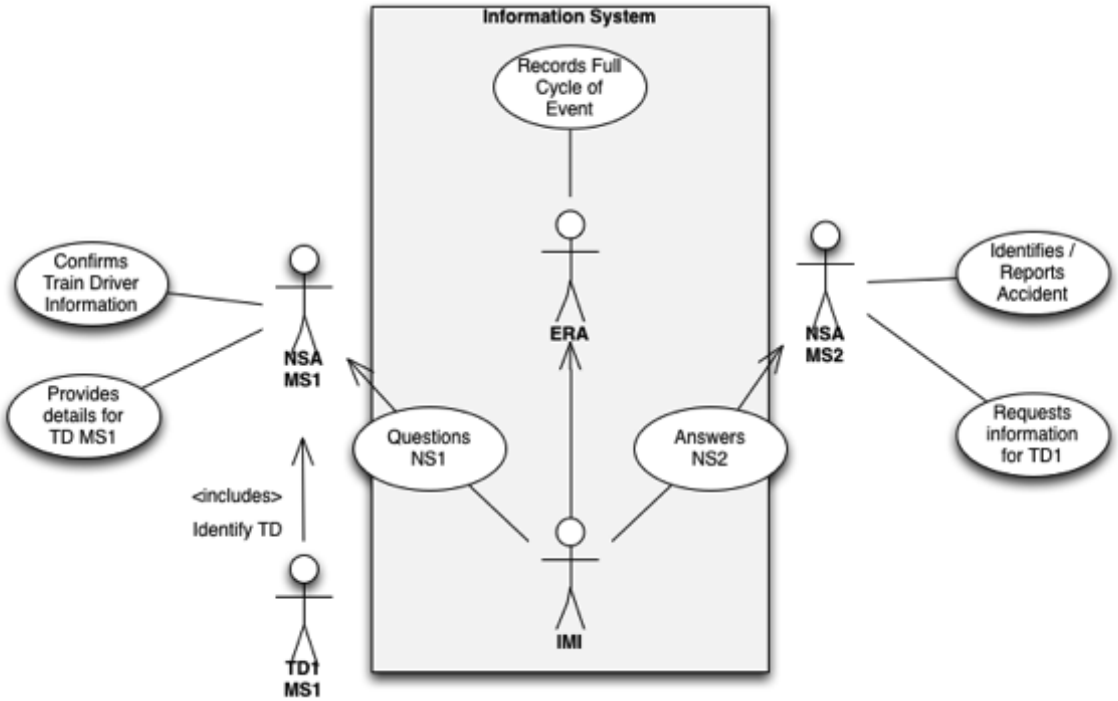
Operational situations concerning the consultation of National Train Driving Licenses Register (NLR)

Potential Actors Involved:
- NSA MS1 to MSn
- Train Driver from MS1 to MSn
- Inspectors
- Auditors
- RU or IM from MS1 to MSn
- ERA

Type of Data:
- NLR-Data
- TDL-Basics
- NLR-Personal
- NLR-Specifics
- CCR-Data
- CCR-Personal
- CCR-Specifics

Case 1.1 **NSA seeks information submitted by another NSA** (minimum: status of the license), in the following cases:

Case 1.1.1 Accident



Important arguments:

- Incident is located in NSA MS2
- NSA MS2 needs to require information about TD1 MS1 for whom NSA MS1 is responsible
- NSA MS2 enters the “system” and is posting the question to NSA MS1
- ERA is having the role of recoding and redirecting information
- IMI is transmitting messages from both NSAs and records them
- All requested Information is stored at NSA MS1 site and distributed to NSA MS2
- ERA is keeping only the records of transaction but not the information itself
- TD1 MS1 could also be part of an RU or IM therefore an additional actor would be added RU/IM MS1 holding TD1 MS1 and NSA MS1 would post the question to the specific RU/IM MS1 and not TD1 MS1

Use Case #1

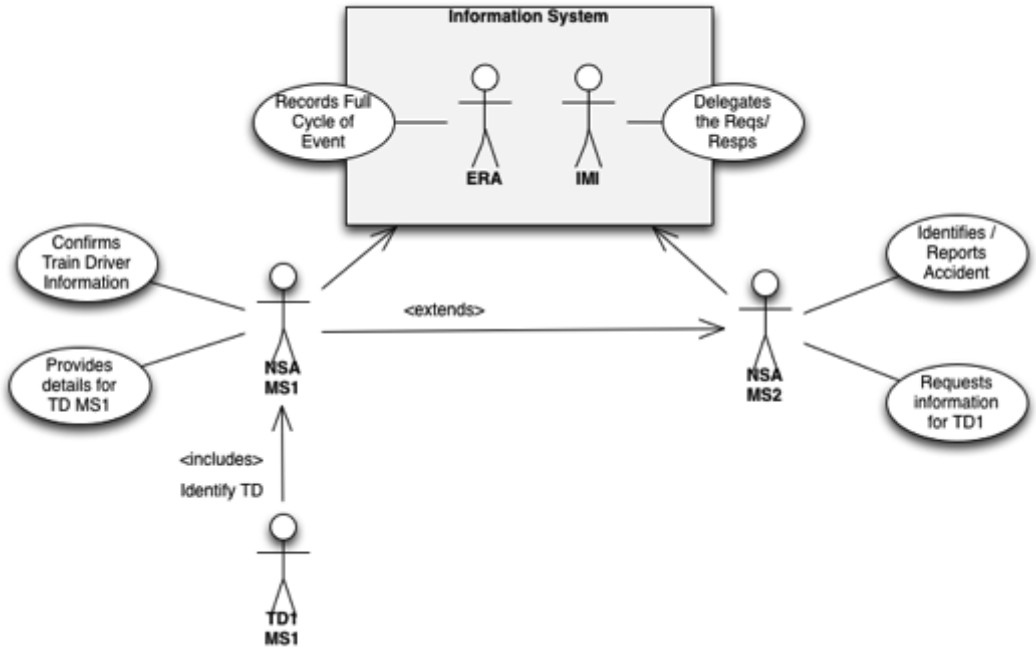
Operational situations concerning the consultation of National Train Driving Licenses Register (NLR)

