



ISA ACCESS TO BASE REGISTRIES

D 2.1 Report on Analysis and Assessment

JOINING UP GOVERNMENTS



This report / paper was prepared for the ISA programme by:

Author's name: Deloitte Consulting CVBA

Company's name: Deloitte Consulting CVBA

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the ISA website:

<http://ec.europa.eu/isa>

TABLE OF CONTENT

1. EXECUTIVE SUMMARY	5
2. INTRODUCTION	7
2.1 STUDY OBJECTIVES AND APPROACH.....	7
2.2 STRUCTURE OF THIS DOCUMENT	7
3. BASE REGISTRIES INTEROPERABILITY MODEL	8
3.1 EUROPEAN INTEROPERABILITY FRAMEWORK.....	8
3.2 THE BASE REGISTRIES INTEROPERABILITY MODEL	11
4. RESULTS OF THE SURVEY	25
4.1 DISCLAIMER	25
4.2 SURVEY SAMPLE	25
4.3 SURVEY RESULTS PER LEVEL AND SECURITY DIMENSION	27
4.3.1 <i>Legal level</i>	29
4.3.2 <i>Organisational level</i>	33
4.3.3 <i>Semantic level</i>	36
4.3.4 <i>Technology level</i>	38
4.3.5 <i>Security dimension</i>	43
4.3.6 <i>Summary of results per level and the security dimension</i>	47
4.4 SURVEY RESULTS PER TYPE OF BASE REGISTRY	50
4.4.1 <i>Business Registries</i>	50
4.4.2 <i>Citizen registries</i>	59
4.4.3 <i>Summary of results per type</i>	66
5. BASE REGISTRIES' BEST PRACTICES	68
5.1 BEST PRACTICES PER LEVEL AND THE SECURITY DOMAIN.....	68
5.1.1 <i>Legal level</i>	68
5.1.2 <i>Organisational level</i>	72
5.1.3 <i>Semantic level</i>	72
5.1.4 <i>Technical level</i>	73
5.1.4 <i>Security dimension</i>	74
6. LIFE EVENTS	77
6.1 LIFE EVENT DEFINITION.....	77
6.2 LIFE EVENT SCENARIOS.....	78
6.2.1 <i>Moving to another country</i>	78
6.2.2 <i>Starting a new business</i>	80

6.2.3	<i>Buying a property</i>	82
6.2.4	<i>Addressing speeding tickets</i>	84
6.2.5	<i>Doing business in another country</i>	86
7.	EU INITIATIVES RELATED TO BASE REGISTRIES	88
7.1	BUSINESS REGISTRIES.....	90
7.2	CITIZEN REGISTRIES	95
7.3	LAND REGISTRIES	98
7.4	VEHICLE REGISTRIES	99
7.5	PROCUREMENT REGISTRIES.....	100
8.	CONCLUSION	104
	ANNEX 1: SCORING PER BASE REGISTRY	107
	ANNEX2: A DETAILED VIEW OF THE EU INITIATIVES ON INTEROPERABILITY OF BASE REGISTRIES	111

1. EXECUTIVE SUMMARY

1. The main objective of this study is to provide recommendations on the cross border interoperability of base registries. In order to do so, a base registries interoperability model was designed, based on the EIF (European Interoperability Framework) interoperability levels. The interoperability levels are: legal, organisational, semantic and technical, enriched with the security dimension.
2. In order to assess interoperability maturity within each of the four interoperability levels and the security dimension, a series of questions (aspects) was created in the model and incorporated into an online survey (for more details see “Template used for the inventory”).
3. The present report provides an analysis and assessment of the cross border interoperability maturity of base registries. A sample of 19 base registries is analysed.
4. In order to analyse the maturity of the cross border interoperability, the results of the survey were analysed using the base registries interoperability model and its scoring. In particular, within each of the interoperability levels and the security dimension, each of the aspects (topic within a level and dimension) was given a weight based on the importance in the context of cross border interoperability. In addition, each question was attributed a score (in total 1) distributed according to the contribution of the provided answer to cross border interoperability.
5. The analysis of cross border interoperability was carried out for each of the four interoperability levels and the security dimension. Findings were presented per level and for the security dimension in a quantitative approach enriched with qualitative comments. A comparison of levels was also undertaken.

The main conclusions of the analysis per level (and dimension) are:

- legal level: an overarching or specific cross border interoperability framework is required,
 - organisational level: the enhancement of transparency and further alignment of best practices is required,
 - semantic level: taxonomy alignment is required,
 - technical level: an improvement in reusability and opening up Identity and Access Management environment to work in the cross border context is needed,
 - security dimension: further alignment of best practices and need for security awareness is required.
6. The analysis is also performed per type of base registry (for business and citizen registries only given that other types of base registries are not representative enough). The main finding suggest that there are still several drawbacks within each of the interoperability levels and the security dimension for both citizen and business registries.
 7. Best practices embedded in the base registries interoperability model were used to asses the survey results. As the next step, the best practices were compared with good practices provided by information found in the survey results. The main finding is that the good practices reconfirm the observations described in the analysis per level and the security dimension.
 8. In order to put the cross border interoperability phenomenon in context, five cross border life event scenarios were applied on the survey results (one per type of base registry:

moving to another country, starting a new business, buying a property, addressing speeding tickets, doing business in another country). The main finding was that none of the scenarios presented can take place based on the “reality” of the survey results at the moment.

9. The last part of the report presents a series of the EU initiatives and an evaluation of their impact on base registries. All but one of the EU initiatives fosters cross border interoperability via legal frameworks or projects.
10. The main conclusion is that according to the survey results, the cross border interoperability of base registries faces several obstacles at all interoperability levels and within the security dimension. In order to overcome these obstacles best practices and recommendations were identified (see also “Final report”).
11. This study can be considered as a starting point of more elaborated research involving a larger and more representative sample of base registries in order to obtain an extended view on the maturity of cross border interoperability in Europe.

2. INTRODUCTION

2.1 STUDY OBJECTIVES AND APPROACH

The objective of this study is to formulate recommendations on facilitating cross border data exchange between base registries based on an interoperability maturity analysis of base registries with respect to the EIF (European Interoperability Framework) levels, enriched with the security dimension. Part of the analysis will also be a check on the interoperability of base registries against a series of cross-border life event scenarios. To conclude the analysis, European Commission (EC) initiatives related to cross-border interoperability will be mapped against the study findings and provide an evaluation of their impact.

The analysis is based on the results of an online survey. The results are analysed using a base registries interoperability model (based on the EIF). The study provides four outputs:

- a high-level analysis per EIF level (Legal, Organisation, Semantic, Technology) and the security dimension and per registry type of the survey sample;
- best practices for the interoperability of base registries, together with an insight into the minimum quality level of a base registry required to become interoperable;
- recommendations on how to foster interoperability through application of cross-border life event scenarios on chosen base registries;
- an assessment of relevant EU initiatives related to cross border interoperability of base registries and how they contribute to the interoperability maturity of base registries.

2.2 STRUCTURE OF THIS DOCUMENT

This document is the deliverable for the second phase of the ISA study on Base Registries and has the following structure:

- chapter 1 provides the executive summary;
- chapter 2 (this chapter) introduces the overall objectives of the ISA study on access to base registries and the approach used for the second phase of the study;
- chapter 3 consists of a description of the base registries interoperability model;
- chapter 4 presents the survey results;
- chapter 5 provides an overview of the best practices and related good practices found in the survey results;
- chapter 6 consists of life event scenarios in order to find gaps, issues and recommendations for base registries;
- chapter 7 provides a list of relevant EU initiatives related to interoperability and their relation to the best practices of base registries;
- chapter 8 provides an overall conclusion of this study;
- in annex, the overall scoring obtained per base registry can be found.

The document finishes with concluding remarks.

3. BASE REGISTRIES INTEROPERABILITY MODEL

3.1 EUROPEAN INTEROPERABILITY FRAMEWORK

The base registries interoperability model is based on the European Interoperability Framework (EIF), managed by the ISA programme and focused on the interoperability of the country administrations. The main objective of the EIF is to assist in the design of European public services. According to the EIF, interoperability is defined as follows:

“Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems”.

As the above definition suggests, interoperability does not limit itself to the exchange of information between ICT systems. It also focuses on cooperation between administrations that aim to work together in delivering European public services.

The base registries interoperability model takes its origins from the conceptual model for public services¹ (see Table below).

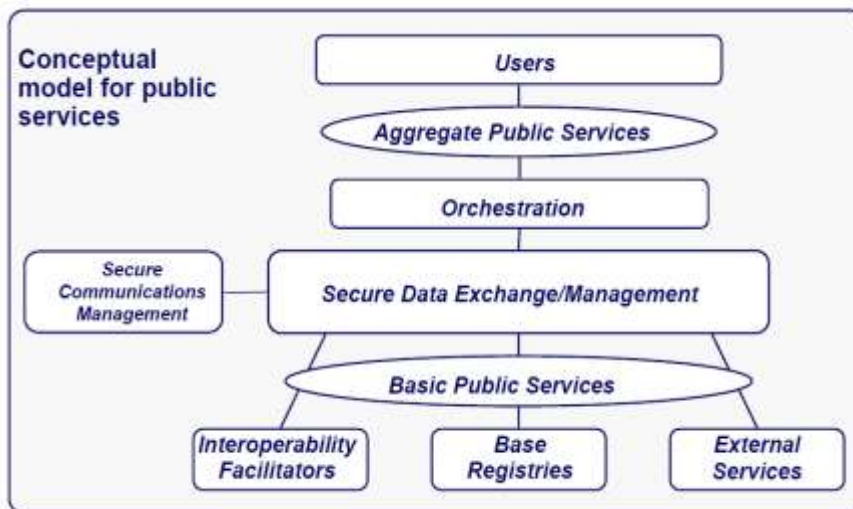


Figure 1. Conceptual model for public services (source: EIF).

¹ Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services. European Commission, Brussels, 16.12.2010 COM(2010) 744 final.

The model consists of three main parts: basic public services, secure data exchange/management and aggregate public services. This study is focused on basic public services. Basic public services include three elements used to build basic European public services: interoperability facilitators, services based on base registries and external services.

The interoperability facilitators are basic public services that can be reused to create aggregated public services. External services are the services provided by third parties. The most important component of basic public services is a set of base registries which “provide reliable sources of basic information on items such as persons, companies, vehicles, licenses, buildings, locations and roads” and “are authentic and authoritative and form, separately or in combination, the cornerstone of public services”.

The conceptual model in practice in terms of cross border interoperability needs to take into account the following four interoperability levels (the political context is left out):

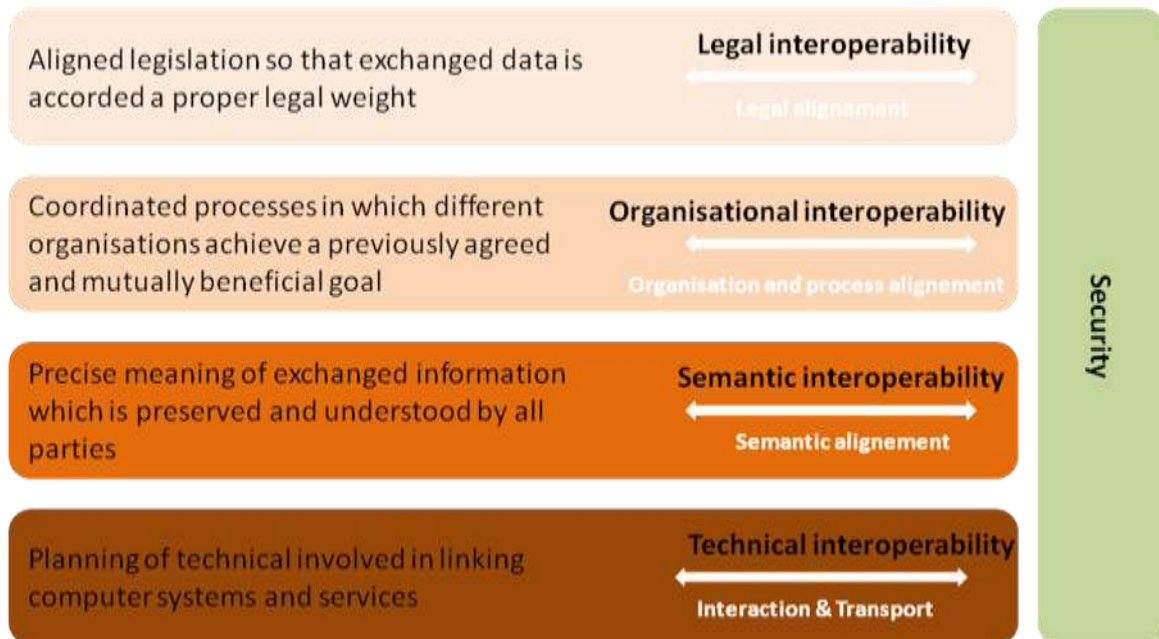


Figure 2. Interoperability levels (source: EIF).

Legal interoperability

According to the EIF, when dealing with cross border interoperability it is necessary to guarantee the legal validity of data across borders and to protect data in originating and receiving countries. The legal level is also helpful for dealing with legal divergences between national public administrations.

Organisational interoperability

This level concerns the cooperation of public administrations across countries in order to reach mutually beneficial goals. It can be done through the integration of business processes and data exchange. It also means that users need to have services which are available, identifiable and user-oriented.

Semantic interoperability

Semantic interoperability means the exchange of information that is understood. It is a challenge in the EU context because of the variety of spoken languages. To address this challenge, one needs to start with semantic interoperability assets and agreements on the meaning of the exchanged information (semantic interoperability aspect). In addition to the multilingual framework and semantic aspect, there is also a syntactic interoperability aspect that deals with the format of the exchanged information such as grammar and schemas.

Technical interoperability

The technical interoperability level refers to linking information systems by means of interface specifications, interconnection services or data integration services. There are no specifications in terms of technology for public administrations, which arises the need to follow either formalised specifications or standards.

Security and compliance

In addition to the above mentioned interoperability levels a transversal “Security” dimension is added to the model. This is due to the fact that the EIF highlights the importance of this topic (EIF version 2.0 page 15):

“Public administration should make their authentic sources of information available to others while implementing the appropriate access and control mechanism to ensure security and privacy as foreseen in the relevant legislation.”

3.2 THE BASE REGISTRIES INTEROPERABILITY MODEL

Based on the conceptual model, the interoperability levels and the security dimension described above, the base registries interoperability model was developed (based on the questionnaire as described in the deliverable “Template used for the inventory”). The high level structure of the model is presented in Figure 3.



Figure 3. The base registries interoperability model.

Measurement procedure

In order to measure each of the four interoperability levels and the security dimension, a series of criteria was defined. Each criterion was assigned a weight (10 points for each level in total) to express its importance in the context of cross border interoperability. As a next step, a series of questions were created for each criterion in order to measure it. Finally, numerical values were assigned to each question in order to assess the answers in a quantitative manner. The process of results gathering was conducted via the online survey sent to local base registry owners (for more information see section 4.2 of this document). As all questions in the survey are mandatory, it can be assumed that the respondents answered to the best of their ability to all questions. Hence, all questions are baselined at zero points (even if the answer has been considered “not applicable”) and the points are assigned according to the scoring table.

Detailed description of criteria and the scoring system for each level

For the **legal level** the following criteria were identified:

- Legal authority,
- Legal requirements on base registry access,
- Legal requirements on information quality,
- Legal requirements on information availability,
- Privacy and confidential information,
- Review of legal aspects,
- EU legislation,
- Other regulatory aspects.

The following table (Table 1) shows the details of the model structure and scoring for the legal level.

Criterion	Questions	Weight		Justification
Leg. 1: Legal authority	<p>Is there a legal basis to operate this base registry? (Y/N)</p> <p>If yes, please provide the reference to the legal foundation</p> <p>Is that legal basis also applicable to other base registries? (Y/N)</p> <p>If yes, please name the registries.</p> <p>Is your base registry legally recognised as the sole source of authentic information regarding the data it holds? (Y/N)</p> <p>At which legislative level has this legal basis been created?</p> <ul style="list-style-type: none"> at national/federal level, at regional/... level, at local level, other (please specify). 	3	<p>1: Legal basis, applicable to others, sole source at higher or equal to regional level</p> <p>0,75: Legal basis, applicable to others, no sole source at higher or equal to regional level</p> <p>0,5: Legal basis, not applicable to others, no sole source at higher or equal to regional level</p> <p>0,25: Legal basis, not applicable to others, no sole source at lower than to regional level</p> <p>0: no legal basis, not applicable to others, no sole source at lower than to regional level</p>	<p>The legal authority of a base registry is a key part of the value of a base registry and its information, hence the weight of “3”. Ideally the level of the legal framework is as high as possible, considering the legislative hierarchy in the country.</p> <p>The explicit reference in the law as sole official source is key for the trustworthiness and relevance of the base registry.</p> <p>An overarching legal framework covering multiple/all base registries indicates that these registries are already subject to the same requirements and legislative changes can be undertaken relatively easily.</p>
Leg. 2: Legal requirements on base registry access	<p>To whom should your base registry be made accessible according to the legal framework:</p> <ul style="list-style-type: none"> to the public to government entities only to parties (persons, companies, authorities or otherwise) defined by law at country/region/local level to parties/ organisations/ companies defined by law without restriction on their nationality, origin or location to parties/organisations/ companies having received authorisation from an internal structure (e.g. a specific 	1	<p>1: public,</p> <p>0,75: government only</p> <p>0,5: parties defined by law</p> <p>0,25: upon request</p> <p>0: law and local level only</p>	<p>This is a standard feature hence the score of “1”. Access requirements ensure adequate protection and privacy and confidentiality. For cross border interoperability between administrations, the more open a base registry is, and the fewer requirements are needed, the easier it will be to allow cross border interoperability.</p>