Potential Actors Involved:
- NSA MS1 to MSn
- Train Driver from MS1 to MSn
- Inspectors
- Auditors
- RU or IM from MS1 to MSn
- ERA

Type of Data:
- NLR-Data
- TDL-Basics
- NLR-Personal
- NLR-Specifics
- CCR-Data
- CCR-Personal
- CCR-Specifics

Case 1.1 **NSA seeks information submitted by another NSA** (minimum: status of the license), in the following cases:

Case 1.1.1 Accident



Important arguments:

- Incident is located in NSA MS2
- NSA MS2 needs to require information about TD1 MS1 for whom NSA MS1 is responsible
- NSA MS2 posting the question directly a question to NSA MS1 out of the "system" but with other means, either provided by NSA MS1 or via email
- All requested Information is stored at NSA MS1 site and distributed to NSA MS2
- TD1 MS1 could also be part of an RU or IM therefore an additional actor would be added RU/IM MS1 holding TD1 MS1 and NSA MS1 would post the question to the specific RU/IM MS1 and not TD1 MS1
- ERA is keeping only the records of transaction but not the information itself after NSA MS1 and NSA MS2 enter the "system" and report both the incident and their reaction. Actual information is not stored by ERA but only the transaction and it's nature
- IMI is the responsible for the delegation of the requests and appointing them to correct NSA

Use Case #1

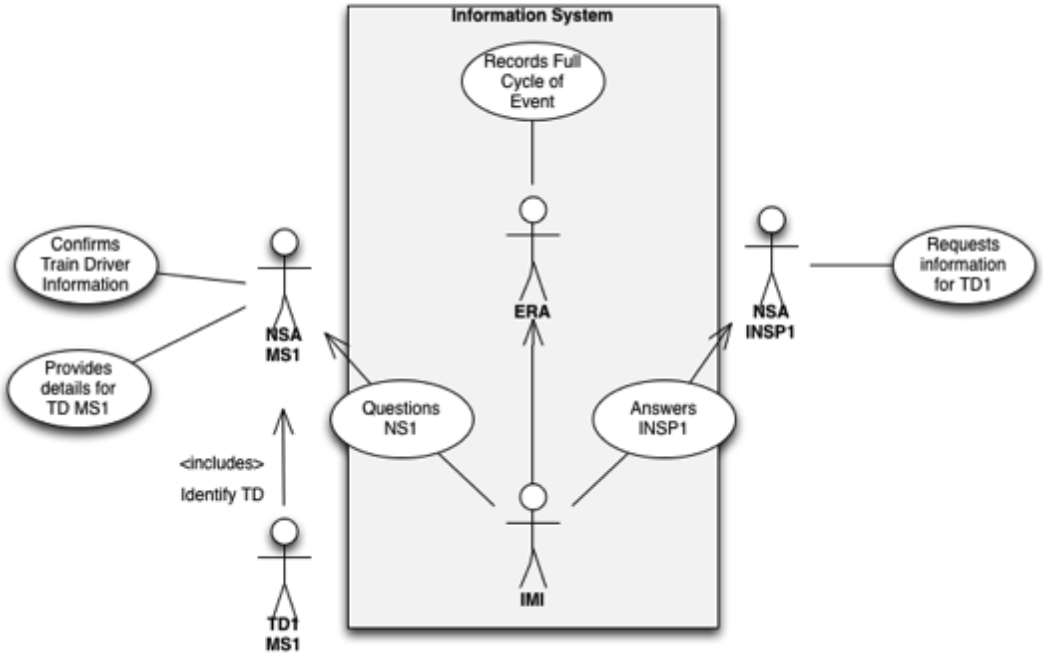
Operational situations concerning the consultation of National Train Driving Licenses Register (NLR)

Potential Actors Involved:
- NSA MS1 to MSn
- Train Driver from MS1 to MSn
- Inspectors
- Auditors
- RU or IM from MS1 to MSn
- ERA

Type of Data:
- NLR-Data
- TDL-Basics
- NLR-Personal
- NLR-Specifics
- CCR-Data
- CCR-Personal
- CCR-Specifics

Case 1.1 **NSA seeks information submitted by another NSA** (minimum: status of the license), in the following cases:

Case 1.1.1 inspections (on sight / on site)1 : Inspection of validity



Important arguments:

- Incident is located in MS2
- INSP1 at MS2 needs to require information about TD1 MS1 for whom NSA MS1 is responsible
- INSP1 enters the “system” and is posting the question to NSA MS1
- ERA is having the role of recoding and redirecting information
- All requested Information is stored at NSA MS1 site and distributed to INSP1
- ERA is keeping only the records of transaction but not the information itself
- TD1 MS1 could also be part of an RU or IM therefore an additional actor would be added RU/IM MS1 holding TD1 MS1 and NSA MS1 would post the question to the specific RU/IM MS1 and not TD1 MS1
- IMI is the responsible for the delegation of the requests and appointing them to correct NSA via the extend system