Criterion	Questions	Weight		Justification
	<p>governance body, a supervisory board, ...)</p> <ul style="list-style-type: none"> to parties/organisations/ companies having received authorisation from an external authority (e.g. an independent national or international organism, ...) other: (e.g. mixed access) (please explain) 			
<p>Leg. 3: Legal requirements on information quality</p>	<p>Is there a legal framework to guarantee the integrity and accuracy of the information before it is entered into the base registry? (Y/N) If yes, please provide the reference to the article(s) or section(s) in the related legal basis.</p> <p>Is there a legal framework to correct the information in case it is found to be erroneous? (after it was entered into the base registry)?</p> <ul style="list-style-type: none"> yes, by the data subject yes, by parties/organisations/ companies having received authorisation, on a voluntary basis yes, by parties/organisations/ companies having received authorisation, on a mandatory basis no other: (please specify). <p>Is there a legal framework to correct the information in case it is found to be erroneous? (after it was entered into the base registry). Please provide the reference to the article(s) or section(s) in the related legal basis.</p>	<p>1</p>	<p>1: legal framework to guarantee the integrity and accuracy and to correct on mandatory basis 0,75: legal framework to guarantee the integrity and accuracy and to correct by data subject (voluntary) 0: no legal framework</p>	<p>This is a standard feature hence the score of "1". This aspect guarantees for integrity and accuracy of data at the time of data input, requirements on data corrections and updates are crucial for the trustworthiness and reliability of the base registry. The fact that the authority has the duty to verify information ensures a higher level of quality than if the level quality relies on voluntary actions.</p>
<p>Leg. 4: Legal requirements on information availability</p>	<p>Is there a legal framework that describes how the base registry can be consulted by its (authorised) users? (Examples of consultation methods might be: 24/7 availability through the internet, on demand extracts sent by a competent authority, ...) (Y/N) If yes, please provide the reference to the article(s) or section(s) in the related legal basis.</p>	<p>1</p>	<p>1: yes 0: otherwise</p>	<p>This is a standard feature hence the score of "1". Clearly defined channels of how information is to be made available enable the practical sharing of information.</p>

Criterion	Questions	Weight		Justification
Leg 5: Privacy and confidential information	Are there any specific rules in the legislation related to the base registry to guarantee the privacy and confidentiality of the information held in the base registry (i.e. other than the general personal data protection and privacy legislation)? (Y/N) If yes, please provide the reference to the article(s) or section(s) in the related legal foundation.	1	1: yes 0: otherwise	This is a standard feature hence the score of "1". Clearly defined privacy and confidentiality requirements on top of the general privacy legislation avoid grey areas where unnecessary refusals to provide information occur.
Leg. 6: Review of legal aspects	Are there any ongoing initiatives to optimise/modernise/review the above legal aspects related to your base registry? (Y/N) If yes, please provide a short summary of these initiatives.	1	1: yes 0: otherwise	This is a standard feature hence the score of "1". Considering legal changes are likely to be needed, , time and effort to reach the needed legal changes can be saved by the fact that the fact that the legal review process is already started.
Leg.7: EU legislation	Is the registry subject to a specific legislative framework at EU level? (Y/N). If yes, please provide a short summary and reference to this framework. Do any bi- or multilateral agreements with EU Member States (or other international legal mechanisms) already exist that enable the cross-border interoperability of the base registry with base registries of other countries? If yes, please provide a short summary and reference to these agreements.	2	1: subject to a specific legislative framework at EU level + bi- or multilateral agreements with EU Member States 0,5: subject to a specific legislative framework at EU level 0,5: bi- or multilateral agreements with EU Member States 0: otherwise	The existence of EU legislation or other bi- or multilateral agreement in the area of the base registry shows that there already is a cross border legal framework dealing with the base registry which may smoothen the (political) path for additional EU legislation. This is an important element in the cross border interoperability, hence the weight of "2".
Leg. 8: Other regulatory aspects	Do you see any possible issues or legal obstacles to enable cross-border interoperability of your base registry with the base registries of other countries in the EU/EEA? (Y/N) If yes, please explain the issue(s) and indicate the severity/impact on enabling cross-border interoperability.		Not applicable	Not applicable

Table 1. Base registries interoperability model – legal level scoring.

For the **organisational level**, the following criteria were identified:

- Positioning towards public services,
- Data organisation,
- Governing body,
- Operational roles and responsibilities.

The following table (Table 2) shows the details of the model structure and scoring for the organisational level.

Criterion	Questions	Weight	Score	Justification
Org.1: Positioning towards public services	<p>Is the base registry:</p> <ul style="list-style-type: none"> • a standalone authentic source of information, potentially accessible by multiple public services? • an authentic information source being incorporated/part of a single larger public service? <p>If it's a part of another service, please state the name of the public service.</p>	2	1: multiple 0: single	The weight of “2” is assigned as positioning towards public services can only be achieved given that operational processes and a governing body exist.

<p>Org.2: Data organisation</p>	<p>Is the registry made of one single logical (data) repository or is it a collection/aggregation of logical (data) repositories? If it's a collection/aggregation, then please list the different (data) sources. Per (data source) data repository, please list:</p> <ul style="list-style-type: none"> the owner, the geographical location (note that one logical repository might consist of multiple physical locations. If so, please list all physical locations), the "reason of existence" of this (data) repository. 	<p>1</p>	<p>1: multiple sources 0: single</p>	<p>The lowest weight of "1" is assigned as this element is a standard feature and not a strict prerequisite for cross border interoperability, which does not mean that data organised as aggregation of logical repositories does not contribute to cross border interoperability.</p>
<p>Org.3: Governing body</p>	<p>Who or what instance (governmental body, institute ...) is responsible for the base registry? Please list the main installed governance bodies (steering committee, advisory committee ...) and the key participants per body. Please briefly describe the functioning of those bodies (reporting lines, meeting frequency, main roles and responsibilities).</p>	<p>3</p>	<p>1: clearly described governance, 0,75/0,5/0,25: partial score if governance structure, roles and responsibilities, processes not identifiable, 0: not described governance/answer could not be derived</p>	<p>This aspect received a weight of "3" as the governing structure embodies and manages the operational processes.</p>
<p>Org.4: Operational roles and responsibilities</p>	<p>Who or what instance (governmental body, institute ...) is responsible for the daily operation of your base registry? Please indicate whether the operational processes are based on best practices? If so, which best practices? If no, why not? Please indicate whether the operational processes:</p> <ul style="list-style-type: none"> are fully documented in a process handbook and audited 	<p>4</p>	<p>1: documented, best practices exist 0,75: documented, no best practices exist 0,5: partially documented, best</p>	<p>The highest weight "4" was assigned to this aspect as clearly defined processes of daily operations of a base registry is a condition <i>sine qua non</i> for a base registry to function. Design of operational process based on best</p>

	<p>against it</p> <ul style="list-style-type: none"> are documented at high level and followed on a best efforts basis are not documented but agreed upon in the organisation and, as such, followed other (please explain). 		<p>practices exist</p> <p>0,25: not documented, best practices exist</p> <p>0,25: documented only on high level, no best practices exist</p> <p>0: not documented, no best practice exist</p>	<p>practices provides a transparent view of functioning of a base registry. This in turn is a starting point in the design of operational processes in the European cross border context.</p>
--	---	--	---	---

Table2. Base registries interoperability model – organisational level scoring.

The following criteria were identified for the **semantic level**:

- Multilingual framework,
- Semantic interoperability,
- Syntactic interoperability.

The following table (Table 3) shows the details of the model structure and scoring for the semantic level.

Criterion	Questions	Weight	Score	Justification
Sem. 1: Multilingual framework	<p>Is the base registry accessible in more than one language? (Y/N)</p> <p>If yes: give all used languages</p> <p>Is it only the interface of your base registry which is multilingual? (Y/N)</p> <p>Is data in the database also stored in the above indicated languages? (Y/N)</p> <ul style="list-style-type: none"> • yes • no • partly <p>If no/partly, please specify.</p>	2	<p>0,5: 2 languages,</p> <p>1: more than 2 languages</p> <p>0: no</p> <p>0,5:partly</p> <p>1: yes</p>	<p>From a user perspective, language is an important element in cross border interoperability. In order not to bias countries with only one official language, the weight of this criterion was reduced to “2” comparing others. The distinction between multilingualism for only the user-interface on one hand and interface data on the other hand has been made.</p>
Sem. 2: Syntactic	<p>Is the data format described in a document available for potential integrators?(Y/N)</p>	4	<p>0,25: yes</p> <p>0,25: yes</p>	<p>The highest score of “4” was assigned to this aspect because syntactic</p>

interoperability	<p>Briefly describe (max. 15 lines) the type of data format: rules about character definition, data file length, numeric data types etc.</p> <p>Is an API available to use base registry functionalities in other applications (like eservices)(Y/N) ?</p> <p>If yes, please indicate how the API can be obtained and which functionalities have been made available.</p> <p>Is the API “publicly” available thus allowing any application developer to use it? (Y/N)</p> <p>If so, which functionalities (read, write, update ...).</p> <p>Are there any web services that use the API?</p> <p>How is syntax checking implemented in any of the interfaces of the base registry? Please specify.</p>		<p>0,25: yes 0,25: yes 0: otherwise</p>	<p>interoperability is evaluated from the level of passively documented database specifications over available API's up to applied web services.</p>
Sem. 3: Semantic interoperability	<p>Is for this base registry a detailed taxonomy description available? Y/N</p> <p>You answered YES to the previous question: "Is for this base registry a detailed taxonomy description available? "</p> <p>Is the base registry actually logically interconnected with other systems using semantic interoperability agreements made with the other system owners? Y/N</p> <p>You answered YES to the previous question:"Is the base registry actually logically interconnected with other systems using semantic interoperability agreements made with the other system owners? "</p> <p>Give one or more examples of these interconnections</p> <p>Is any single standard on syntactic or semantic compliance applied for your base registry (e.g. ISO, ETSI, CEN, W3C)? Y/N</p>	4	<p>0,25: yes 0: otherwise 0,25: yes 0: otherwise</p> <p>Questions on Standards: 0,5: yes 0:otherwise</p>	<p>The highest score of “4” was assigned to this aspect because semantic interoperability is the ultimate criterion for cross border interoperability and a proven taxonomy based interconnection is a necessity to realise this. Compliance with international standards give this process extra value.</p>

Table 3.Base registries interoperability model – semantic level scoring.

The following criteria were identified for the **technical level**:

- Technological reusability capability,
- Interfacing to other systems,
- User (human) interfaces,
- Authorising third party users,
- Authenticating third party users.

The following table (Table 1) shows the details of the model structure and scoring for the technical level.

Criterion	Questions	Weight	Score	Justification
Tech. 1: Technological reusability capability	Does the base registry have reusable technology components that might be of interest to build additional/new base registries within your country? (Y/N) If so, please provide some clear examples. In case of software components: does the licensing model allow for sharing and reuse (e.g. Open Source components)? (Y/N) If yes, please provide some clear examples. -Is the governing organisation willing to make this reusable component available (through documentation, architectural design, source code, ...) to the other European countries if requested?(Y/N)	1	1: reusable technology components that might be of interest to build	This aspect is a contributor to cross border interoperability and not a key enabler, hence it was assigned the lowest score of "1".
Tech. 2: Interfacing to other systems	Does your base registry have interfaces available to connect to other existing systems (e.g. other departments, legal identities ...) and/or new registries? (Y/N) Are these interfaces documented? Completely/Partly/Not documented. What is the preferred technical interface to use to exchange data	3	0,5: if interfaces available to connect to other existing systems 0,30: if the interface is completely documented 0,20: if the interface is	The ability to interface to other systems is a necessary condition for interoperability. In addition the interface needs to be documented and the technology needs to be chosen accordingly. Hence it was

Criterion	Questions	Weight	Score	Justification
	with the base registry? (e.g.: File transfer, Direct database connection, XML messages,...) To what extent is the interfacing technology of the base registry based on open standards for potential usage by other European countries?		based on open standards	assigned the highest score of "3".
Tech. 3: User (human) interfaces	Please briefly describe the user interfaces of the base registry (human interfaces build to use the functionalities of the base registry). Please list any particular functionality worth mentioning that could be seen as innovative or differentiating with respect to other base registries.	1	1: if there are innovating elements	This aspect is a contributor to the cross border interoperability and not a key enabler, hence it was assigned the score of "1".
Tech. 4: Authorising third party users	Assuming the base registry is interconnected with other base registries or services. Is there a governance model to maintain the interfaces (create, modify, delete) with those third parties? (Y/N)? If so, please provide the main characteristics. To what extent does the governance model cover the usage of the base registry by other European countries? Please specify.	3	1: if there is a governance model that also covers other European countries 0,5: if the governance model does not cover other European countries	Authorising third party users is as important as authenticating third party users. This aspect receives a weight of "3" as the operational management (=governance model) is crucial to administer the technology. The technology itself is not enough. Hence it was assigned the highest score of "3".
Tech. 5: Authenticating third party users	What technology is used for Identity and Access Management. In other words, what technology is implemented to authenticate and authorise users of the base registry? Please specify. To what extent is the authentication technology open for usage of the base registry by other European countries? Please specify.	2	1: if the authentication technology is open for usage by other European countries	Authorising third party users is as important as authenticating third party users a weight of "2" was assigned to this aspect as technology is an important element enabling the authentication of third parties.

Table 1. Base registries interoperability model – technology level scoring.

The following criteria were identified for the **security dimension**:

- Applicable security policies,
- Security governance,
- Information security classification,
- Access control,
- Compliance.

The following table (Table 24) shows the details of the model structure and scoring for the security dimension.

Criterion	Questions	Weight	Score	Justification
Sec. 1: Applicable security policies	Is there a security policy used for this base registry? If yes, please give references of recognised security standards that are implemented (e.g.: ISO 27001, ...).	3	1: multiple 0: single	The basic requirement in the security dimension is security policy; hence it was assigned the highest score of “3”.
Sec. 2: Security governance	Is there a governance model (describing organisation, roles and responsibilities, processes, procedures and technology) that controls the operational aspects of security? <ul style="list-style-type: none"> • level 1: Initial (Processes unpredictable, poorly controlled and reactive), • level 2: Managed (Process characterised for projects and often reactive), • level 3: Defined (Process characterised for the organisation and is proactive), • level 4: Quantitatively Managed (Process managed and controlled), • level 5: Optimising (Focus on process improvement). Is there a disaster recovery plan (dealing with business continuity requirements, calamities, ...) in place for your base registry?	3	0: Level 1: Initial (Processes unpredictable, poorly controlled and reactive) 0,25: Level 2: Managed (Process characterised for projects and often reactive) 0,5: Level 3: Defined (Process characterised for the organisation and is proactive) 0,75: Level 4: Quantitatively Managed	Security governance serves to reinforce the security policy and is also a basic requirement (direct link) therefore it was assigned the highest score of “3”.

Criterion	Questions	Weight	Score	Justification
	(Y/N).		(Process measured and controlled) 1: Level 5: Optimising (Focus on process improvement)	
Sec. 3: Information security classification	Is there an information classification system in use for your base registry? (Y/N) Is the classification system set up according to? : <ul style="list-style-type: none"> the sensitivity of the information (Y/N), the access to the information (Y/N), the functional value of the information (Y/N), any other criterion. 	1	1: yes 0: no +0,33333 for answers 1 to 3 answer 4 to be assessed case by case	This is a standard security feature, hence it was assigned the lowest score of "1".
Sec. 4: Access control	Which security requirements/ clearances need to be fulfilled by a person or entity requesting access to your base registry for this to be granted (e.g. Government approval, Independent committee review, signing nondisclosure agreements,...)? Does the base registry use an Identity and Access Management system? (e.g.: Unique users need to authenticate, a reason for the request of certain data needs to be given, approval needed for certain information, ...) ? Please explain the key characteristics.	2	1: positive security requirements/clearances + Identity and Access Management system 0,5: positive security requirements/clearances + no Identity and Access Management system 0,5: no positive security requirements/clearances but Identity and Access Management system 0: no security requirements/clearances + no Identity and Access Management system	The second highest score of "2" was assigned to this aspect as a user should have a set of security requirements to adhere to once the security policy and security governance is in place.
Sec. 5: Compliance	Are security audits (verifying compliance with legal requirements, security policies, applicable use of international standards and	1	1: yes 0: no	This is a standard security feature, hence it was assigned the score of "1".

Criterion	Questions	Weight	Score	Justification
	respect of internal controls, policies and procedures) performed on your base registry? Please specify types of performed audits. <ul style="list-style-type: none"> • yearly internal control, • policy and procedure review, • bi-yearly review of compliance towards standards, • other. 		Q2: interesting background information, no score related	

Table 2. Base registries interoperability model – security dimension scoring.

4. RESULTS OF THE SURVEY

4.1 DISCLAIMER

All the results and analysis reported in this section are based on the survey results as submitted through the on-line survey tool. A closed question survey was used to limit the interpretation of questions. The answers, as submitted, are a starting point of the analysis and are taken “as is”. No additional oral validation has been undertaken to avoid bias in answers.

Please note that all derived results, comments, recommendations, etc. are based on the results obtained from 19 selected base registries. Therefore, the results of this study must always be interpreted with respect to this limited sample and not to base registries in general.

Last but not least: this study investigates the interoperability maturity and not the maturity of the base registry as such. A base registry can be a local reference of best practices and innovation, but still have a low score on cross border interoperability maturity, as the registry was not designed for that functionality.

4.2 SURVEY SAMPLE

In order to analyse the base registries through the prism of the previously described levels (legal, organisational, semantic and technical) and the security dimension, it was decided to use a survey as it provides results in a standardised format facilitating further analysis. In addition, an online survey was chosen as a method due to the ease of results tracking and gathering. The survey consists of sixty one question grouped according to the four levels and the security dimension. A detailed description of the survey content and rationale for each question is presented in the deliverable *D1.0.1. Template used for the inventory*. The below table (Table 4) presents the sample of base registries. The following abbreviations are used in the Table 4 and throughout the document:

- B: business registry
- C: citizen registry
- L: land and property registry
- P: procurement and information registry
- V: vehicle registry

Please note that this study does not analyse the performance of base registries as such, but analyses the cross border interoperability of base registries. Hence, it was also decided to render the results anonymous as the value of the survey is to be found in the “aggregated” result analysis and not in the data of the named registry itself.

Base registry name	Base registry type	Country
Belgian Public Tender Bulletin	P	BE
Registers of the population	C	BG
Car registration	V	CY
Registry of territorial identification, addresses and real estate	L	CZ
The Central Office of Civil Registration	C	DK
Estonian Population Register	C	EE
National Board of Patents and Registration in Finland	B	FI
Special Registry of the Ministry Interior	C	EL
National Company Publicity and Information Registry System	B	HU
Public Administration ordering Registry	P	IT
Tax Information System	B	LV
Caisse Nationale de Santé	C	LU
Addresses and Buildings	L	NL
Centralny Rejestr Ubezpieczonych - Central Ensuree Registry (CRU)	C	PL
Cadastru de Contribuintes	C	PT
The list of Entrepreneurs	B	SK
IDIS	B	SI
General Services for DATA verification	C	ES
TDS database	B	SE

Table 4. The analysed sample of base registries.

In Annex 1, the diagrams illustrating the maturity of cross border interoperability for each of the 19 base registries can be found.

In order to identify a sample of base registries, life events were used as a starting point. As there is no standard set of European life events, a set of 20 eGovernment services was identified and then matched with relevant countries by means of the online sophistication indicator (please see the deliverable “Inception Report” for more details). As a final result, one base registry supporting a given service was chosen per country.