Use Case #2

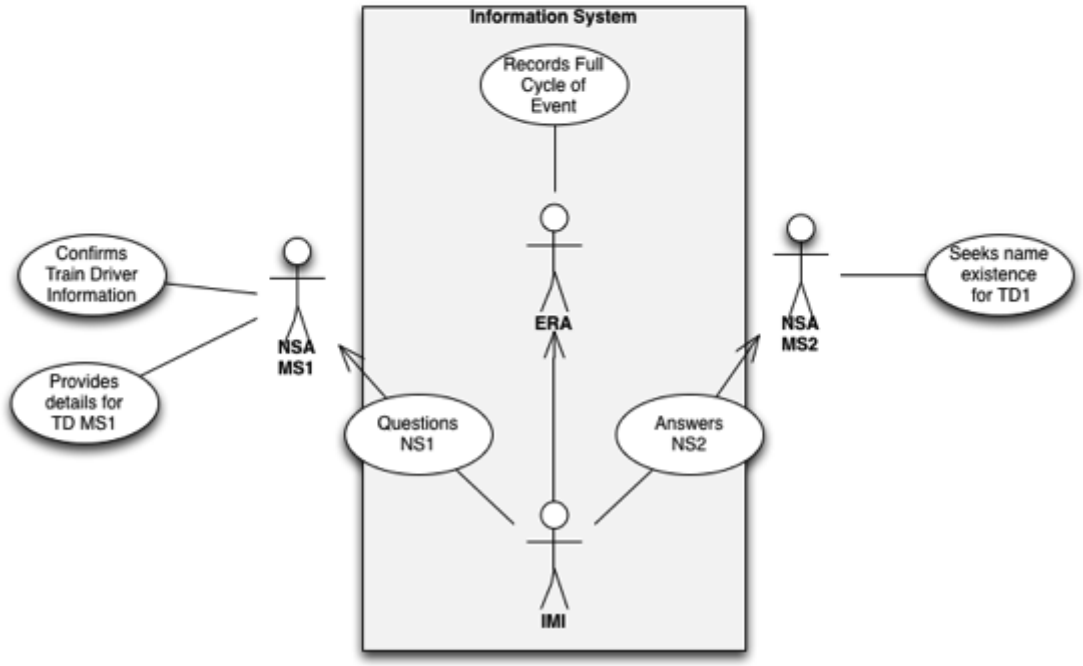
NSA seeks information submitted by NSA others

Potential Actors Involved:
- NSA MS1 to MSn
- Train Driver from MS1 to MSn
- Inspectors
- Auditors
- RU or IM from MS1 to MSn
- ERA

Type of Data:
- NLR-Data
- TDL-Basics
- NLR-Personal
- NLR-Specifics
- CCR-Data
- CCR-Personal
- CCR-Specifics

Case 2.1 **NSA seeks information submitted by another NSA**

Checking the existence of a name in their database



Important arguments:

- Incident is located in MS2
- INSP1 at MS2 needs to require information about TD1 MS1 for whom NSA MS1 is responsible
- INSP1 enters the “system” and is posting the question to NSA MS1
- ERA is having the role of recoding and redirecting information
- All requested Information is stored at NSA MS1 site and distributed to INSP1
- ERA is keeping only the records of transaction but not the information itself
- TD1 MS1 could also be part of an RU or IM therefore an additional actor would be added RU/IM MS1 holding TD1 MS1 and NSA MS1 would post the question to the specific RU/IM MS1 and not TD1 MS1
- IMI is the responsible for the delegation of the requests and appointing them to correct NSA

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
2.	**NSA passes on information to the requesting NSA**	**TDD, Article 22.1 (b)**	**NSA < NSA**			**X**					
3.	**NSA seeks information submitted by NSA_n others:**										
	Checking the existence of a name in their database	***TF***	**NSA >NSAs**		**X**						

Use Case #2

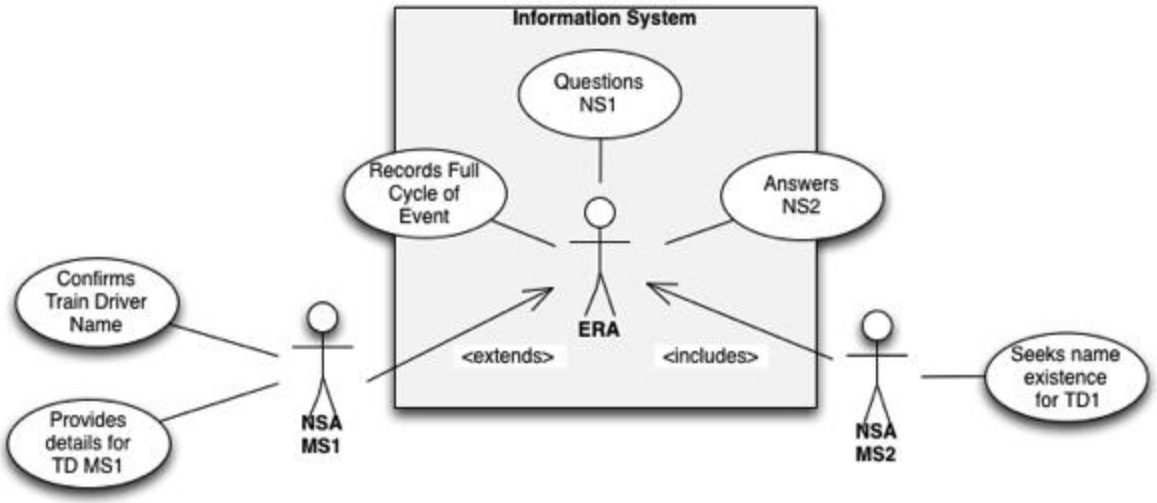
NSA seeks information submitted by NSA others

Potential Actors Involved:
- NSA MS1 to MSn
- Train Driver from MS1 to MSn
- Inspectors
- Auditors
- RU or IM from MS1 to MSn
- ERA

Type of Data:
- NLR-Data
- TDL-Basics
- NLR-Personal
- NLR-Specifics
- CCR-Data
- CCR-Personal
- CCR-Specifics

Case 2.1 **NSA seeks information submitted by another NSA**

Checking the existence of a name in their database



Important arguments:

- Request of TD name existence from NSA located in MS2
- ERA is having the role of recoding and redirecting information
- All requested Information is stored at NSA MS1 site and distributed to NSA MS2
- ERA is keeping only the records of transaction but not the information itself
- TD1 MS1 could also be part of an RU or IM therefore an additional actor would be added RU/IM MS1 holding TD1 MS1 and NSA MS1 would post the question to the specific RU/IM MS1 and not TD1 MS1

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
4.	**NSA_n informs the requesting NSA**										
	Result of the checking	*TF*	NSA >NSAs			x			x		
5.	**NSA delivers information to employers of drivers (RU/IM or others) for TDL issued by the same NSA**										
	Information of reasoned decision on suspension of a TDL and indication of the procedure to be followed for recovering the licence	TDD Article 29.4 (a)	NSA >E	R			x		x		
6.	**NSA informs the driver**										
	Information of reasoned decision on suspension of a TDL and indication of the procedure to be followed for recovering the licence	TDD Article 29.4 (a)	NSA >TD	R			x		x		

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
7.	**NSA passes on information to NSA where the licence was issued + all other NSAs**										
	Requesting further inspection to the NSA that issued the licence	TDD Article 29.4 (b)	NSA>NSA	RR	x		x		X		
	Informs the NSA having issued the licence that a TDL is suspended	TDD Article 29.4 (b)	NSA>NSAs				x		x		
8.	**NSA passes on information to NSA requesting further inspection+ all other NSAs**										
	Notification of its decision (after request of further investigation)	TDD Article 29.4(b)	NSA >NSAs				x	x	x		Article 29.4 (b) foresees max. four weeks for decision
9.	**NSA passes on information to all other NSAs**										
	Decision after request of further investigation	TDD Article 29.4 (b)	NSA>NSAs				x	x			
	Notification of its decision to prohibit the train drivers from operating in its area of jurisdiction, pending the report of the body issuing a complementary certificate	TDD Article 29.4(c)	NSA >NSAs				x		x		Article 29.4 (b) foresees max. four weeks for decision

	Notification of withdrawn licences?								x		
	…(other to be proposed by the TF)										

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
10	**NSA passes on information to the EC**										
	Information of having requested further inspection on a licence issued by a NSA of another MS	TDD Article 29.4 (b)	NSA >EC				x	X			
	A licence issued by a NSA of another MS is suspended	TDD Article 29.4 (b)	NSA >EC				x	X			
	The NSA having issued the TDL notifies its decision	TDD Article 29.4 (b)	NSA >EC				x	X			
	Notification of its decision to prohibit the train drivers from operating in its area of jurisdiction, pending the report of the body issuing a	TDD Article 29.4(c)	NSA >EC				x	X			

	complementary certificate										
11	**ERA seeks information to an NSA for monitoring**	**DEC17/2010, Annex I.4**	**ERA>NSA**	**RR**	**x**			**X**			
12	**NSA passes on information to ERA for monitoring**	**DEC17/2010, Annex I.4**	**NSA>ERA**			**x**		**X**			
13	**ERA seeks information to NSAs for monitoring**	**DEC17/2010, Annex I.4**	**ERA>NSAs**	**RR**	**x**			**X**			
14	**NSAs pass on information to ERA for monitoring**	**DEC17/2010, Annex I.4**	**NSAs>ERA**			**x**		**X**			

	Operational situations	Legal reference	Code for relation	Type of access/ request	Type of action (R) Request	Type of action (A) Answer	Type of action (INA) Inform Notify Alert	Time critical Low	Time critical Med	Time critical High	When time critical=High explain the reason
15	**Employer of train drivers (other than RU/IM) seeks information submitted by one NSA**										
	Status of the licence	DEC17/2010, Annex I.4	E>NSA	RR	x				X		
16	**RU/IM seeks information submitted by one NSA**										
	Status of the licence	DEC17/2010, Annex I.4	RU/IM>NSA	RR	x				X		
17	**NSA passes on information to employer of train drivers, (including RUs/IMs)**										
	Status of the licence	DEC17/2010, Annex I.4	NSA>E			x			X		
18	**Train Driver seeks information on own data**										
	No limit is indicated for this item	TDD Art. 22.3	TD>NSA	R	x			X			
19	**NSA passes on information to train driver**										
	No limit is indicated for this item	TDD Art. 22.3	NSA>TD			x		x			

20	**National Investigation Bodies seeks information**										
	No limit is indicated for this item	TDD Art. 22.3	NIB>NSA		x				x		
21	**NSA passes on information to NIB**										
	No limit is indicated for this item	TDD Art. 2.3	NSA>NIB			x					

2.1) Operational situations concerning the consultation of Complementary Certificates Register (CCR)