The analysis takes into account 19 base registries distributed among the following types:

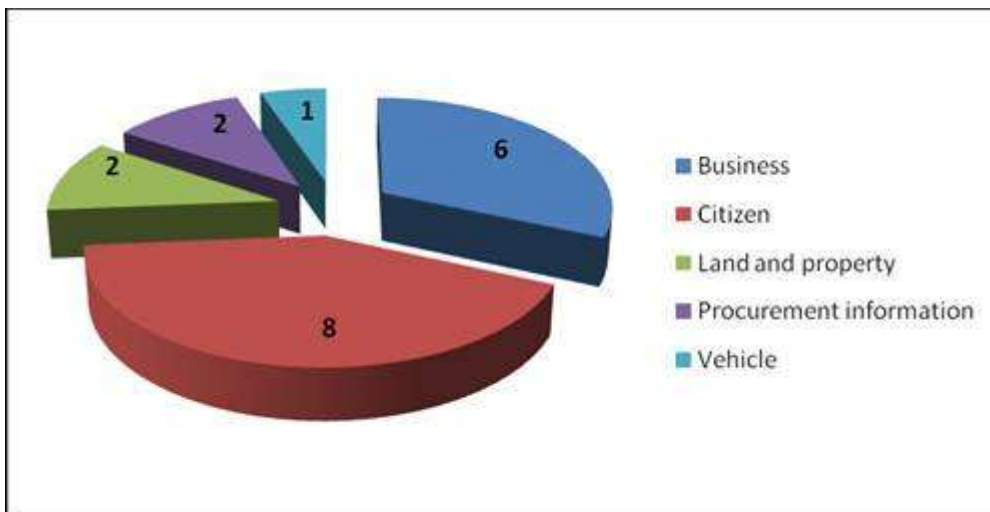


Figure 4. Registry types.

The results of the survey are presented per level and per type in sections.

4.3 SURVEY RESULTS PER LEVEL AND SECURITY DIMENSION

This section consists of an analysis of results per level. The analysis of the survey results proceeds as follows:

- each level, the security dimension and aspect² of the survey data was analysed,
- graphs for each of the four levels and aspects (legal, organisational, semantic, technical) and the security dimension were created,
- each graph was analysed and described: comparative analysis between and within levels (and the security dimension) was undertaken,
- for each of the four levels and the security dimension, recommendations were made, based solely on the survey results.

² There are four interoperability levels (legal, organisational, semantic and technical and each level is divided into number of aspects (e.g. semantic level has multilingual framework aspect, syntactic interoperability aspect and semantic interoperability aspect). The same exercise is done for the security dimension.

Figure 5 and Figure 6 below are used in the analysis.

The overall maturity scores per level and the security dimension are presented on a Figure 5 below:

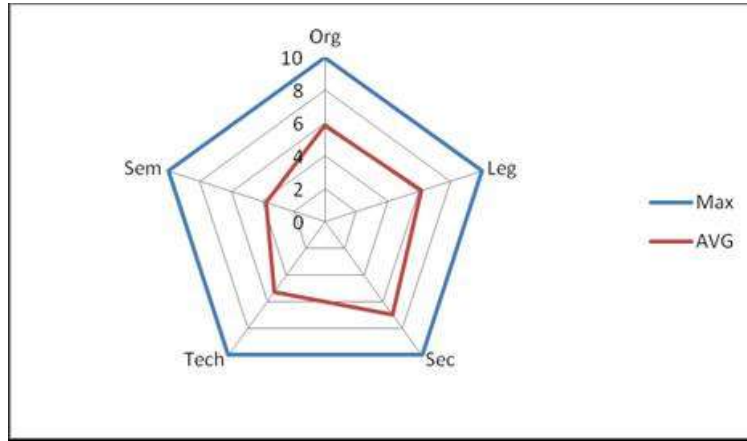


Figure 5. Maximum and average scores per level and the security dimension of the base registries interoperability model.

Level/dimension	Organisational	Legal	Security	Technical	Semantic
Average	6	6,16	6,96	5,28	3,79

Table 3. Average scores per level and the security dimension.

The overall maturity scores of maturity per type of base registry for each level and the security dimension are presented on a Figure 6 below:

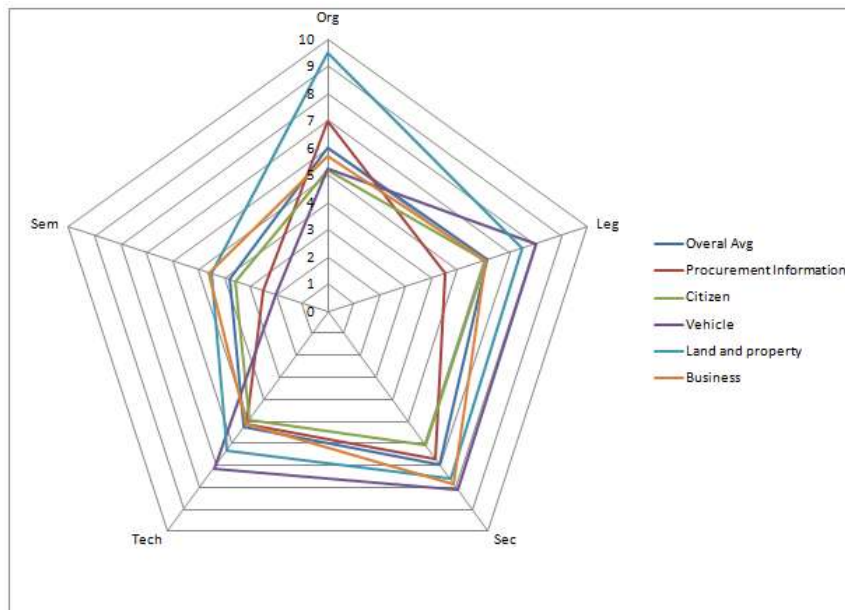


Figure 6. Average scores per type of a base registry.

4.3.1 Legal level

The legal level is the second level in the analysis of the interoperability of base registries. The level of the analysis investigates the legal framework and legal requirements of base registries. The level concerns legal authority and legal requirements on information (access, quality, availability and confidentiality) and the EU legislation. Legal level covers the following aspects:

- Legal authority,
- Legal requirements on base registry access,
- Legal requirements on information quality,
- Legal requirements on information availability,
- Privacy and confidential information,
- Review of legal aspects,
- EU legislation,
- Other regulatory aspects.

As outlined in Figure 45 and Table 3 below, the legal level is the second best performing level after the security dimension, in terms of the interoperability maturity of base registries. On average, the base registries in the sample in the legal level score 6,16 out of 10 points.

Legal authority

It can be observed that all respondents indicated a legal framework in which their respective base registries operate. However, the legal frameworks differ greatly among countries, areas or types of base registries.

On one hand, it is possible to deduct that not all base registries in the sample are explicitly established by a legal act. They are instead created by a public administration to operationally comply with its public tasks as defined by law. For example, a base registry in the area of tax has been created by the tax authorities in order to effectively fulfil their duties as defined by law.

On the other hand, the answers show that in specific areas, such as national citizen registries, the relevant base registry is created by a specific legal act (for example 'law on base registry A') or by a specific part of an overarching legal act (for example 'chapter base registry A in the Social Security Code'), which explicitly creates the base registry.

Only 2 respondents indicated that in their countries there is a specific, overarching framework for base registries which is not specific to a subject area. In these countries, the overarching requirements for all base registries are defined at one level, while the specificities per base registry are defined in order to fully meet the requirements of the subject area. In one country, the overarching framework can be found in an overarching act, with the specificities per base registry within the same act in specific sections. In the other country, the overarching framework is set out in a governmental program, while the legal framework of the base registries as such is found in a specific legal act which complies with the governmental program.

All respondents indicated a national or federal level for the legal framework of their base registry. However, this may be due to the method of selection of base registries based on life

events, given that in countries with federal structures, the level of the legal framework covering a base registry corresponds to the competencies of a state's constituencies with legislative powers (if there are any). Considering this legal concept of matching the legislative level to the competency level (with legislative powers), it cannot be concluded that the legal framework of all base registries are situated at the national or federal level, but they may also be at the regional (or other) level if a legislative 'level' exists. For example, countries A and B are federal countries. If in a country A the competency of base registry X is at the federal level, the legislative framework for the base registry will be found at a federal level. If in a country B the competency is at the regional level, in principle, there will be a separate base registry per region and a corresponding legal framework per region, which will likely not be identical to the legal framework of the other region(s).

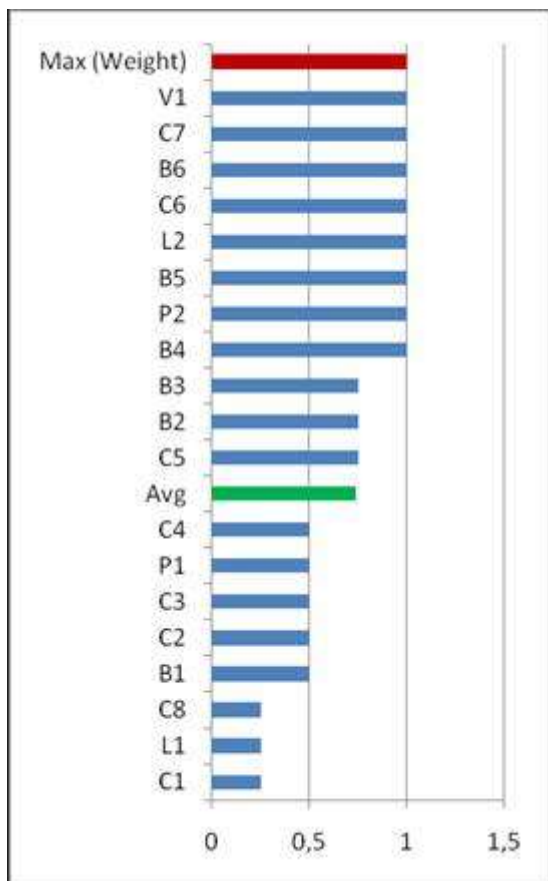


Figure 7. Legal requirements on base registry access.

Legal requirements on base registry access

By analysing the access to the information held in a base registry, the results of the survey vary greatly. However, all respondents indicated that the access to the base registry is regulated by law.

Furthermore, a number of respondents indicated that some parties, such as governmental institutions, have full access to the information, while other parties, such as companies or persons, may only receive restricted access. Only 3 respondents indicated that the authorisation of an internal structure is required to gain access. None of the respondents indicated that authorisation of an external structure (an independent organ such as a supervising authority) is required.

Only 1 respondent indicated explicitly that there is no restriction regarding the nationality or origin of the party requesting access where access to the base registry is not open to the general public. This indicates that most legal frameworks appear not to refer to this subject explicitly or clearly enough and that consequently legislative action may be required in many countries to ensure that

access by non-national parties is not an issue solely due to the fact that they are located in another country.

Legal requirements on information quality

Most base registries (16 out of 19) are subject to legal requirements on the quality of the information which is entered in the base registry and on the quality of the information that is already included in the base registry (i.e. on keeping information accurate and up to date (16 out of 19). The list of 16 base registries with requirements on the quality on data entry is not the same as the list of the 16 base registries with requirements on the quality of data entered, which indicates that these requirements are not necessarily linked to each other. 10 respondents, including all the public procurement information base registries in the survey, indicated that the responsibility of keeping the information accurate and up-to-date is an obligation for the person or party to whom the information relates, as part of their administrative obligations. 6 respondents indicated that information corrections and updates can take place on the initiative of several parties, such as the person or party involved (as part of their administrative obligations), municipalities, courts, notaries and other institutions (which indicates a distributed information collection method through trusted parties) and/or the public administration managing the base registry (which indicates the administration has an information verification duty). This is the case for all of the land and property registries in the sample. For the other types of base registries, the survey replies indicate that the approach taken differs per country.

Legal requirements on information availability

12 respondents indicated that the legal framework applicable to the base registry describes how the base registry can be consulted by its (authorised) users. It appears that this is the case for most business, citizen and land registries, but not all. This indicates that the approach regarding regulating this more 'practical' aspect of base registries differs per country and per base registry type. This may indicate that there are several approaches to handling this matter; on the one side, there is the specification in the law of the procedures on how information is to be provided, and on the other side, the lack of specifications in law to make the service offering possibilities and channels more flexible.

Privacy and confidential information

About half of the respondents (10) indicated that there are additional legal requirements regarding confidentiality and privacy applicable to a base registry, in addition to the applicable general data protection and privacy laws and regulations. These base registries contain large amounts of personal data.

Review of legal aspects

Half of the respondents (9) indicated the legal framework currently applicable to a base registry are at present or will in the near future be subject to review in order to optimise and modernise the legal framework to better fit the requirements of the fast information demanding society of today. These legal frameworks under review can be found in all base registry types of the survey.

EU legislation

14 respondents indicated the existence of a legal framework at EU level (10 respondents) and/or bi- or multi-lateral agreements with other EU Member States (6 respondents) that aim at cooperation in the area of base registries. This indicates that these initiatives currently already serve as first legal steps towards cross border interoperability of base registries. It however also appears that none of the legal frameworks mentioned can, as they currently exist, fully enable the cross border interoperability of base registries. The EU frameworks mentioned are mostly situated within the geographical information area (INSPIRE³), VAT⁴, public procurement⁵ and business registries⁶. The bi- or multilateral agreements are related to employment, company information, vehicle information and geographical information. Only one of the citizens' registries indicated an international framework in the area of marriages.

Other regulatory aspects

The survey's final question was an open question investigating legal obstacles or issues that hinder international interoperability. 6 respondents indicated no legal obstacles towards interoperability, however, all the others did, but for different reasons, not all of which are directly linked to specific issues related to base registries. 1 respondent indicated that the international recognition of electronic signatures is a obstacle because an electronic signature is needed to access the base registry. Other respondents indicated that there are issues regarding the transposition of aspects which are not-strictly legal into the law, such as the semantic definitions (as currently developed in INSPIRE) or the cost of providing information to non-national parties. 2 respondents indicated that personal data protection restrictions would be a legal obstacle towards more interoperability, even though there is already a harmonised privacy landscape in the EU due to the Privacy Directive⁷.

³ Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), and its related regulations. For more information, please visit <http://inspire.jrc.ec.europa.eu/>

⁴ Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, and its amending and related acts. For more information, please visit http://europa.eu/legislation_summaries/taxation/l31057_en.htm

⁵ For more information, please visit http://ec.europa.eu/internal_market/publicprocurement/rules/current/index_en.htm

⁶ For more information, please visit http://ec.europa.eu/internal_market/company/business_registers/index_en.htm

⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. For more information, please visit http://ec.europa.eu/justice/data-protection/law/index_en.htm

4.3.2 Organisational level

The organisational level is the first level in the analysis of the interoperability of base registries. The level covers the positioning of base registries towards public services, data organisation (structure, management) as well as governance in terms of governing bodies as well as processes, roles and responsibilities.

Figure 5 presents the performance in terms of the cross border interoperability potential. This result is based on the base registries interoperability model. As outlined in Figure 5 and Table 3, the organisational level is the third best performing level, after the security and the legal levels respectively, in terms of maturity of interoperability of base registries. On average, the base registries in the sample score 5,7 out of 10 points in organisational level.

From the point of view of the type of base registry (see Figure 6), on average, the land and property registry scores the highest (9,5 out of 10 points) and the citizen base registry scores the lowest (5 out of 10 points) in the organisational level. The sample contains two land registries and seven citizen registries. On average, the land and property registries score the highest in the governing body aspect, which entails a simple governing structure (2 to 3 governing structures allowing relatively easy international cooperation) and a well described governing process (including roles and responsibilities, reporting and meetings frequency that allow a relatively smooth adaptation for opening up the base registry). The citizen base registry scores the lowest, on average, mainly in aspects such as positioning towards public services and data organisation.

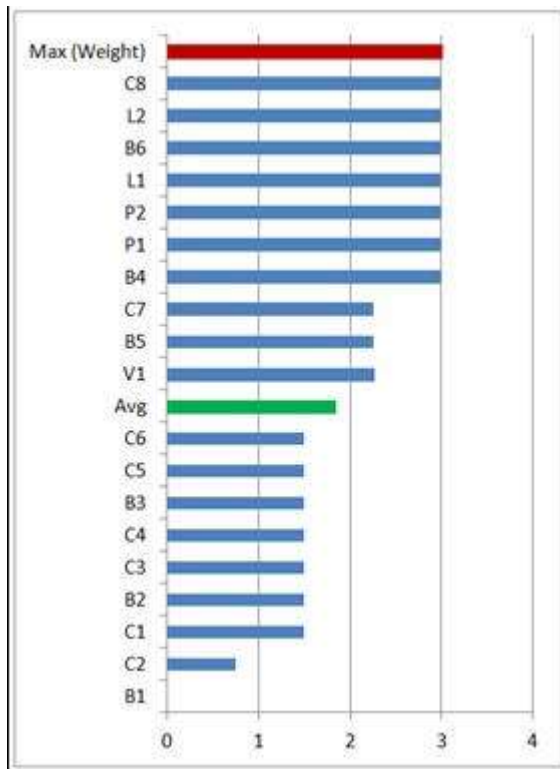
In particular, this means that citizen base registries in the sample are the least mature vis-à-vis interoperability by being a standalone (isolated) source of information not incorporated in a public service and by being made of one logical data repository of information.

Positioning towards public services

The aspect “*Positioning towards public services*” relates to a base registry being a standalone source of information or an authentic source of information incorporated in a public service. 12 out of 19 base registries in the sample score above the average indicating affiliation to a larger public service. The remaining part of the sample reveals the characteristics of an isolated repository of information. Overall, most base registries in the sample reveal potential for future interoperability in the above aspect.

Data organisation

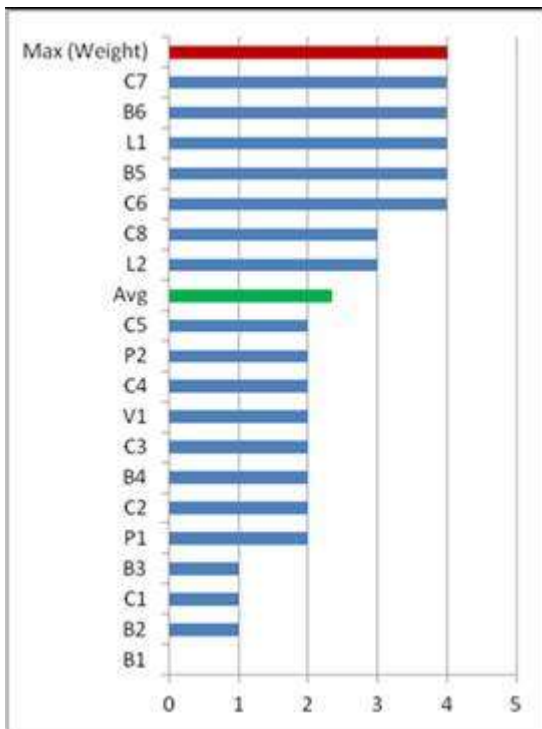
The aspect “Data organisation” concerns data organisation in terms of a single or aggregated data structure. 6 out of 19 base registries score above average in this aspect. This means that these base registries function as a collection/aggregation of data that suggests data organised in a centralised way which facilitates interoperability. The majority of base registries in the sample (12 out of 19) are single data repositories that call for integration/aggregation into bigger structures in order to meet the interoperability requirements. Overall, the base registries in the sample are organised mostly in a decentralised, fragmented manner and do not meet the interoperability criteria defined by the base registries interoperability model.