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
22	**NSA seeks information submitted by RU/IM:**										
	No limit to information in the CCR is provided.	DEC17/2010, Annex II.4	NSA >RU/IM		x				X		
23	**RU/IM passes on information to the requesting NSA**										
	No limit to information in the CCR is provided.	TDD, Article 22.2(b)	RU/IM > NSA			x			x		

	Operational situations	Legal reference	Code for relation		Type of action			Time critical			When time critical=High explain the reason
				Type of access/ request	(R) Request	(A) Answer	(INA) Inform Notify Alert	Low	Med	High	
24	**NSA where a TD operates(NSA 2), seeks information on a CC, submitted by RU/IM in another Member State:** • **directly to the RU/IM or** • **via the NSA where the RU is resident**	**TDD, Article 22.2(c)** **+** **DEC17/2010, Annex II.4**	**NSA2 >RU** **or** **NSA2>NSA1 >RU**	**-**			**X**				
	In case of accident	***TF***			**X**						
	In case of incident, near-miss or other dangerous occurrence (e.g.: SPAD)	***TF***			**X**						
	In case of inspections (on sight / on site)1 : Inspection of validity	TDD Art 29.1			**X**						
	In case of inspections (on sight / on site)2: Check of having a license	TDD Art 29.1			**X**						
	In case of check (“double-give-out”)	***TF***			**X**						
	In case of audit	***TF***			**X**						
	…										

	…										
25	**RU/IM passes on information directly to the NSA2 requesting the information or via the NSA where the RU is resident**		**RU/IM>NSA 2** **Or** **RU/IM>NSA >NSA2**			**X**					

	Operational situations	**Legal reference**	**Code for relation**		**Type of action**			**Time critical**			**When time critical=High explain the reason**
				Type of access/ request	**(R) Request**	**(A) Answer**	**(INA) Inform Notify Alert**	**Low**	**Med**	**High**	
26	**Train drivers seeks for information on CC**	**TDD Article 22.3**	**TD>RU/IM**		**x(*)**						
								X			
27	**RU/IM seeks information submitted by RU/IM other (?)**	***TF***	**RU/IM> RU/IM**		**X**						

28	**RU/IM provides information to another RU/IM**	***TF***	**RU/IM< RU/IM**								

(*) Data shall be provided in paper

29 Annex 15: Use-Cases concept data

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

Assumed: at least in one MS the NLR and the CCRs are <u>not</u> in/at the same Responding Register-Localisation

► **Principle Tasks:**
- Control, infilling and corrections.
- Analysis of each constellation under the given criteria
- Discovery of conjunctions among the results in the different tables, which promise effective solutions and perhaps benefits

(I.) **All Potential Participants** for Requests and Responses

Participants (in the point of view of MS-1)	**Potential Requester**	**Potential Responder**
NSA MS-1	yes	yes
TrainDriver MS-1 with TDL of MS-1	yes	no
Sec.Forces etc. of MS-1	yes	no
RU/IM MS-1	yes	yes
NSA MS-other	yes	yes
TrainDriver MS-other with TDL of MS-1	yes	no
Sec.Forces etc.MS-other	yes	no
RU/IM MS-other	yes	yes
ERA	yes	yes
All other Persons or Organisations	forbidden	not included

Verifiability of a Requester*	**Reasonability of their Requests**	
self-evident	self-evident to all data	
with his application for TDL	given to all of his data	
(given, way is to clarify)	given as authority to all data	
problematic	in single cases to specific data only	+
given as NSA	given as authority to all data	
with his application for TDL	given to all of his data	
(given, way is to clarify)	given as authority to all data	
very problematic	in single cases to specific data only	#
given	given as authority to all data	

*see Table (V.)

► **Tasks:** …

► **Résumés:** …

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(II.) **Types of Data-Fields** for Requests (Possible Requested Contents)

Types	**Definition**	**Explanation**	**Candidates for Request**	**Quantity of Response**	**Frequency**	**Time-Criticalness**	**Efforts for Authorisation***	
"NLR-Data"	Lic.Reg.-Data	whole data of a Nat.Lic.-Register (NLR) of a NSA	NSAs, Sec.Forces	differing	…..	low	small	
"TDL-Basics"	Basic Data of Licence itself only	all data, printed on the frontispiece of licence (part of NLR-Data)	NSAs, Sec.Forces	**small**	…..	**high**	**small**	
"NLR-Personal"	Individual Personal Data	for a Train Driver, all of his individual data in a NLR (part of NLR-Data)	Train Drivers (TD)	one data-set		low	small	
"NLR-Specifics"	Restricted Data	specific data, one RU/IM is authorised to know (part of NLR-Data)	RUs/IMs	differing	…..	low	**very large**	+
"CCR-Data"	Certif.Reg.Data	whole data from a CC-Register of an undertaking	NSAs, Sec.Forces	differing	…..	low	small	
"CCR-Personal"	Individual Personal Data	for a Train Driver, all of his individual data in a CCR (part of CCR-Data)	Train Drivers	one data-set		low	small	
"CCR-Specifics"	Restricted Data	specific data, another RU/IM is authorised to know (part of CCR-Data)	RUs/IMs	differing	…..	low	**very large**	+

* … for the "Candidates for Requests" (see column left)

► **Tasks:** **…**

► **Résumés:** **…**

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(III.) **All Potential Request-Combinations.** – Matrix shows: Requesters vs. Requested Contents

Requester	Requested **TDL-Nr.-Sign …**	**Owner of Register / Register-Location**	**Requested Contents**	**Quantity of Response**	**Frequency**	**Time-Criticalness**	**Efforts for (prior) Authorisation**	**Permissibility of Requests**	
NSA MS-1 itself	of MS-1	NSA MS-1	TDL-Basics	small	…..	high	self-evident	self-evident	
- " - itself	of MS-1	NSA MS-1	NLR-Data	differing	…..	low	self-evident	self-evident	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	differing	…..	low	very small	self-evident	
TrainDriver himself	of MS-1	NSA MS-1	NLR-Data	differing	…..	low	very small	own data	
- " - himself	of MS-1	RU/IM-11 MS-1	CCR-Data	differing	…..	low	very small	own data	
- " - himself	of MS-1	RU/IM-**12** MS-**1**	CCR-Data	differing	…..	low	very small	own data	
- " - himself	of MS-1	RU/IM-**21** MS-**2**	CCR-Data	differing	…..	low	very small	own data	
Sec.Forces etc. MS-1	of MS-1	NSA MS-1	TDL-Basics	small	…..	high	installed: v.small	total	
- " -	of MS-1	NSA MS-1	NLR-Data	differing	…..	low	installed: v.small	total	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	differing	…..	low	middle	total	
RU/IM-11 MS-1	of MS-1	NSA MS-1	NLR-Specifics	differing	…..	low	large	partial	
- " - itself	of MS-1	RU/IM-11 MS-1	CCR-Data	differing	…..	low	self-evident	self-evident	
- " -	of MS-1	RU/IM-**12** MS-**1**	CCR-Specifics	differing	…..	low	large	**problematic**	+
NSA MS-2	of MS-1	NSA MS-1	TDL-Basics	small	…..	high	very small	total	
- " -	of MS-1	NSA MS-1	NLR-Data	differing	…..	low	very small	total	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	differing	…..	low	small	total	
Sec.Forces etc. MS-2	of MS-1	NSA MS-1	TDL-Basics	small	…..	high	installed: v.small	total	
- " -	of MS-1	NSA MS-1	NLR-Data	differing	…..	low	installed: v.small	total	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	differing	…..	low	middle	total	
RU/IM-21 MS-2	of MS-1	NSA MS-1	NLR-Specifics	differing	…..	low	**very large**	partial	+
- " -	of MS-1	RU/IM-11 MS-1	CCR-Specifics	differing	…..	low	**very large**	**problematic**	++
NSA MS-3	of MS-**2**	RU/IM-11 of MS-**1** via 1. NSA MS-**2** via 2. NSA MS-1 (?)*	CCR-Data	differing	…..	low	small	total	
Sec.Forces etc. MS-3	of MS-**2**	RU/IM-11 of MS-**1** via 1. NSA MS-**2** via 2. NSA MS-1 (?)*	CCR-Data	differing	…..	low	middle	total	
RU/IM-31 MS-3	of MS-**2**	RU/IM-11 of MS-**1** via 1. NSA MS-**2** via 2. NSA MS-1 (?)*	CCR-Specifics	differing	…..	low	**very large**	**problematic**	++

* see Table (VII.)

► **Tasks:** Control, corrections and additions.

► **Résumés:** **…**

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(IV.a) **Situations / Cases of Requests** (see: basing on **TaskForce-Discussion of February, 29th**)

Cases	**…**	**Frequency**	**Time-Criticalness**	**Extension of Response**	**required/ useful**	**according to 2007/59/EU**	**Candidates for Request**	**Effort for prior Preparation of their Authoris.**
accident	…..	very small	…..		required	§ 29	…..	…..
incident (e.q. spads)	…..	small	…..		required	§ 29	…..	…..
inspection (on sight)	…..	small	time-crit. (?)		required	§ 29	…..	…..
audit	…..	large	…..		…..	Annex	…..	…..
check (“double-give-out”)	…..	large	…..		useful	…..	…..	…..
inform of involved licence (incl. suspection)	…..	…..	…..		required	…..	…..	…..

(IV.b) **Situations / Cases of Requests** (see: **"Feasibility Study", Version 1-0.3.3.** of 12.3.2012, § 4.3)

Questions on the current state of your NLR	**Frequency**	**Time**	**…**	**Required**	**…**
1. Inform of validity of license					
a. Accidents	Low	Low	…..	Yes	…..
b. Incidents	Low	Low	…..	Yes	…..
c. Inspection on sight					
i. Inspection of validity	High	Critical	…..	Yes	…..
ii. Check of having a license	High	Medium	…..	Yes	…..
d. Audits	High	Critical	…..	Yes	…..
e. Application phase	High	Medium	…..	No	…..
f. Check “double give out”	Medium	Medium	…..	Yes	…..
2. Inform of license’s invalidity	High	Critical	…..	Yes	…..

► **Tasks:** Fill-out and additions.
Extension with further situations for and cases of (reasoned) requests; including all potential participants (s. table I.)
Prove all potential request/response-combinations for realistic cases (s. table III.)
Include the different types of data for requests (s. table II.)
Include considerations about authorisations (s. table V. and VI.)