Governing body

The aspect “Governing body” concerns the base registry governing instance and its functioning. Around half of base registries in the sample (10 out of 19) score above average revealing simple organisational structure (2 to 3 instances) that might easily work with international parties and clearly defined processes. The remaining base registries (7 out of 9) demonstrate simple governing structure, but mostly lack well described governing processes. In this regard, given the limitations of the results of the survey and quality of responses, it is not certain if the processes do not exist or are not well documented/followed. Overall, there are best practices in place, but the operational processes might not exist or are badly described.

Figure 8. Governing body.



Operational roles and processes

The last aspect “*Operational roles and processes*” concerns operational roles and responsibilities related to management of a given base registry. 7 out of 19 base registries perform well in this level. Most of them follow best practices, such as ITIL® or ISO frameworks, and have fully documented processes which are audited. The remaining 12 base registries mostly follow best practices (9 out of 12) and their processes are mostly documented (10 out of 12), however, no regular audit is performed. Overall, most of the base registries in the sample follow best practices concerning their operations, however the lacking control element is the audit of the operational processes.

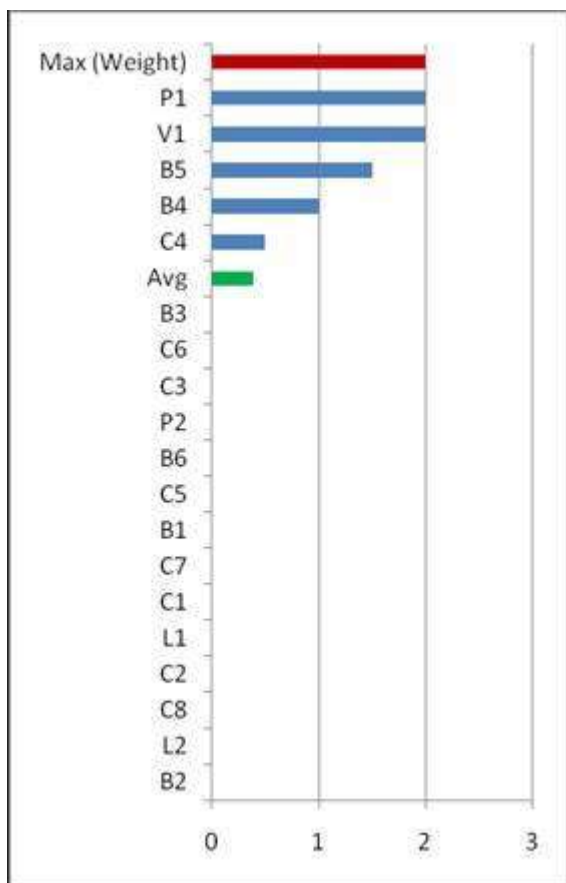
Figure 9. Operational roles and processes.

4.3.3 Semantic level

The semantic level is the fifth and last level in the analysis of the interoperability of base registries. The level analyses if there is a uniform syntax and semantic framework across all base registries. In particular, it investigates if a base registry is accessible in more than one language, if the data format is described in a format available for potential integrators, and if there is an API and taxonomy. Semantic level covers the following aspects:

- Multilingual framework,
- Syntactic Interoperability,
- Semantic interoperability.

By looking at Figure 5 and Table 7, it becomes clear that the semantic level is the worst performing level in terms of the interoperability maturity of base registries. On average, the base registries in the sample score 3,8 out of 10 points in the semantic level. This result could be explained by the difficulty in meeting the semantic criteria as far as interoperability and cross border services are concerned. It can also be argued that this criterion is not the highest priority when it comes to operating and managing base registries at a local level, but becomes very important in an interoperable context.



Multilingual framework

When considering the first indicator, “multilingual framework”, only 5 out of 19 base registries have an interface in more than one language. 2 out of 19 base registries have data stored in more than 1 language. For 3 out of 5 base registries multilingual aspects are limited to an interface in more than one language. Those multilingual base registries concern examples of “business registries” from “small language groups”. Only 2 registries where data is also available in more than one language originate from countries with more than one official language. It goes without saying that for countries where only one official language is spoken, most of the base registries are in one language only. However, as far as interoperability and cross border services are concerned, the interface at least needs to be available in different languages.

Figure 23. Multilingual framework, syntactic and semantic interoperability for different types of base registries.

Syntactic interoperability

“Syntactic interoperability” aspect defines whether the base registry data formats are precisely defined in standard formats and schemas and if this information is available. 73% of the assessed registries in the sample have the documentation about their data formats available for potential integrators.

10 out of 19 base registries have an API for the integration of base registries functionalities in other applications and only half (5 out of these 10) is publicly available for the use of third party developers. In most of the cases these public API are only used for reading the data. 8 out of the 19 base registries have web services that use the API.

Semantic interoperability

“Semantic interoperability” defines the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of both systems. In other words, it answers the question of whether the data found in the same field of two different registries have the same meaning.

Only 7 out of 19 base registries have a detailed taxonomy available and only 2 of these registries are logically interconnected with other systems using semantic interoperability agreements made with the other system owners. 2 of these base registries function in the European context. The first is a business registry, in which information is based on the Single Administrative Document (SAD)⁸ used in all EU countries. The second is a procurement information registry in which all public tenders that must be published at EU-level are sent to the European Publish Office by a structured mail (zip file in annex, containing xml-files) and a check at the syntactical and semantic level is done.

Concerning the compliance with syntactic and semantic standards, 11 out of the 19 base registries are not compliant with these requirements. Referring to the typology of base registries, it is possible to say that the best performers are among the “business registries”. The multilingual performance is mainly low and independent from the typology. The average score for the syntactical interoperability is almost 50% in the sample, while the semantic interoperability has a result of 38% in the sample.

⁸ http://ec.europa.eu/taxation_customs/customs/procedural_aspects/general/sad/index_en.htm

4.3.4 Technology level

The technology level intends to provide more insights into the technological ability of the base registry to support cross border interoperability. In order to assess this, five aspects will be covered, listed in the table below. The technology level covers the following aspects:

- Technological reusability capability.
- Interfacing to other systems.
- User (human) interfaces.
- Authorising third party users.
- Authenticating third party users.

When looking at the overall averages at the different levels, the technology level scores rather low with respect to interoperability maturity: 5,27 out of 10 (Figure 5). The main reasons are described in the following paragraphs. Clearly, technology-wise, base registries are organised to serve local stakeholders. Opening up in a cross-border context is technologically feasible but is prevented by the need for standardisation and governance.

Looking at the technology level from the point of view of a type of base registry, it is possible to observe a slight variation in interoperability maturity. Although land and property registries and vehicle registries are not well represented in the sample (see Table 3), citizen and business registries are at the lower end of the maturity spectrum. However, a detailed analysis does not reveal clear differentiating elements supporting a structural lower maturity of those registries. It is only possible to indicate that in the sample, the land registries and in particular the one vehicle registry, score overall slightly better with regards to the technology parameters.

Technological reusability capability

1 base registry scores the maximum while 8 other base registries score above average (and above 0.5). It is possible to observe that a considerable number of the base registries (8 out of 19) have reusable components that might be of interest for other base registries. However, only half of them are subject to a licensing model that would allow the sharing of software components. 2 base registries declare that they have the “appropriate” licensing model but they do not have reusable components.

Of the 8 registries with reusable components, only 4 governing organisations seek to share those components through knowledge transfer (documentation, architectural design, source code, etc.). Surprisingly, another 7 registries – without reusable components – do want to share information regarding their technological resources.

Overall, around 50% of the surveyed base registries receive more than 50% of the scoring.

Interfacing to other systems

The scoring on the interfacing maturity is overall very high. All base registries pass the 50% score. All 19 of the surveyed base registries declare that they can interface with other systems. 12 of the 19 registries also indicate that their interfaces are fully documented. The remaining 7 declare a partial documentation.

The vast majority (17 out of 19) uses XML as an interface format. 4 out of 19 registries have a web service available. Roughly half of the surveyed registries have open standards in use which would support technological access in a cross border context.

In some individual cases, email transfer and direct database access is operational. It is interesting to note that one land registry has aligned its standards to the INSPIRE⁹ requirements which is a starting point on the road towards the cross border interoperability.

⁹ Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

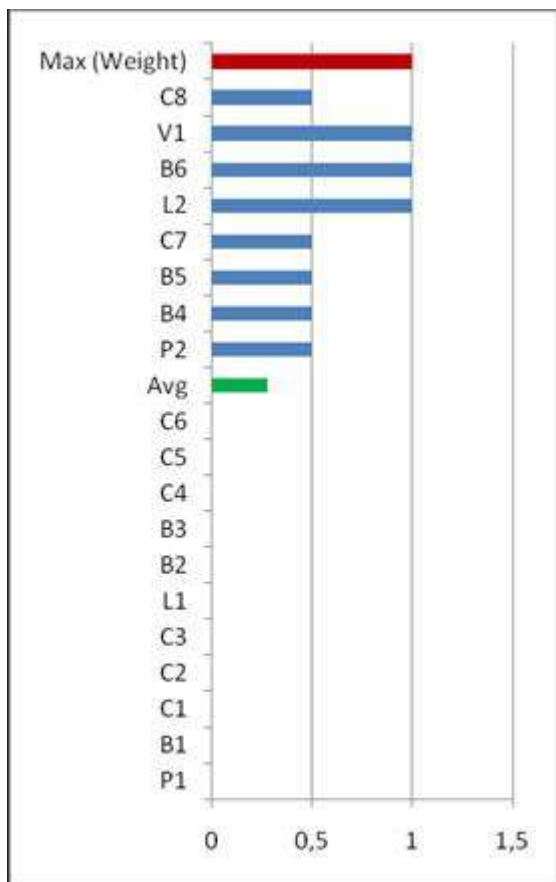


Figure 14. Interfacing

User (human) interfaces

Whether or not a base registry has a human interface was not taken into account in the scoring as this is not relevant from an interoperability perspective. The score was solely given to the innovative character of the interface. However, the concept “innovative” can have different meanings. Nevertheless, in order to differentiate the received answers, the following criteria were taken into account:

- If a base registry uses a multichannel communication, a push technology, or has established multipurpose communication channels towards different types of service requestors, a base registry scores 1 point,
- If a base registry demonstrates an enhanced user experience features (forms, electronic signature, extended language usage...), it scores 0,5 point,
- If nothing is mentioned or the mentioned information is not reflected in the above criteria, the base registry scores 0 points.

Based on the above scoring, 3 base registries received the maximum score. 5 registries received half a point. The remaining 11 received zero points.

It is difficult to judge qualitatively the innovative character of user interfaces. However, quantitatively, the fact that half of the respondents were not able to mention any innovative feature might indicate the preference for solidness, robustness and reliability of a system (potentially based on a legacy back office) to support the delivery of the required functionalities.

Note that, cross-referencing to the interface results, new (proven) technology is used to support the delivery of those services.

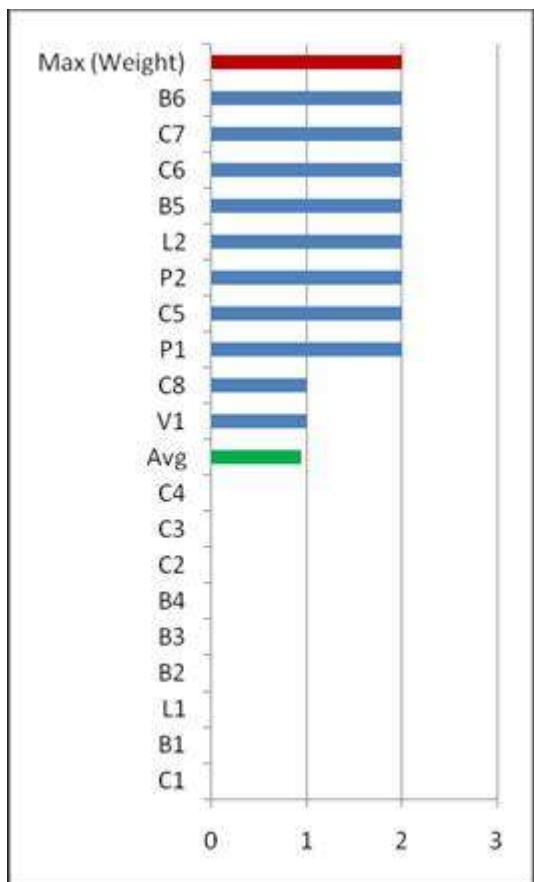


Figure 10. Authentication in a cross-border context.

Authenticating and authorising third party users

The fact that an authentication platform is in place, was not scored. If the authentication platform was open for usage by other European countries a score of 2 was received. A score of 1 was given if the platform was indirectly open to other European countries (e.g. through dedicated networks).

10 of the 19 respondents indicated openness towards other European countries. The basic arguments are the use of standard authentication mechanisms and the openness in case the European third party invests in a PKI infrastructure. 1 base registry uses a dedicated network to provide access to its services.

Most of the remaining base registries indicated either a lack of readiness or awareness to open up their base registry to other European third parties. Note that the type of authentication technology strongly differs from one base registry to another, ranging from common authentication platforms or own developed platforms to very low or unknown (to the respondent) technology platforms.

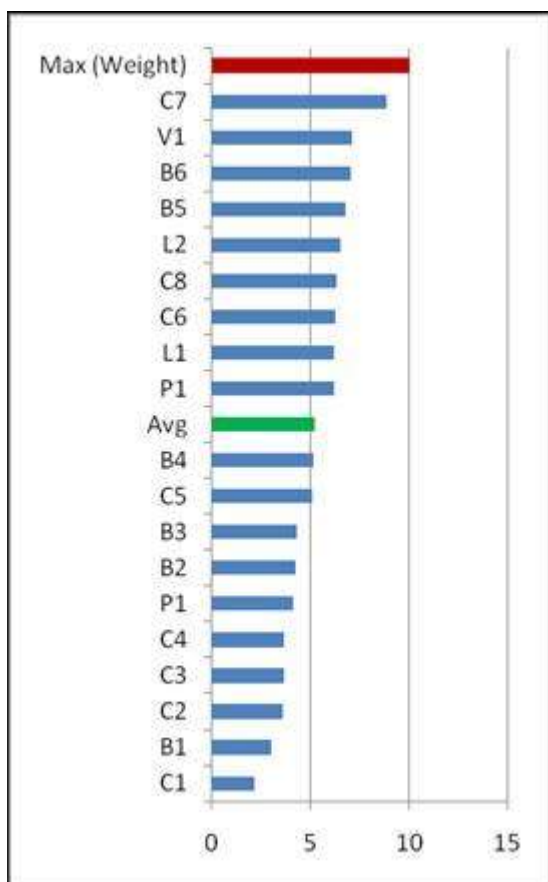


Figure 11. Overview: technology questionnaire results.

Overall, 10 of the 19 respondents score above average. It could be concluded that, from a technological point of view, the base registries are focused on service provisioning to their “internal” market and that the technology challenges to open up towards other European countries are mostly related to the authorisation / authentication aspects.

The interfacing aspects and the use of technical standards can be considered in line with common expectations, taken into account some innovative setups. Progress is required with respect to the reusability of components.

4.3.5 Security dimension

The security dimension is the fourth level in the analysis of the interoperability of base registries. This dimension investigates Security Policies, Security Governance, Security Compliance and Identity and Access Management. These security aspects give a basic overview of the importance of security currently applied by the selected base registries and what the differences between several European countries are. Security dimension covers the following aspects:

- Applicable security policies,
- Security governance,
- Information security classification,
- Access control,
- Compliance.

It is clear from Figure 5 and Table 3 that the security dimension is the best performing compared to other interoperability levels in terms of the interoperability maturity of base registries. On average, the base registries in the sample in the security dimension score 6,96 out of 10 points.

In general, the results of the survey indicate that essential security aspects are given the appropriate attention when setting up the base registry to guarantee confidentiality, integrity and the availability of the base registry. Although this does not guarantee successful integration and interoperability, essential security components for integration seem to be available. The following table gives an overview of the questionnaire results.

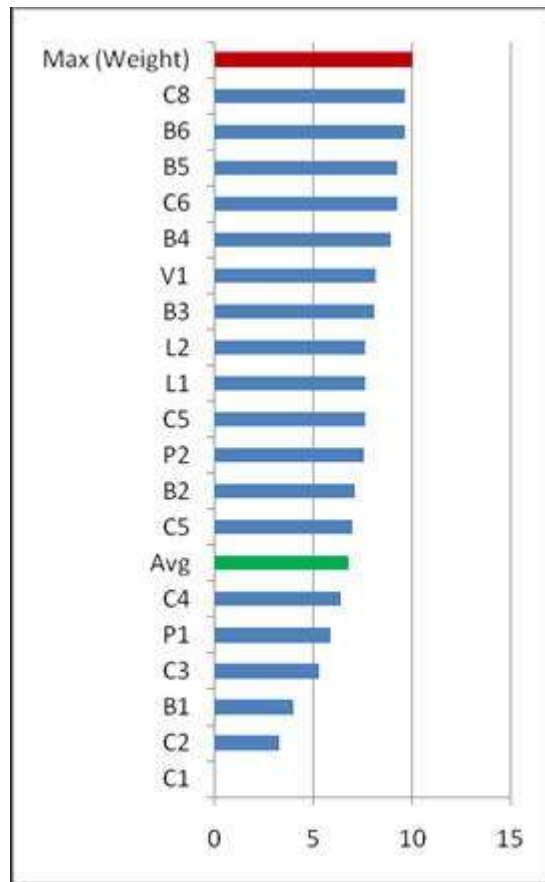


Figure 12. Overview: security questionnaire results.

Although the results lead to a relatively positive scoring for security within the base registries (and these scores are the basis for this analysis), some answers given by the base registry owners indicate that the operational environment of the base registry may not be reflected. The formulation of the answers clearly show that the interviewees who filled in the questionnaire do not always have the required/correct information to clearly answer questions, might not be aware that they have given unclear responses or might not be willing to provide accurate, correct and complete information.