► **Résumés:** **…**

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(V.) Management of **Verification, Identification and Authentification**

All procedures of Interoperable Systems based on medial* structures only. This demands a physical/real or factual inspection (here marked as "Verification") additionally.
Therefore three ranges (A) of **existential entities** and (B) of **right entities** are to bring in compliance with each other:

(A.) The **existential entities**: A person/institution ask under his name for **login-code** to the register. So an administrator has to do:			
1. Verification	it's: correlation among the medial person/institution* and the real person/institution	This is to clarify for each pers./inst., that he/it is real/physical one, he/it says he/it is.	#
2. Identification	it's: correlation among the medial pers./int.and the characteristic code** of them	After Verification person/institution his/its account can be given by an Register-Admin	
3. Authentification	it's: correlation among the real pers./inst.on and the characteristic code of them	After Identification a person/institution can log in an system via his/its code	

*medial person/institution: person/institution only known by letter, phone, mail, website, … **characteristic code: "user name" and "password"

(B.) The **right-entities**: A person/institution ask for **access-rights to data** in the register. So an administrator has to do:			
1. Verification	it's: correlation among the requested range an the factual legitimated access-range	To clarify for each pers./inst. the access-rights for which parts of whose data-set	#
2. Identification	it's: correlation among the factual access-range and the given access-rights	After Verification each pers./inst. can allocate to his/its data by an Register-Admin	
3. Authentification	it's given with the characteristic code	After Identification a person/institution can access to his/its data via his/its code.	

► **Résumés:**
(A.2.) and (A.3.), (B.2.) and (B.3.) are answered till today only.
Point (B.1.) isn't answered, because the concept of roles is orientated at the characteristics of the requesters, but not at the data-sets.
The **verification** as essential point for legitimation (A.1.) is not even mentioned, much less treated.
Verification procedures are not necessary for Train Drivers itself, ERA, NSAs, or limited necessary for Sec. Forces.
But verification procedures are necessary for the cooperation with RUs/IMs!
A verification of RUs/IMs on principle is factual not to realise or with a maximum of efforts only. But a lot of verifications must be realised by each MS anew and Europe-wide.
Possible solution: one Register of all RUs/IMs Europe-wide. This register is to prepare with their verifications. So it includes their identifications automatically.
Solution for an individualisation of data-set-groups and their

► **Tasks:**
To A.: Development of a **RU/IM-Register Europe-wide**.
To B.: 1. Identifying of specific data-ranges, RUs/IMs can give access orderly. Perhaps: the data-clusters are so individual, that no systematic grouping will be possible
2. Solutions for (a) a RU/IM-specific/individual fractionation of the data-sets (b) profiling the specific/individual access-rights of RUs/IMs to the fractions of data-sets.

► **Further Résumés:** **…**

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(VI.) Efforts of **Authorisation of a Requester**

Requester	Requested **TDL-Nr.**	**Owner of Register / Register-Location**	**Requested Data Range**	**Way of Verification***	**Way of Identification***	**Effort of Verification**	**Effort of Identification**	**Effort of futher Maintenance**	**Eff., connecting rights to data**	
NSA MS-1 itself	of MS-1	NSA MS-1	NLR-Data	in-house	in-house	self-evident	self-evident	self-evident	self-evident	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	simple	simple	small	small	small	very small	
TrainDriver himself	of MS-1	NSA MS-1	NLR-Data	is verified	is identified	very small	very small	very small	small	
- " - himself	of MS-1	RU/IM-11 MS-1	CCR-Data	is verified	is identified	very small	very small	very small	small	
- " - himself	of MS-1	RU/IM-**12** MS-**1**	CCR-Data	is verified	is identified	very small	very small	very small	small	
- " - himself	of MS-1	RU/IM-**21** MS-**2**	CCR-Data	is verified	is identified	very small	very small	very small	small	
Sec.Forces etc. MS-1	of MS-1	NSA MS-1	NLR-Data	1 time only	1 time only	1 time only	1 time only	small/middle	very small	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	-?-	-?-	small	small	middle	very small	
RU/IM-11 MS-1	of MS-1	NSA MS-1	NLR-Specifics	-?-	-?-	prob. large	prob. large	large	**large**	+
- " - itself	of MS-1	RU/IM-11 MS-1	CCR-Data	in-house	in-house	self-evident	self-evident	self-evident	self-evident	
- " -	of MS-1	RU/IM-**12** MS-1	CCR-Specifics	-?-	-?-	prob. large	prob. large	prob. large	**large**	+
NSA MS-2	of MS-1	NSA MS-1	NLR-Data	simple	simple	very small	very small	very small	very small	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	via NSA MS-1?	via NSA MS-1?	small	small	small	very small	
Sec.Forces etc. MS-2	of MS-1	NSA MS-1	NLR-Data	1 time only	1 time only	1 time only	1 time only	small/middle	very small	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	via NSA MS-1?	via NSA MS-1?	1 time only	1 time only	middle	very small	
RU/IM-21 MS-2	of MS-1	NSA MS-1	NLR-Specifics	-?-	-?-	prob. very large	prob. very large	prob. very large	**very large**	#
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	difficult (s.above) via NSA MS-1?	difficult (s.above) via NSA MS-1?	prob. very large	prob. very large	prob. very large	**very large**	#
NSA MS-3	of MS-**2**	RU/IM-11 MS-**1** via NSA MS-**2**	CCR-Data	-?-: via NSA MS-2, then NSA MS-1?	via NSA MS-2, then NSA MS-1?	very small	very small	very small	very small	
Sec.Forces etc. MS-3	of MS-**2**	RU/IM-11 MS-**1** via NSA MS-**2**	CCR-Data	-?-: via NSA MS-2, then NSA MS-1?	via NSA MS-2, then NSA MS-1?	1 time only	1 time only	middle	very small	
RU/IM-31 MS-3	of MS-**2**	RU/IM-11 MS-**1** via NSA MS-**2**	CCR-Specifics	via NSA MS-2, then NSA MS-1: very difficult (s.above)	via NSA MS-2, then NSA MS-1 difficult (s.above)	prob. very large	prob. very large	prob. very large	**very large**	#

* Verification, Identification: see Table (V.)