Based on experience and professional judgment, this difference should be taken into account when drawing conclusions about the (security) maturity dimension of the base registries in relation to integration, interoperability and sustainability of the base registries.

Security Policy & Governance

Most European countries have a security governance program in place to steer the operational security environment of a base registry. These security governance programs are mostly based on the ISO 27001 (or older ISO 17799) standard which offers a standard security governance framework. In some countries, the base registries are regulated by law and specific legislation is applied, based on or comparable with the ISO 27001 standard, as the security governance framework.

18 out of 19 base registries indicated they have some form of Security Governance in place for operation of the base registry. This results in most respondents indicating a maturity level between 3 “Defined” and 4 “Quantitatively Managed” for Security Governance which is considered to be a relatively high score. Some respondents define a maturity level of 2 “Managed” or even 1 “Initial” which indicates that for full interoperability and integration, some countries will need to grow further and become more mature in terms of security governance to obtain efficient and sustainable integration and interoperability with other countries.

The security governance result also includes business continuity and disaster recovery topics. 6 out of the 19 base registries indicated that they do not have business continuity and disaster recovery plans defined for the offered services.

Information Security Classification

Given that base registries deal with authoritative information(i.e. information which the base registry owns), which in many cases is not publically available, information classification needs to be applied to ensure that the requested information is only made available to authorised entities.

13 of the 19 base registries indicated that they apply information classification to the information stored in their base registry. Some respondents indicated that they mostly do not apply information classification because the base registry itself is publicly accessible, and as such does not require classification.

From an integration and interoperability point of view, information classification is an essential feature given that, if base registries were to integrate at an international level, information classification could be required.

Access Control

For the access control questions, a distinction needs to be made between public and non-public base registries. Public base registries are publicly accessible and do not always require user authentication to gain access to the base registry. Therefore, these base registries have lower requirements for Identity and Access Management than base registries storing sensitive information.

The fact that a base registry has an Identity and Access Management platform in place is thus strongly related to the type of base registry and corresponding information classification requirements.

Based on the responses of the questionnaire, it is possible to conclude that when Identity and Access Management is required for the correct operational functioning of the base registry, an Identity and Access Management platform is available.

In most of the sample base registries, information was not publicly accessible and thus only made available to authorised entities. 16 of the 19 questioned base registries confirmed that they have an identification, authentication and authorisation mechanism in place 1) to identify the entity requesting information from the base registry, 2) to authenticate the requesting entity to ensure that the entity can effectively prove its identity and 3) to authorise the requesting party to obtain the information requested based on the information classification and authorisation scheme.

These requirements are fulfilled by most base registries when requesting entities:

- must sign an agreement before obtaining access to the base registry,
- receive a personal identification and authentication token, for example a PKI certificate or username/password,
- are authorised based on a specific authorisation scheme or an RBAC (Role Based Access Control)¹⁰ model.

Compliance

A security policy needs to be enforced and verified and therefore a regular audit of a base registry should ensure that the operational environment of a base registry complies with the defined operational (security) framework.

Regarding compliance, the results of the questionnaire vary in that answers range from “No compliance verification” to “External audit for compliance,” and one country performs daily and bi-weekly checks of transactional information to ensure compliance with defined standards. These results indicate that on a compliance level, a large variety exists between the questioned base registries. These results might indicate that the real operational environment can differ from the defined security and operational policies. If there is a difference between the defined policy and the actual operational environment of the base registry, integration and interoperability between multiple base registries can become difficult.

13 of the 19 questioned base registries indicated that they have an audit program to validate compliance of the base registry with the defined policies and procedures. This implies that 68% of the questioned base registries are able to verify compliance with internally defined policies and procedures, but it also means that 32% of the base registries are unable to prove that the defined policies and procedures are put into practice.

This result can indicate that the generally positive result of the security questions should be put in context and can be an indication that some answers given to the questionnaire do not reflect the real life situation of the operational security environment of the base registry.

¹⁰ <http://csrc.nist.gov/groups/SNS/rbac/>

4.3.6 Summary of results per level and the security dimension

To summarise, on average, the security dimension scores the highest (70% on the scale of maturity) and the semantic level scores the lowest in the sample (only 38% on the maturity scale). It can therefore be said that the highest potential for interoperability is within the security dimension and that there is progress to be made within the semantic level.

The **legal level** is the second best performing (62%). In terms of the legal framework, all respondents indicated its existence, at the national or federal level, but it can also exist at the regional or other level, if the legal “level” exists there. Several respondents indicated that their base registry is not established by a specific legal act, however some respondents identified a legal act for base registries in specific areas (e.g. real estate). In the aspect concerning the requirements for access to information, the legal framework exists for all base registries. In the case of business registries, however, information is available to the public, whereas for other base registries access is restricted to a defined target audience. In addition, some parties, such as governments, have full access to the information in base registries, whilst other, such as companies or people, have restricted access. In terms of legal requirements for quality of information, all base registries in the sample have a legal framework describing how information has to be entered and maintained. For some base registries, however, the update of the information can be undertaken at the request of other parties with administrative duties (e.g. municipality, court, notary etc). As far as the international initiatives are concerned, 10 out of 19 respondents mentioned the EU legal framework and 6 mentioned bi/multilateral agreements with EU Member States. Finally, most of the respondents mentioned legal obstacles to cross-border interoperability such as the international recognition of electronic signature, the transposition of non-legal aspects into law, and the cost of providing information to non-national parties or personal data protection.

Within the **organisational level**, which is third in terms of interoperability potential (60%), land and property registries score the highest (9,5 out of 10 points) and citizen base registries scores the lowest (5,8 out of 10 points), when looking from a base registry type perspective. As far as the aspects within the organisational level are concerned, 11 of the 18 base registries score above average in the positioning towards public services. According to the base registries interoperability model, this means that 11 base registries are potentially accessible to multiple public services and are therefore prepared for interoperability. Within the data organisation aspect, 12 out of 18 base registries score below the average. This indicates that 12 base registries do not meet the cross border interoperability criteria (defined by the base registries interoperability model) requiring a base registry data to be an aggregated logical data repository. For the governing body aspect, most of the base registries (10 out of 19) have a simple governing structure (i.e. 2 to 3 instances contribute to easier communication with external parties as defined by the base registries interoperability model) and a well described governance structure. The remaining base registries (7 out of 19) have a simple structure, but lack a well described governance structure. Within the operational roles and processes aspect, 7 of the 19 base registries completely match the interoperability criteria by having the

operational processes fully documented and audited. The main drawback of the remaining 12 base registries is the lack of an audit of the operational processes.

The **semantic level** is the worst performing level of the five identified (38%). Within the multilingual aspect, only 5 of the 19 base registries have interfaces in more than one language. When it comes to syntactic interoperability 73% of base registries have documentation for data formats that are available for potential integrators. 10 out of 19 base registries have an API for integration of base registries functionalities. 7 of the 19 have web services using the API. As far as semantic interoperability is concerned, 7 out of 19 base registries have a detailed taxonomy available and 3 of these 7 are logically interconnected with other systems using semantic interoperability agreements. 2 of these 7 function in the European context. 10 of the 19 base registries are not compliant with syntactic and semantic standards.

The **technical level** is in fourth place (53%). From the point of view of a typology of base registries, land and property and vehicle registries are the best performers in terms of potential cross border interoperability. Concerning the technological reusability capability, half of the respondents indicated the existence of reusable components for other base registries and within these, 50% indicated a licensing model enabling sharing technology and 50% wish to share their technical components. Another 7 respondents do not have reusable components, however, wish to share them. In regard to the interfacing to other systems, all countries mentioned that their base registries can interface with other systems (XML is the most used interface format). 11 respondents indicated a full documentation and 7 a partial documentation. Within the last aspect, authentication in a cross-border context, 50% of respondents indicated openness towards other European countries in terms of the utilisation of standard authentication mechanisms and openness in case a European third party invests in a PKI infrastructure.

Purely based on the survey results, the **security dimension** is the best performing of the interoperability levels as it reaches the maturity of interoperability context (70%). Knowledge of security concepts and vocabulary is essential in understanding the correct meaning of the survey questions.

As far as the security governance aspect is concerned, most countries have a security governance framework (ISO27001 or older ISO17799) or a compliance legal framework. Within the information security classification, most respondents apply information classification, but others do not as their base registries are publicly available. For the access control aspect, most base registries have their information available to the authorised parties and therefore have an identification, authentication and authorisation mechanism. Regarding compliance, a significant variety in terms of policies exists.

The “good” results of the security dimension can also be explained by the existing attention paid to security and especially the “privacy” aspects in public life.

In a workshop, the ongoing European Interoperability Architecture (EIA) project and the Member States agreed on a draft dependency schema between the EIA levels presented in Figure 18 below. This schema defines the sequence in which the interoperability levels should be followed in order to create/enable the cross border interoperability of base registries. In the

schema, the legal interoperability level is a precondition for the organisational level which in turn is a precondition for the semantic and the technical levels respectively. The security dimension needs to be taken into account within each of the four interoperability levels. The results of the analysis per level indicate the highest score for the legal and organisational levels respectively (see Figure 18 below). These scores are in line with the EIA schema. The semantic interoperability level scores low as the language aspect is still treated locally at present. The technical interoperability level also scores relatively low and progress is needed at this level vis-à-vis cross border interoperability. The security dimension scores very high, which is logical as security is of vital importance within any base registry.

The fact, that even at the legal and organisational level scores are still “modest”, indicates that most of the base registries are serving their “internal” national market and are not organised (yet) for cross-border services. If a base registry were to take initiatives to open up its information to other cross border services, then the percentages at all levels could significantly increase. At the legal level, it should be taken into account that the base registry might not be capable of launching an initiative on its own but that the registry can depend on the national or European administrations for further initiative-taking.

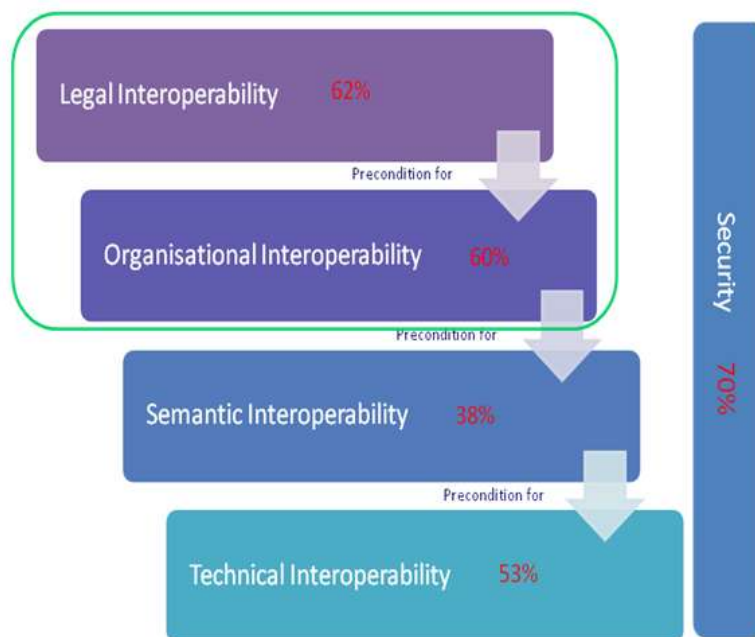


Figure 13. Interoperability levels and the survey results per level and the security dimension.

4.4 SURVEY RESULTS PER TYPE OF BASE REGISTRY

This section consists of an analysis of business and citizen registries as these two types of base registries are representative in the sample (6 business registries, 7 citizen registries) compared to property and land registries (2), procurement information registries (2) and vehicle registries (1). In the analysis per type within the citizen registries, 7 instead of 8 citizen registries were selected as these 7 citizen registries are core citizen registries and thus more representative. The 8th citizen registry provides access to multiple citizen registries. In the analysis per level, 8 citizen registries were retained as the 8th citizen registry could be considered an aggregated citizen registry.

The analysis of the survey results of business and citizen registries proceeds as follows:

- within business and citizen registries clusters, based on data content, were created,
- graphs for each of the four levels (legal, organisational, semantic, technical) and the security dimension were created,
- each graph was analysed and described: comparative analysis between and within clusters were made,
- for each of the four levels and the security dimension for business and citizen registries recommendations were made, based solely on the survey results.

4.4.1 Business Registries

This section describes the sample of base registries with regard to the business registries. It starts with the definition of a business registry and the description of the sample and finishes with the analysis of the survey results and the conclusion.

The overall performance of business registries per level and the security dimension is as follows:

Security dimension	Legal	Organisational	Technical	Semantic
7,83	6,08	5,70	5,10	4,58

Table 4. Business registries and their performance per level.

The following abbreviations are used throughout this section:

- CD: customs declaration registry
- CI: company identification registry
- V: VAT registry

The need for cooperation

In order to leverage opportunities provided by the Single Market with regard to conducting business activities in a cross border context, easy access to company information across countries is needed. The European Commission¹¹ highlights the need to facilitate the access to business registries in order to protect stakeholders and third parties. It also emphasises the need to strengthen business registries' cooperation in the context of cross border procedures such as mergers, seat transfers, establishment of branches and insolvency proceedings. In addition, cross border access to company information reduces cost of conducting business abroad.

As the European Commission mentions, the root services provided by business registries, such as storing and managing company data, are the same across countries. However, the European landscape of base registries is heterogeneous when it comes for instance to data organisation (organised mostly at regional or national level), differences in technology and languages in which the information is stored. These divergences across countries constitute barriers for cross border business activities.

Sample description

The sample contains 6 business registries:

- 3x company identification registries
- 2x vat registries
- 1x customs declaration registry

Among the three company identification registries, two contain data related to registering a new business and one contains the list of entrepreneurs. The VAT registries contain a summary of VAT information used for tax and administrative purposes (e.g. information for VAT refunds). The customs declaration registry contains information about import and export used for tax purposes.

Analysis of survey results – legal level

As mentioned in section 3 (base registries interoperability model), the legal level in the context of cross border interoperability concerns the following aspects:

- Legal authority,
- Legal requirements on base registry access
- Legal requirements on information quality,
- Legal requirements on information availability,
- Privacy and confidential information,
- Review of legal aspects,
- EU legislation.

¹¹ Green Paper. The interconnection of business registries. {SEC(2009) 1492}. Brussels 04.11.2009. COM(2009) 614 final.

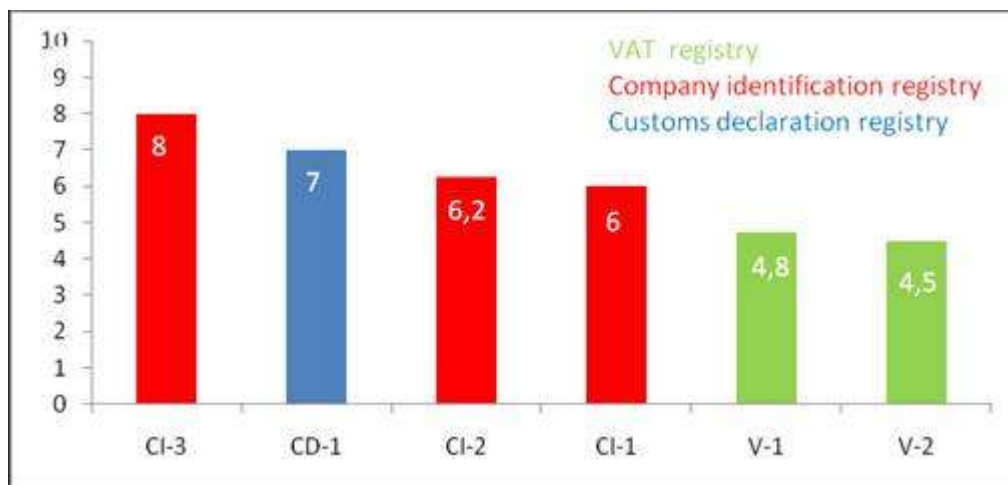


Figure 14. Business registries – legal level.

By looking at Figure 18, it is possible to see that the VAT registries have the lowest performance of the three types of business registries. The V-1 and the V-2 lose points as neither has a legal framework describing how the base registry can be consulted by its users and their legal framework is not currently under review. Moreover, the V-1 does not have (additional) legal rules established to guarantee privacy and the confidentiality of information in a base registry. The legislative framework of the V-2 was created at a lower than national/federal level and there is no legal framework to correct the wrongly entered information in a base registry.

The company identification registry cluster consists of CI-1 and CI-2 registries which perform well from the cross border interoperability perspective and lose points as they do not have any mechanisms for reviewing/updating their legal aspects. CI-1 does not possess a framework describing how a base registry can be viewed by its users neither does it have the legal rules to guarantee the confidentiality and privacy of information. CI-2 is not subject to any legal framework at the EU level.

The customs declaration registry is the second best business registry after CI-3. This is due to the fact that it does not have a legal framework to correct wrongly introduced information into a base registry and it does not have legal rules to guarantee privacy and the confidentiality of base registry information.

Business registries within the legal level score 6,08 out of 10 (see Table 9) in terms of cross border interoperability potential. The survey results within the sample show two VAT and new company registries clusters at different scoring levels. According to the base registries interoperability model and the survey results, in order to boost the potential for the cross border interoperability for business registries, it is necessary to introduce a legal framework enabling the correction of wrongly introduced information into a base registry, a legal framework establishing the rules for consulting a base registry by its users, a legal framework to guarantee the confidentiality and privacy of information in a base registry and a mechanism enabling the review/update/modernisation of legal aspects of a base registry.

Analysis of survey results – organisational level.

As mentioned in the chapter 3 (base registries interoperability model), the organisational level consists of the following aspects:

- Positioning towards public services,
- Data organisation,
- Governing body,
- Operational roles and responsibilities.