► **Tasks:** Control, infilling and corrections.
For each constellation: search for scenarios/cases-of-request, to enhance and enrich the tables IV.
Combination with table III., looking for conjunctions.

► **Résumés:** **…**
finally: development of **cost-benefit-considerations of the practice of the work-flows**, connected with the other matrices.

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(VII.) **All Possible Work-Flow-Runs of Requests.** - Request-Response-Pathways (Assumed: all requests managed by an ERA-platform)

Requester	Requested **TDL-Nr.**	**Respondent Register-Location**	**Requested Data Range**	**Request-Pathway**	**Answer-Pathway**	**Path Automation**	
NSA MS-1 itself	of MS-1	NSA MS-1	TDL-Basics	NSA1 → NLR1	directly	self-evident	
- " - itself	of MS-1	NSA MS-1	NLR-Data	NSA1 → NLR1	directly	self-evident	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	NSA1 → ERA → CCR11	via ERA ?	easy	
TrainDriver himself	of MS-1	NSA MS-1	NLR-Data	TD11 → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	TD11 → ERA → CCR11	via ERA ?	easy	
Sec.Forces etc. MS-1	of MS-1	NSA MS-1	TDL-Basics	Sec.F.11 → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	NSA MS-1	NLR-Data	Sec.F.11 → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	Sec.F.11 → ERA → NLR1 → CCR11	via ERA ?	easy	
RU/IM-11 MS-1	of MS-1	NSA MS-1	NLR-Specifics	RU11 → ERA → NLR1	via ERA ?	easy	
- " - itself	of MS-1	RU/IM-11 MS-1	CCR-Data	RU11 → CCR11	directly	self-evident	
- " -	of MS-1	RU/IM-1**2** MS-1	CCR-Data	RU11 → ERA → CCR12	via ERA ?	easy	
NSA MS-2	of MS-1	NSA MS-1	TDL-Basics	NSA2 → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	NSA MS-1	NLR-Data	NSA2 → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	NSA2 → ERA → NSA1 → (ERA ?) → CCR11	via ERA ?	middle	
Sec.Forces etc. MS-2	of MS-1	NSA MS-1	TDL-Basics	Sec.F. → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	NSA MS-1	NLR-Data	Sec.F. → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	RU/IM-11 MS-1	CCR-Data	Sec.F.21 → ERA → NSA1 → (ERA ?) → CCR11	via ERA ?	middle	
RU/IM-21 MS-2	of MS-1	NSA MS-1	NLR-Specifics	RU21 → ERA → NLR1	via ERA ?	easy	
- " -	of MS-1	RU/IM-**11** MS-1	CCR-Data	RU21 → ERA → NLR1 → (ERA ?) → CCR11	via ERA ?	middle	
NSA MS-3	of MS-**2**	RU/IM-11 of MS-**1** via NSA MS-**2**	CCR-Data	NSA3 → ERA → NLR2 → (ERA ?) → NLR1 → (ERA ??) → CCR11	directly or indirectly?	possible?	#
Sec.Forces etc. MS-3	of MS-**2**	RU/IM-11 of MS-**1** via NSA MS-**2**	CCR-Data	NSA3 → ERA → NLR2 → (ERA ?) → NLR1 → (ERA ??) → CCR11	directly or indirectly?	possible?	#
RU/IM-31 MS-3	of MS-**2**	RU/IM-11 of MS-**1** via NSA MS-**2**	CCR-Data	RU31 → ERA → NLR2 → (ERA ?) → NLR1 → (ERA ??) → CCR11	directly or indirectly?	possible?	#

► **Tasks:** Control and corrections.
Check-up of the realisability and the effort for each case
Considerations about the work-flow structure and perhaps addition of other possible work-flows
Discussion of the ERA-Transits

► **Résumés:** …

Cruxes of Feasibility + = difficult # = very difficult / perhaps insolvable ▼

(VIII.) Variations of **Expected Sorts of Registers**

Register	**Description**	**Location**	**at NSAs**	**at RUs/IMs**	**expected quantity of RUs/IMs**	**…**	**Automation**	
Paper-based		Card Index	no	possible/allowed	…..		impossible	#
Simply Electronic		Workstation	only beginning	small RUs/IMs	…..		difficult	+
Database (Stand alone)		Workstation	only beginning	small RUs/IMs	…..		difficult	+
Database (IntraNet)		Network	final standard	great RUs/IMs	…..		possible	

► **Tasks:** Control and additions.
Consider in each constellation: the needed effort of an undertaking for a (higher level) data-security-system.
Search of those kinds of information systems, which can guarantee the inclusion of all sorts of allowed registers.

► **Résumés:** **…**

(IX.) Restrictions of MSs in **Handling of Personal Data** #

Member State		**Allowing Storage of Pers. Data externally (in EU)**	**Allowing Delive-ring of Pers. Data externally (in EU)**	**Other Restrictions 1**	**Other Restrictions 2**	**Other Restrictions 3**	**…**	**Formalized Minimum Standards**
Belgium		…..	…..	…..	…..			…..
Bulgaria		…..	…..	…..	…..			…..
Denmark		…..	…..	…..	…..			…..
…..		…..	…..	…..	…..			…..
…..		…..	…..	…..	…..			…..
…..		…..	…..	…..	…..			…..
…..		…..	…..	…..	…..			…..

► **Tasks:** Clarify the questions, which are asked in the text
Explore the law situations and fill up.

► **Résumés:** **…**

- END OF DOCUMENT -