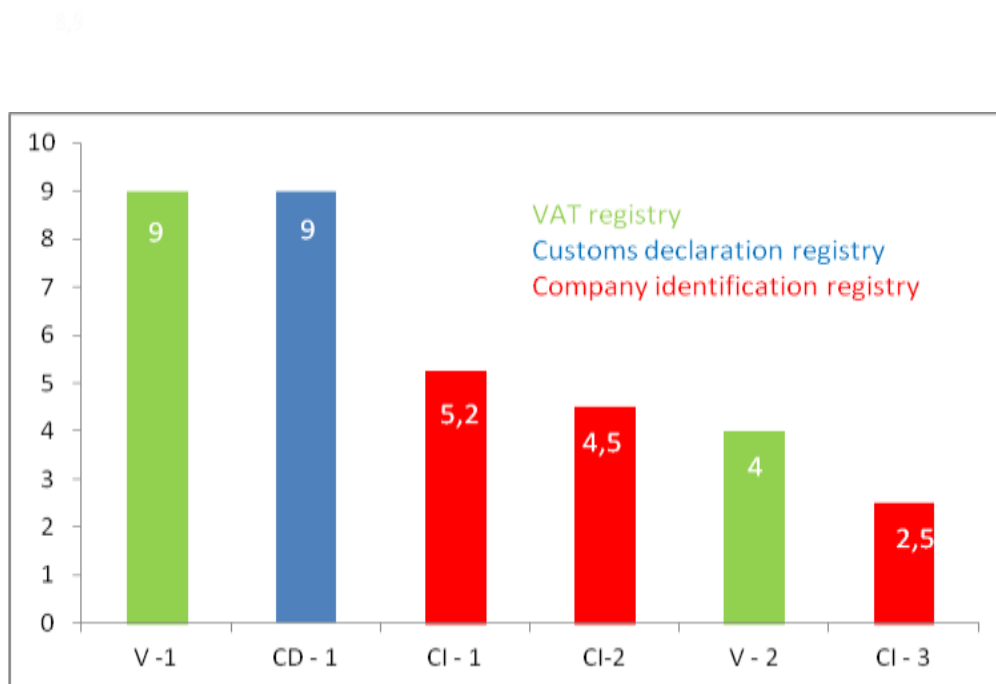


Figure 15. Business registries – organisational level.

By looking at Figure 15, it is possible to observe that the company identification registry cluster performs relatively poorly compared to the VAT and the customs declaration registries. According to the survey results, the low score of company identification registries is mainly due to the lack of best practices and audit of operational processes, as well as due to the lack of a simple governing structure (2 to 3 instances) and a well described governing model. However, the company identification registry CI -3 scores the lowest as this registry is part of a process of transition from a paper into an electronic eGovernment service and the respondent was not in a position to answer all of the questions. Taking into account the scoring model described above and the weights attributed to each of the sub-levels, the high score of V-1 and CD-1 can be attributed to the existence of a simple, well documented governing body (2 to 3 institutions) based on best practices and audited operational processes. Business registries within the organisational level score 5,46 out of 10 points (see Table 9) which positions this level in third place in terms of a cross border interoperability potential. As mentioned above, in order to enable the cross border interconnection of business registries, it is necessary to focus on the establishment of a simple governing body and a governing model, to follow best practices for processes and to perform an audit.

Analysis of survey results - semantic level

As mentioned in the chapter 3 (base registries interoperability model), the semantic level; in the context of cross border interoperability, concerns the following aspects:

- Multilingual framework,
- Syntactic interoperability,
- Semantic interoperability.

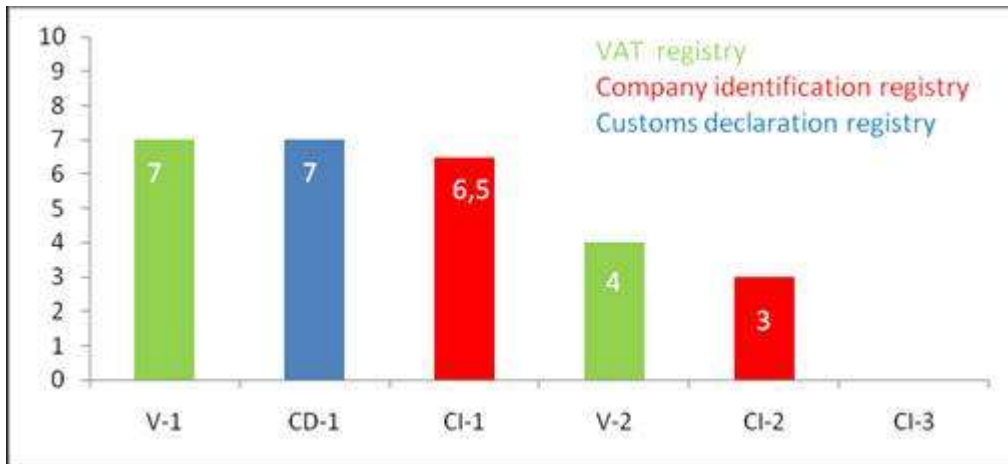


Figure 16. Business registries – semantic level.

Figure 23 shows a heterogeneous performance within the VAT and the new company registry clusters. According to the survey results, the main difference between V-1 and V-2 is that V-2 has neither the detailed taxonomy description available nor a single standard on semantic or syntactic compliance. Within CI it is interesting to examine the difference between CI-1 and CI-2 - CI-3 scores 0 as no answer to the semantic question was provided. The main difference in the performance of CI-1 and CI-2 is that the data format of CI-2 is not described in a document available for potential integrators. In addition, CI-2 does not have an API allowing the use of base registry functionalities in other applications, an API is not publicly available for other developers and no web services use the base registry's API. As in the previous levels, the CD-1 registry scores well and loses points with regards to the multilingual framework as a base registry data and interface are only available in one language.

Business registries within the semantic level score 4,58 out of 10 (see Table 9) in terms of a cross border interoperability potential. This is the worst performing level. The survey results indicate that a detailed taxonomy description is needed for a base registry, in addition to a semantic or syntactic compliance standard. Furthermore, the data format should be described in a document available for potential integrators and there should be an API enabling the use of a base registry in other applications. Moreover, an API should be available for other developers and other web services should be able to use the base registry's API.

Analysis of survey results – technical level

As mentioned in the chapter 3 (base registries interoperability model), the technical level, in the context of cross border interoperability, concerns the following aspects:

- Technical reusability capability,
- Interfacing to other systems,
- User (human) interfaces,
- Authorising third party users,
- Authorising users.

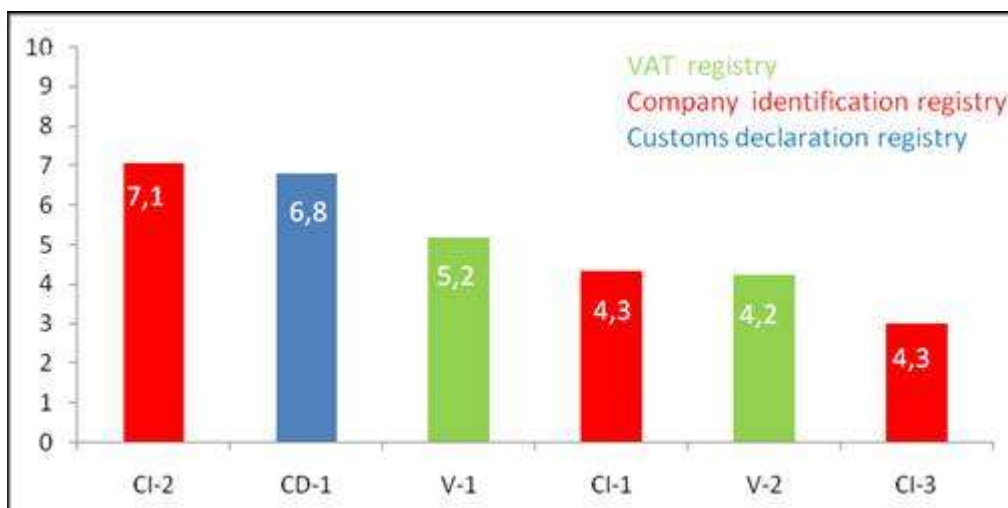


Figure 17. Business registries – technical level.

By looking at Figure 17 no trends can be observed as the clusters of business registries are dispersed. This suggests heterogeneity with regards to the technological aspects across countries in the sample. It is interesting, however, to examine the reason for the differences within the new company registry and the VAT registry clusters. As at the organisational level, the low score for CI-3 is due to the ongoing transition of the project described in the previous section. The main difference (taking into account the weights in the model) between CI-1 and CI-2 stems from the lack of (open) Identify and Access Management technology and the lack of the governance model for the authorisation of third party users in the cross border context. Within the VAT registries, V-2 loses points as the user interface of the base registry is not based on open standards for potential foreign users and because the governing organisation is not willing to make the reusable base registry technology components available. CD-1 owes its second position among the business registries to the fact that its user interface is only partly documented and is based on old, open standards.

Business registries within the technical level score 5,10 out of 10 points (see Table 9) which positions this level in fourth place in terms of cross border interoperability potential. The survey results within the sample of business registries reveal heterogeneity within business registries clusters. The necessary improvements in terms of cross-border interoperability are open technology and a governance model for identification and authorisation of access to base registries as well as the possibility of international sharing of base registries' reusable components.

Analysis of survey results - security dimension

As mentioned in chapter 3 (base registries interoperability model), the security dimension, in the context of cross border interoperability, concerns the following aspects:

- Applicable security policies,
- Security governance,
- Information security classification,
- Access control,
- Compliance.

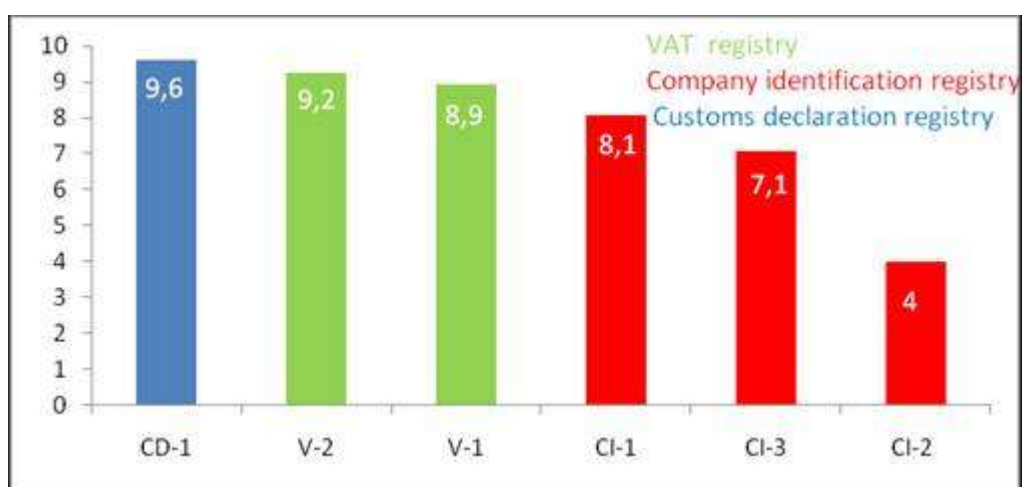


Figure 18. Business registries – security dimension.

By looking at Figure 18 it is possible to clearly observe aggregated clusters of business registries. The best performing registry, in terms of potential for cross border interoperability, is CD-1. It only loses points with regards to its security governance model which is quantitatively managed (processes managed and controlled) instead of focusing on a process improvement (being the best contributor to cross border interoperability according to the base registries interoperability model). The second best performing business registries is the VAT cluster. V-1 and V-2 lose points when it comes to the security governance model, which is characterised by defined processes without a focus on a process improvement, and for the disaster recovery plan. The CI cluster is more diverse than the V cluster. The differences between CI-1 and CI-2 stem mainly from the fact that CI-2 has a security governance model characterised by unpredictable, poorly controlled and reactive processes, while CI-1's security governance model has managed and controlled processes that better contribute to cross border interoperability according to the base registries interoperability model (for details see 3.2).

Business registries within the security dimension score 7,83 out of 10 (see Table 9) in terms of cross border interoperability potential. This is the best performing level. The survey results within the sample show that improvements are necessary in terms of the security governance model and its processes. None of the business registries' security governance models focus on process improvement which is the highest scored contributor to cross border interoperability according to the base registries interoperability model.

Business registries- recommendations

The table below (Table 5) summarises the necessary improvements for the cross border interoperability identified within the survey results per level for business registries. The recommendations come from the drawbacks identified in the above analysis.

Level/dimension	Recommendation
Legal	It is recommended to establish a legal framework to define requirements on the correction of wrongly introduced information into a base registry. This feature is recommended as, in order to be reliable and valid, data should be changed under a supervision of a legal mechanism.
	It is recommended to establish a legal framework ruling how a base registry is to be consulted or consultable by its users. The feature is another element that contributes to reliable and valid data repository.
	It is recommended to establish a legal framework to introduce additional measures to guarantee the confidentiality and privacy of information in a base registry. This feature is another contributor to reliable and valid data repository.
Organisational	The establishment of a simple governing body (2 to 3 instances) is recommended with at least one instance responsible for a base registry and one instance responsible for the operations of a base registry. A simple governing body contributes to cross border interoperability as external parties have a clear understanding of who to contact.
	A governance model for operating a base registry is recommended as clear definitions of processes, roles and responsibilities are an important element of transparency required in a cross border communication and interconnection between base registries.
	It is recommended to follow best practices (e.g. ITIL®) as a basis of definition of operational processes for base registries. Best practices can be seen as a reference framework inspired by proven cases of effectively and efficiently functioning processes.
	It is recommended to perform regular audit of operational processes to avoid divergences from initially implemented processes based on best practices.
Semantic	A detailed taxonomy description for a base registry is required in order to make sure that different definitions, concepts, elements within data entries are correctly understood across countries.
	A syntactic/semantic standard applied to a base registry is recommended as, in order to have an efficient information exchange, a standard format and a common understanding of information exchanged across countries.
	A data format described in a document available for potential integrators is necessary as clear rules of data format are needed for efficient data exchange.

Level/dimension	Recommendation
	An API enabling the use of a base registry in other applications, an API publicly available for other developers and an API that can be used by other web services are recommended as these technical features clearly contribute to the opening up of a base registry towards other applications/web services, which is a basic requirement of interoperability.
Technical	<p>An open technology and governance model for identification and authorisation of access to base registries is recommended in order to ensure transparent governance of access to base registries.</p> <p>An international sharing of base registries reusable components is recommended as it increases productivity saves time, reduces costs and allows the interoperability between applications.</p>
Security (dimension)	A security governance model is required to help a base registry, via defined processes, to comply with security policy.

Table 5. Recommendations for business registries.

4.4.2 Citizen registries

This section describes the sample of base registries with regards to the citizen registries. It starts with the definition of a citizen registry and the description of the sample and finishes with an analysis of the survey results and the conclusion.

The overall performance of citizen registry per level and the security dimension is the following:

Legal	Security dimension	Organisational	Technical	Semantic
6,06	6,05	5,19	4,94	3,56

Table 6. Citizen registries and their performance per level and the security dimension.

The following abbreviations will be used throughout this section:

- E: foreign employees,
- FN: fiscal number registry,
- P: persons registry.

The need for cooperation

One of the four freedoms of the European Union provided by the Single Market is the freedom of movement. It refers to the right for citizens to travel, live, work (permanently or temporarily) or study in another country. The freedom of movement gains special importance in the context of today's financial crisis when people leave the countries touched by the difficult economical situation and move to other countries. It should, however, not only be facilitated by cross border interconnection of base registries, but it should also enable the states to have a transparent view on information about its citizens.

Sample description

The sample consists of 7 citizen registries:

- 5 persons registries,
- 1 fiscal number registry,
- 1 foreign employees registry.

The persons registries contain birth, marriage and death registries for the civil status of the persons and the other persons registries contain baptism details and adoption details. The fiscal number of persons registry contains data used for tax purposes and the foreign employees registry contains data about medical expenses of the foreign employees.

Analysis of survey results – legal level

As mentioned in the section 3.3, the legal level in the context of cross-border interoperability, concerns the following aspects:

- Legal authority,
- Legal requirements on base registry access
- Legal requirements on information quality,
- Legal requirements on information availability,
- Privacy and confidential information,
- Review of legal aspects,
- EU legislation.

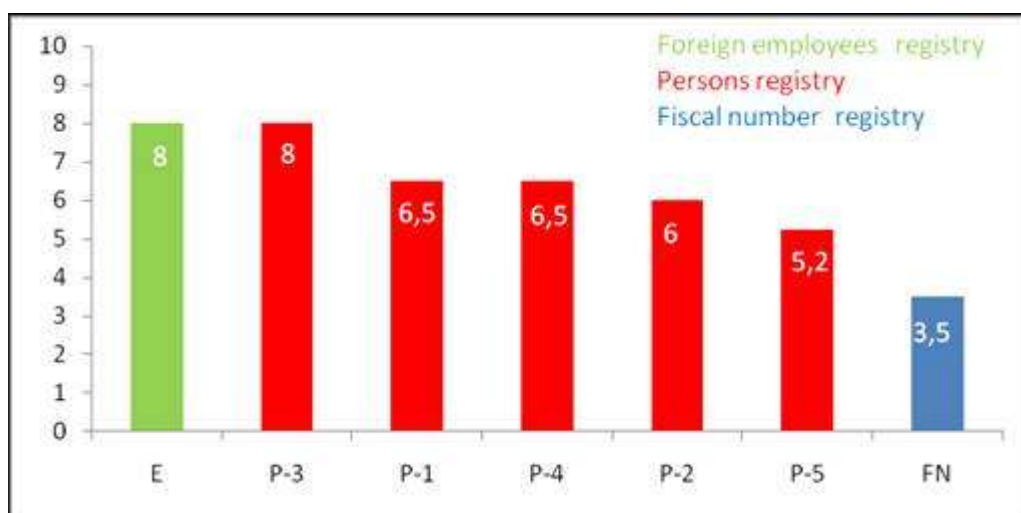


Figure 19. Citizen registries – legal level.

Figure 19 shows an aggregated cluster of persons registries revealing a variety of scores within the cluster. It is interesting to examine the reason for differences between P-3 and P-5. The main difference, according to the survey results and the model, comes from the fact that P-5 is only available to parties / organisations / companies which have received authorisation from an internal structure, as opposed to P-3 which is available for the public (the highest scored factor in the model). In addition, P-5 is not subject to any initiatives that optimise/modernise/review the legal aspects of the base registry. The E and the FN registries are at the extreme ends of the score scale in this level. The E registry loses points due to the fact that it is not subject to any EU legislative frameworks. The FN registry performs much worse as it lacks a legislative framework that guarantees confidentiality and privacy of information stored in a base registry, as well as a framework describing how the base registry should be consulted. This citizen registry is neither subject to initiatives that would optimise/modernise/review its legal aspects, nor is it subject to the EU legal frameworks.

Citizen registries within the legal level score 6,06 out of 10 (see Table 6) and position themselves in first place in terms of cross border interoperability potential. The survey results call for progress in the availability of the information stored in a base registry (availability to public is the highest ranked factor). It is also recommended that a base registry's information is optimised/modernised/reviewed according to a legal framework and that a base registry is subject to the EU legal framework. In addition, there should be a legal framework defining how a base registry should be consulted.

Analysis of survey results – organisational level

As mentioned in section 3 (base registries interoperability model), the organisational level, in the context of cross border interoperability, concerns the following aspects:

- Positioning towards public services,
- Data organisation,
- Governing body,
- Operational roles and responsibilities.

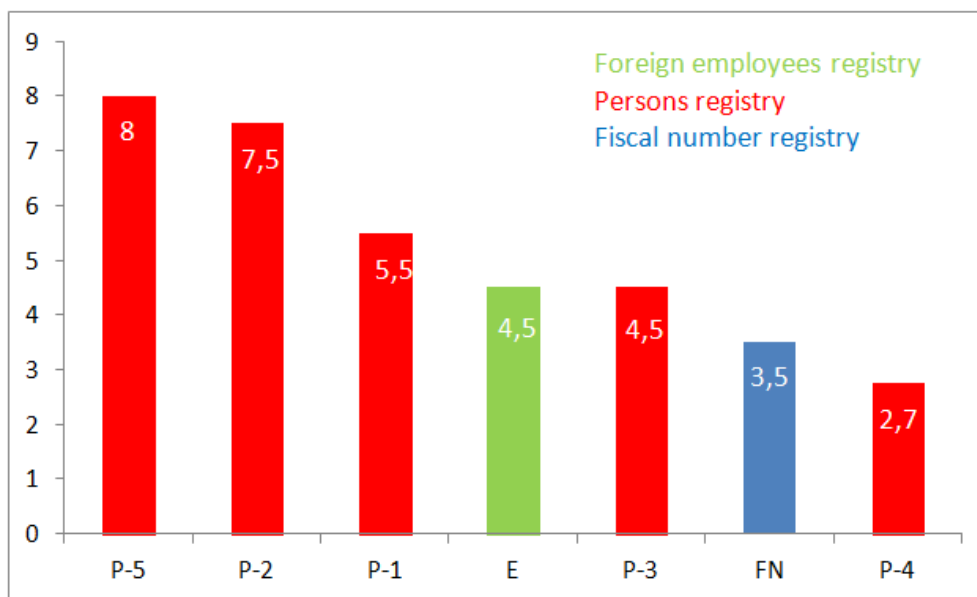


Figure 20. Citizen registries – organisational level.

Figure 20 illustrates the division of the persons registry cluster into two groups, which is an interesting aspect to examine. According to the survey results and the base registries interoperability model, the main difference between P-5, P-2, P-1 and P-4 stems from the fact that P-4 does not have either fully documented processes on which audit is performed, or a simple governing structure (2 to 3 instances) with well described functions of governing process, compared to P-5, P-2 and P-1. The E registry scores poorly in terms of not documented processes, non existing best practices and the lack of an audit. The FN registry owes its low score mainly to partly documented processes, the lack of best practices and the lack of an audit.

Citizen registries within the organisational level score 5,19 out of 10 (see Table 6) and position themselves in the third place in terms of cross border interoperability potential. According to the survey results and to the base registries interoperability model, in order to create opportunities for cross border interoperability, fully documented operational governing processes based on best practices and an audit should be in place. This is not present in the entire sample of the citizen registries. The missing cross border interoperability factor is also the

lack of a simple governing structure and the lack of well described functions of governing processes.

Analysis of survey results – semantic level

As mentioned in the section 3 (base registries interoperability model), the semantic level; in the context of cross border interoperability, concerns the following aspects:

- Multilingual framework,
- Syntactic interoperability,
- Semantic interoperability.

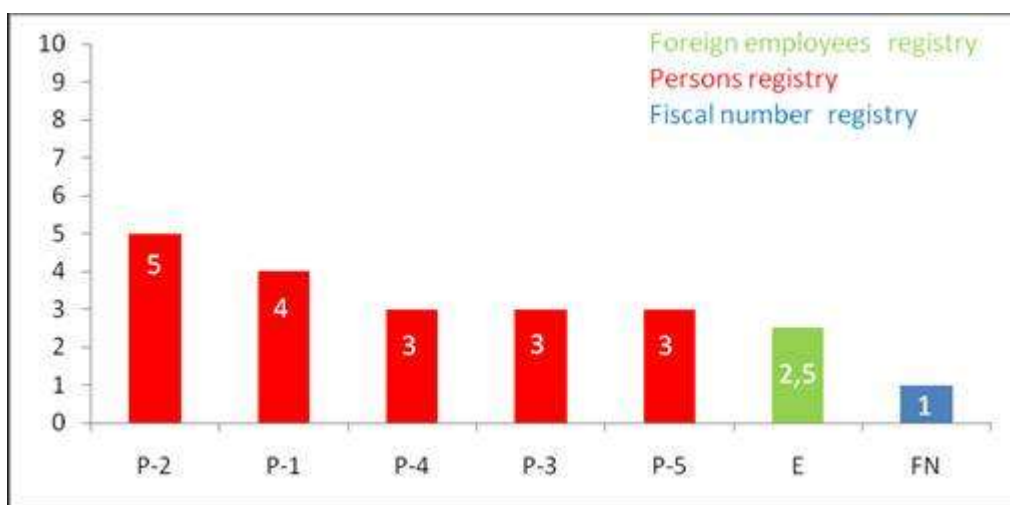


Figure 21. Citizen registries – semantic level.

Figure 21 shows that the persons registry cluster is the highest performing. P-4, P-3, P-5 score lower than P-2 due to the fact that P-4, P-3, P-5 do not have a publicly available API for developers, or any web services that use their API. Moreover P-4 and P-5 do not have an API available to use base registry functionalities in other applications. P-1 scores lower than P-2 as it does not have a detailed taxonomy available for a base registry, it is not interconnected with other systems using semantic interoperability agreements and no single standard on syntactic and semantic compliance is applied to P-1.

Citizen registries within the semantic level score 3,56 out of 10 (see Table 15) and position themselves in last place in terms of cross border interoperability potential. In order to contribute to cross border interoperability, the semantic and syntactic sub-levels need to be improved. In addition to the weaknesses mentioned above, an improvement is also required within the multilingual framework, as none of the citizen base registries have this framework applied.

Analysis of survey results – technical level

As mentioned in the section 3 (base registries interoperability model), the technical level, in the context of cross border interoperability, concerns the following aspects:

Technical reusability capability,

- Interfacing to other systems,
- User (human) interfaces,
- Authorising third party users,
- Authorising users.

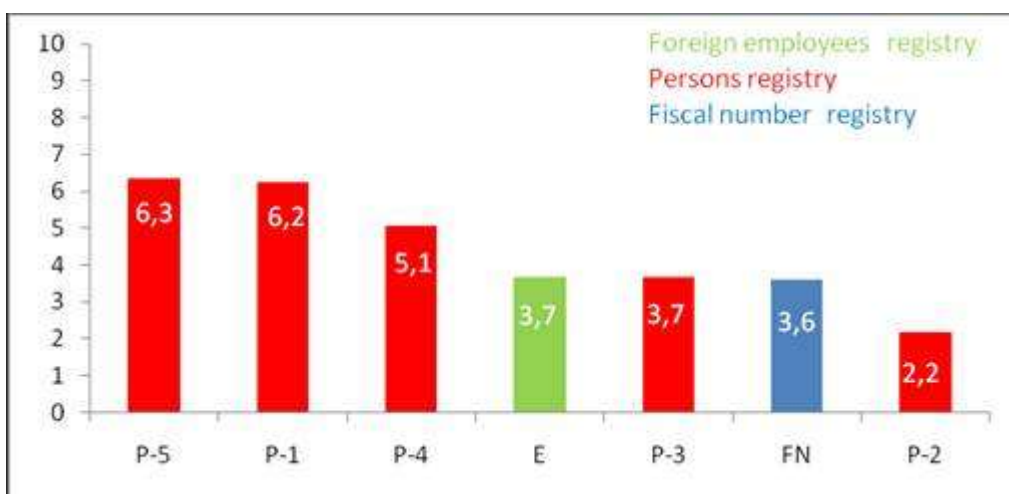


Figure 22. Citizen registries – technical level.

Figure 22 shows that the persons registry forms one group of P-5, P-1 and P-4 scoring higher than P-3 and the P-2. The essential difference, based on the survey results and the base registries interoperability model, between the P-5, P-1, P-4 and P-3, P-2 is that P-3 and P-2 do not have an interface governing model, in case base registries are interconnected, and they do not have the technology to identify and authorise third party users. The performance of the E and the FN registries is comparable to that of P-3.

Citizen registries within the technical level score 4,94 out of 10 (see Table 6) and position themselves in fourth place in terms of cross border interoperability potential. According to the survey results and to the base registries interoperability model, an increase in cross border interoperability potential can be achieved if the citizen registries have a model governing the interface with other base registries (if several base registries are interconnected) and a (open) technology for identifying and authorising third party users.

Analysis of survey results – security dimension

As mentioned in the section 3 (base registries interoperability model), the security dimension, in the context of cross border interoperability, concerns the following aspects:

- Applicable security policies,
- Security governance,
- Information security classification,
- Access control,
- Compliance.

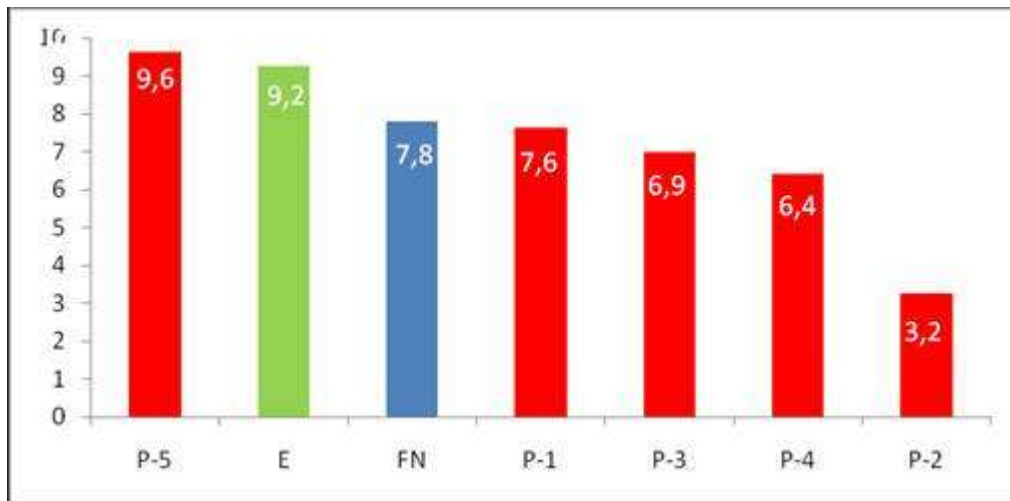


Figure 23. Citizen registries – security dimension.

Figure 23 shows that persons registries are more or less aggregated in one group (which is heterogeneous from the point of view of scores) with P-5 scoring much higher in comparison. According to the survey results and the model, the main difference between P-1 and P-2 is that P-2 does not have an applicable security policy as opposed to P-1. The essential difference between P-5 and P-2 is the lack of the applicable security policy and the lack of security requirements to access P-2. The E registry scores relatively highly in this sample and loses points as the governance model controlling the operational security aspects is based on processes which are controlled and managed without a focus on process improvement (the highest scored element). The score for the FN registry is explained by the lack of a disaster recovery plan and operational security governance model with controlled and managed processes (no focus on process improvement).

Citizen registries within the security dimension score 6,05 out of 10 (see Table 15) and position themselves in second place in terms of cross border interoperability potential. As per the results of the survey and the model, it is recommended to focus on the introduction of security policy and security requirements to access citizen registries. It is also suggested to use a disaster recovery plan and to apply an operational security governance model characterised by processes that are improved on a continuous basis.

Citizen registries – recommendations

The below table (Table 7) summarises the necessary improvements for cross border interoperability identified within the survey results per each level for citizen registries. These recommendations are based solely on the drawbacks identified in the above analysis.

Level/dimension	Recommendation
Legal	A legal framework should define how the information stored in a base registry is made available. This feature ensures that exchanged data is only accessible to predefined public, based on the data content and data classification.
	A base registry should be subject to an EU legal framework as the legal control at the EU level can contribute to protection of (sensitive) data but also streamline administrative procedures.
Organisational	It is recommended to have fully documented operational governing processes based on based practices. Documented processes enable transparent communication and best practices foster trust as they represent tested and successfully followed approaches. A regularly performed audit is recommended as it makes sure that operational processes are constantly in line with best practices.
	It is recommended to establish a simple governing body (2 to 3 instances) with at least one instance responsible for a base registry and one instance responsible for the operations of a base registry). A simple governing body contributes to cross border interoperability as external parties have a clear understanding of who to contact.
Semantic	A multilingual framework understood as a base registry accessible in more than one language plus data stored in more than one language is necessary due to the linguistic diversity of the EU.
	Semantic interoperability should be expressed as: <ul style="list-style-type: none"> - detailed taxonomy of concepts used in data entries - base registry logically interconnected with other systems using semantic interoperability agreements made with other system owners, - single standard on syntactic or semantic compliance applied for a base registry. These elements are recommended as they ensure a clear, mutual comprehension of information stored in base registries across countries.
	An API enabling the use of a base registry in other applications, an API publicly available for other developers and an API that can be used by other web services are recommended as these technical features clearly contribute to the opening up of a base registry towards other applications/web services, which is a basic requirement of interoperability.
Technical	A model governing the interface with other base registries (if several base registries are interconnected) is recommended in order to have a clear understanding of roles, responsibilities and the technology governing the data exchange.
	(Open) technology for identifying and authorising third party users is necessary in order to assure that only authorised users can access the data stored in a base registry.

Level/dimension	Recommendation
Security dimension	A security policy is necessary to establish trust between base registries. In addition, in order for a base registry to comply with the security policy, a governance model (processes, roles and responsibilities, technology) needs to be in place.
	A disaster recovery plan for a base registry is needed to ensure continuity of functioning of a base registry in case of unexpected and unplanned events.

Table 7. Recommendations for citizen registries.

4.4.3 Summary of results per type

Within the business registries the following types of business registries were identified: the company identification registry, the VAT registry and the customs declaration registry. They were analysed through the prism of the five levels defined previously by the base registries interoperability model. Business registries score the highest within the security dimension and the worst within the semantic level. These results are in line with overall performance of all types of base registries.

Within the organisational level the company identification registry forms a clear cluster with one exception being a base registry which is undergoing a transition from a paper to an electronic system of management. The company identification registry scores the lowest due to lack of best practices, audit and a simple governance structure (2 to 3 instances). The highest score is attributed to a VAT registry having a simple governing body, best practices and audit in place.

Within the technical level there is no clear trend as the clusters of business registries are dispersed. The new company registry received the lowest score, however this is the exception mentioned above. The next worst performing business registry is a VAT registry as its user interface is not based on open standards for potential integrators and the technical components are not available for reuse. The highest score is attributed to the new company registry which has an open Identify and Access Management technology and a governance model for authorisation of third party users in a cross border context. Grouped VAT and new company registries can be observed within the legal level. The lowest scoring is a VAT registry as it does not have a legal framework for how to consult its information and it is not subject to a legal review. The highest score is given to the new company registry, due to the existence of the legal framework to correct wrongly introduced information and legal rules to guarantee privacy and confidentiality of base registries information.

Within the security dimension clearly grouped clusters of business registries can be observed. The highest score is attributed to the customs declaration registry which loses some point only due to the security governance model not being focused on the process improvement. The lowest scoring business registry is the new company registry as its security governance model is characterised by poorly controlled and reactive processes.

The semantic level does not reveal a clear grouping of business registries clusters. The highest score is attached to the VAT registry as it has a detailed taxonomy available and it poses a single standard on semantics and syntactic compliance. The lowest score is given to the new company registry due to the fact that it is undergoing a transformation from a paper to

an electronic management system. The second lowest scoring base registry is also a new company registration registry as it has a data format not described in a document available for potential integrators.

Within the citizen registries, the following types of business registries were identified: the persons registry, the fiscal number registry and the foreign employees registry. They were analysed through the prism of the five levels defined previously by the base registries interoperability model. Citizen registries score the highest within the legal level and worst within the semantic level.

It can also be observed that accessibility depends on the nature of a base registry. Business registries and public procurement registries allow access to (part of) their information to the public, while for most other type of base registries, access is restricted by law to a defined target audience.

As far as the organisational level is concerned, there are two groups within the persons registry scoring the highest and the lowest within citizen registries. The lowest scoring group within the persons and overall within the citizen registries are persons registries which do not have fully documented processes on which audit should be performed or a simple governing structure (2 to 3 instances).

In the technical domain, two groups within the persons registry clusters can be observed, scoring the highest and lowest in this level. The lowest scoring group of persons registries does not have an interface governing model or a technology to identify and authorise third party users.

Within the legal domain the highest score is given to the foreign employees registry. The only drawback of this registry is that it is not subject to any EU framework. The lowest scoring citizen registry is the fiscal number registry that does not have additional legal measures guaranteeing confidentiality and the privacy of information stored in a base registry, or a legal framework describing how the base registry should be consulted.

The persons registries are at two extremes of the scoring scale within the security dimension. The highest performing one is a persons registry with a security policy to access its information.

At the semantic level, clearly grouped persons registries can be observed. The highest score is given to a persons registry with a detailed taxonomy available. The lowest scoring citizen registry is the fiscal number registry which received no points for semantic interoperability as it does not have a detailed taxonomy available, any semantic interoperability agreements agreed between system owners and no single standards on syntactic and semantics compliance applied.

5. BASE REGISTRIES' BEST PRACTICES

5.1 BEST PRACTICES PER LEVEL AND THE SECURITY DOMAIN

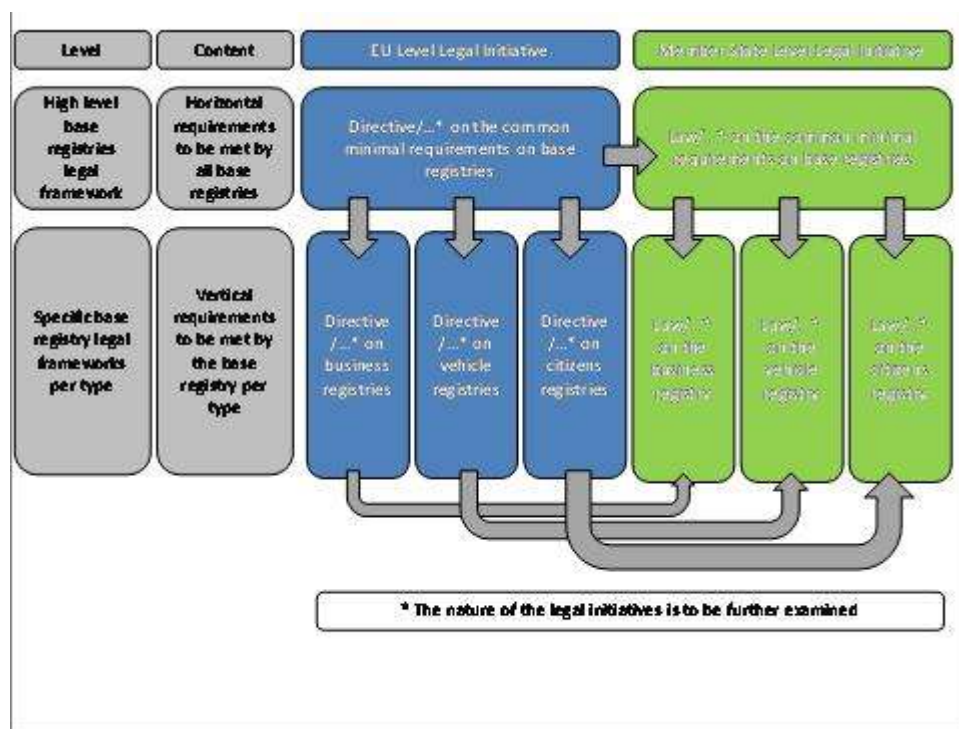
This section will describe best practices on which the base registries interoperability model is based. Next the good practices will be described, based on the survey results. The “best practices” defined in the base registries interoperability model are standards (such as ITIL®, ISO20k etc.), proven experience and the industry best practices. As opposed to best practices, good practices are the practices already in place in a specific context.

Note that the best practices must always be seen in the context of cross border interoperability.

5.1.1 Legal level

Criterion	Best practices	Good practices
<p>Leg. 1: Legal authority</p>	<p>A common understanding of the high level requirements of base registries, unrelated to the country, level or type (i.e. at horizontal level), is required.</p> <p>These high level/horizontal requirements are to be transposed / adopted into the legal framework applicable to a base registry so as to achieve a base line of trustworthiness across EU base registers. To achieve this, the minimum set of high level requirements to be met by each base registry (legal framework) is to be developed at EU level and to be adopted by the Member States to ensure harmonisation at a horizontal level (across base registry types). The nature of the legal initiatives (directive, communication, law, decree, etc) is to be further examined.</p> <p>Furthermore, the specific requirements per base registry type which cannot be identical for each base registry type (such as on accessibility) (i.e. vertical requirements), should also be developed at EU level and adopted by the Member States to ensure harmonisation at a vertical level (per base registry type). The nature of the legal initiatives at EU level may differ, but the legal initiatives at Member State level are to be of a</p>	<p>2 respondents indicated that in their country there is an overarching (legal) framework applicable to all base registries in the country, with which all base registry legal frameworks have to comply.</p> <p>17 out of 19 correspondents indicated that their base registry is regulated by a specific law.</p> <p>In the area of geographic information, respondents indicated the INSPIRE Directive as a driving force for interoperability between Member States.</p>

Criterion	Best practices	Good practices
	<p>legislative nature.</p> <p>These specific/vertical requirements may differ per base registry type or level due to the nature of the base registries. The level of confidentiality or sensitivity, the public or classified character of the relevant data, the need for legal certainty of the information quality, whether it is open to the private sector or not, and many other characteristics will require a specific approach per base registry type.</p> <p>The below figure provides a graphical presentation of this legal framework setup.</p>	



Criterion	Best practices	Good practices
Leg. 1: Legal authority (cont.)	<p>High level requirements:</p> <p>The information held by the base registry is recognised by law as the sole source of authentic information within the level of the base registry.</p> <p>The area/scope of and the data held by the base registry should be clearly defined.</p>	<p>17 of 19 respondents indicated that their base registry is legally recognised as the sole source of authentic information regarding the data it holds.</p>

Criterion	Best practices	Good practices
	<p>The base registries recognised by an EU Member State are recognised by other EU Member States.</p> <p>Public administrations in the EU are obliged to make use of the base registry when they need official authentic information.</p> <p>Information from base registries (complying with the same base registry requirements on quality as mentioned under Legal 3 below) maintained by public administrations in other EU Member States, are recognised as 'trusted data'</p>	
Leg. 2: Access	<p>High level requirement :</p> <p>There are clear procedures related to the accessibility of information held by base registries which should not as such deny the access to non-national parties.</p>	<p>All respondents indicated that the access to their base registry is regulated by law, however only 1 indicated explicitly that the law does not set a restriction on the country of origin of the party requesting access.</p>
Leg. 3 : Quality	<p>High level requirement :</p> <p>There are clear and strict procedures that guarantee the data quality at data entry and during maintenance.</p>	<p>16 out of 19 respondents indicated that there are requirements regarding data quality at data entry.</p> <p>16 out of 19 respondents indicated that there are requirements regarding data quality during maintenance.</p>
Leg. 4: availability	<p>High level requirement :</p> <p>There are clear procedures related to the availability of information held by base registries which should not as such deny the access to non-national parties</p>	<p>12 respondents indicated that the legal framework applicable to the base registry describes how the base registry can be consulted by its (authorised) users.</p>
Legal 5 : Privacy and confidentiality	<p>High level requirement :</p> <p>Base registries apply the appropriate organisational and technical measures to ensure the level of privacy and confidentiality required for the information managed by the base register.</p>	<p>10 correspondents indicated that there are additional legal requirements regarding confidentiality and privacy applicable to a base registry, in addition to the applicable general data protection and privacy laws and regulations.</p>
Legal 6 : Other	<p>High level requirement :</p> <p>The legal framework for base registries should remain</p>	<p>This aspect was indicated as a possible legal obstacle for cross</p>

Criterion	Best practices	Good practices
	<p>technologically neutral, so as to avoid unnecessary legislative adaptations due to technology changes. However, to enable cross-border interoperability a set of minimum technology requirements or targets should be defined so as to achieve interoperability in practice. Such technology requirements are described in the section below.</p>	<p>border interoperability in the survey.</p>
	<p>Requirements to be defined per base registry type: There is a common understanding on semantics, which is transposed where necessary into legal definitions.</p>	<p>This aspect was indicated as a possible legal obstacle for cross border interoperability in the survey.</p>
	<p>Requirements to be defined per base registry type: There is clarity on the financial aspects (costs) of providing to or receiving information from a party in another Member State.</p>	<p>This aspect was indicated as a possible legal obstacle for cross border interoperability in the survey.</p>
	<p>Requirements to be defined per base registry type: The responsibilities of a non-national information receiver are clearly defined (for example : the duty to report erroneous data entries ; the duty to treat the information confidential, if applicable).</p>	
	<p>Requirements to be defined per base registry type: The liability of parties in a cross-border and interoperable information scheme is well defined.</p>	

It is important to note is that the above requirements are only related to the ‘cross-border interoperability’ of base registries, and do not suffice as basis for the ‘general’ legal framework of a base registry.

5.1.2 Organisational level

Criterion	Best practices	Good practices
Org.1: Positioning towards public services	a base registry should be an authentic information source accessible by multiple public services	12 out of 19 base registries in the sample indicate a potential of being accessible by multiple public services
Org.2: Data organisation	a base registry data should be a collection/aggregation of logical data repositories; this feature expresses the readiness of a base registry to cooperate/interconnect with other base registries	6 out of 19 base registries have their data organised as a collection/aggregation of logical data repositories
Org. 3: Governing body	a base registry should be governed by a simple structure (2 to 3 instances), its governing processes (roles and responsibilities, reporting, meetings frequency) should be clearly described; this makes a base registry open to other base registries' governing structures	10 out of 19 base registries have a simple governing structure and well described governance model; the remaining 7 base registries have a simple structure but not well described governance model
Org.4: Operational roles and responsibilities	a base registry's operational processes should be based on best practices that are fully documented in a process handbook and audited against it; this transparency of processes enables an interconnection of base registries as processes can be mutually adapted in order to work together	7 out of 19 base registries indicate fully documented processes and existence of audit controls; 6 out of 19 base registries indicated the use of ITIL® best practices; other base registries indicate best practices like "research practices", in-house developed best practices, legal framework, IDABC functional requirements

5.1.3 Semantic level

Criterion	Best practices	Good practices
Sem. 1: Multilingual framework	A base registry should have a data model which is ready to accommodate different languages. In a European cross border context, the public interface of the base registry at least should be available in all official EU languages.	5 out of 19 base registries have an interface in more than one language. For 3 out of 5 base registries, multilingual aspects are limited to an interface in more than one language, including examples of "business registries" from "small language groups". Only in 2 registries data was also available in more than one language in countries with more than one official language.
Sem. 2: Syntactic	A base registry should have its data format defined via grammars, formats	73% of the assessed registries in the sample have documentation about their

Criterion	Best practices	Good practices
interoperability	<p>and schemas.</p> <p>An API needs to be available for other information providers (public or for internal use depending the nature of the information) to use base registry functionalities in other applications.</p> <p>Syntax checking needs to be implemented for external exchange of data.</p>	<p>data formats available for potential integrators.</p> <p>10 out of 19 base registries have an API for the integration of base registries functionalities into other applications and only half (5 out of these 10) are publicly available for the use of third party developers. In most cases, these public APIs are only intended for reading the data. 8 out of the 18 base registries have web services that use the API.</p>
Sem. 3: Semantic interoperability	<p>A base registry should have a detailed taxonomy description available based on an existing international standard and needs to have an operational interconnection with other system owners.</p>	<p>7 out of 19 base registries have a detailed taxonomy available and only 2 of these registries are logically interconnected with other systems using semantic interoperability agreements made with the other system owners. 2 of these base registries function in the European context.</p> <p>As far as the compliance with syntactic and semantic standards is concerned, 8 out of the 19 base registries are compliant with these requirements.</p> <p>With regards to the typology of base registries, it can be said that the best performers are among the “business registries”. The multilingual performance is mainly low and independent from the typology. The average score for syntactical interoperability is almost 50% in the sample, while semantic interoperability has a result of 38% in the sample.</p>

5.1.4 Technical level

Criterion	Best practices	Good practices
Tech. 1: Technological reusability capability	<p>A base registry should have reusable technology components to enable other public administrations to build/modify their base registries using technology solutions that worked elsewhere; in the case of software components, a licensing model should exist allowing for sharing and reuse; a public</p>	<p>8 out of 19 base registries indicated the existence of reusable technology components (e.g. web interfaces, web services); 6 out of 19 base registries indicated a licensing model allowing for sharing and reuse (e.g. an in-house built framework introducing a web services based technology, open source); 11 out of 19 base registries’</p>

Criterion	Best practices	Good practices
	administration should be willing to share its base registry's reusable components (through documentation, architectural design, source code).	owners indicated a willingness to share their components
Tech. 2: Interfacing to other systems	The Base registry should have a fully documented interface available to connect to other existing systems (e.g. other departments, legal identities ...) and/or new registries; the interfacing technology should be based on open standards for potential use by other European countries.	All base registries have interfaces to connect to other existing systems, however, only 12 out of 19 interfaces are fully documented; 7 out of 19 indicated open standards for interfacing. The vast majority (17 out of 19) uses XML as an interface format. 4 out of 19 registries have a web service available.
Tech. 3: User (human) interfaces	The interface has up-to-date technology increasing efficiency of interoperability.	The following examples of interface innovation were provided in the survey: information can be published and retrieved in up to 4 languages (depending on the publication languages of the buyer), digital signature, internet application for auctioning and registration of vehicles via web from companies
Tech. 4: Authorising third party users	In order to manage access rights to a base registry by third party users, there should be a governance model in place maintaining (create/modify/delete) the interfaces at the European level.	3 out of 19 base registries have an interface governance model in place
Tech. 5: Authenticating third party users	A base registry should function using technology that authenticates and authorises third party users; this technology should be open for use by other European countries.	All base registries have an authenticating/authorising platform; 11 out of 19 have this technology potentially open for other European requestors.

5.1.4. Security dimension

From a security point of view, base registries should apply several best practices to ensure interoperability when communicating with each other and securely exchanging information.

Depending on the type of base registry, the importance given to these security requirements varies, for example a base registry which makes public information available might not require users to authenticate before querying the base registry, while a national registry storing the identities of its citizens is not publicly available and users will need to authenticate themselves and must be given authorisation before information from the base registry can be obtained.

Criterion	Best practices	Good practices
Sec. 1: Applicable security policies	<p>Consider Confidentiality, Integrity and Availability when defining security best practices.</p> <p>Take into account authenticity and non-repudiation principles to ensure that: (1) the base registry can identify itself to requesting entities and vice versa and (2) that queries to the base registries are logged in an audit trail to ensure that a query to the base registry can be proven afterwards.</p>	<p>18 out of 19 base registries indicated that a form of Security Governance was in place for the operation of the base registry.</p>
Sec. 2: Security governance	<p>Consider the industry accepted best practice for security governance (ISO 27001 and ISO 27002 standards).</p> <p>Define the applicable security governance. The security governance model describes how the operational aspects of security are defined. This security governance model describes the organisation itself, defined roles and responsibilities, processes, procedures and used technology that controls the operational aspects of security. ISO 27014 can be used as a reference.</p>	
Sec. 3: Information security classification	<p>Apply information classification on the information stored and made available by the base registry in line with the defined 5 requirements: confidentiality, integrity, availability, authenticity and non-repudiation. This information classification will define what type of security controls are required and how external parties will be able to query the base registry and what information will be made available to them.</p> <p>Use a structural approach in which general security policies should be available which define how the base registry applies security within its day to day operations.</p>	<p>13 out of 19 base registries indicated that they apply information classification for the information stored in their base registry. Some respondents indicate they mostly do not apply information classification because the base registry itself is publicly accessible, and as such does not need to be classified.</p>

Criterion	Best practices	Good practices
<p>Sec. 4: Access control</p>	<p>Set up an identity and access management platform responsible for 3 main tasks: identification, authentication and authorisation of the entity requesting information from the base registry.</p> <p>Use a role-based access control (RBAC) management scheme which allows an efficient and sustainable access control management policy to be defined.</p>	<p>16 of the 19 base registries questioned confirmed that they have an identification, authentication and authorisation mechanism in place: 1) to identify the entity requesting information from the base registry, 2) to authenticate the requesting entity to ensure the entity can effectively prove its identity and 3) to authorise the requesting party to obtain the information requested based on the information classification and authorisation scheme.</p>
<p>Sec. 5: Compliance</p>	<p>Ensure that the information security policies and security governance processes are followed as defined by performing regular security policy and practices audits.</p> <p>Perform security audits on an organisational level and a technical/implementation level to confirm that the operational environment of an organisation is working according to the defined policies and procedures or, if required, steer the organisation when non-compliance with defined policies and procedures has been identified.</p>	<p>The results of the questionnaire vary in that answers range from “No compliance verification” to “External audit for compliance,” and one country performs daily and bi-weekly checks of transactional information to ensure compliance with defined standards. 13 out of the 19 base registries questioned indicated that they have an audit program to validate compliance of the base registry with the defined policies and procedures. This implicates that 68% of the base registries are able to verify compliance with internally defined policies and procedures. It also means that 32% of the base registries are unable to prove that the defined policies and procedures are put into practice.</p>

6. LIFE EVENTS

6.1 LIFE EVENT DEFINITION

According to the IDABC12 programme (Interoperable Delivery of European eGovernment Services to Public Administrations, Business and Citizens, the predecessor of ISA), a life event is an important stage in the life of a citizen, such as registering at a school, getting married or buying a property. In a cross border situation, this process requires cooperation between a home public administration providing data and a foreign public administration, receiving and processing the data.

This section presents a life event scenario for each type of a base registry (see Table 8 below). Each scenario is divided into two parts. The first part consists of a life event taking place in a “perfectly interoperable world”. The second part consists of a life event happening in the context of the “survey world” described solely by the survey results.

Registry type	Life event	Justification
Citizen	Moving to another country	The future municipality should be able to consult the personal data in the former country.
Business	Starting a new business	Registry for a new business (branch, franchise) in another country.
Land	Buying a property	Ability to consult land information in another country to be able to buy it (through an administration or a notary in the residing country)
Vehicle	Addressing speeding tickets (living in another country)	The ability to receive the vehicle information of a foreign car in the context of fines
Procurement	Doing business in another country (e.g. looking for local public sector business opportunities)	Search for tenders for niche expertise opportunities in any European country.

Table 8. Life event scenarios and types of base registries.

¹² <http://ec.europa.eu/idabc/en/document/1644/5848.html>

6.2 LIFE EVENT SCENARIOS

6.2.1 Moving to another country

In a perfect interoperability world, the moving to another country scenario is presented in the Figure 24 below. This scenario involves a citizen registry, and in particular, the persons registry. There are 5 persons; registries in the sample that qualify for the scenario.

Scenario

Mr ABC residing in a country H (home country) is offered an excellent job in a country F (foreign country). He decides to take this opportunity and moves to the country F.

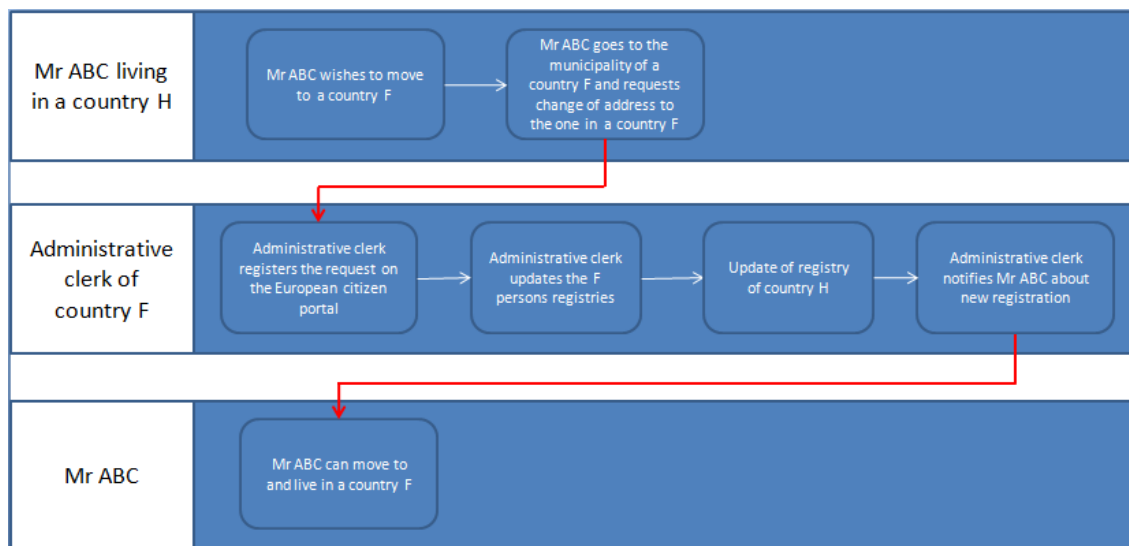


Figure 24. Moving to another country in “interoperable world”.

Survey results

Legal aspects

The action described in the above scenario may be hindered by legal obstacles, mainly due to the below reasons.

All persons registries have a legal framework in place at the national level, which is a good starting point for adapting to the EU level, however it is not clear if the electronic data as such is recognised as ‘official data’ by other Member States. It may be that additional steps are required (such as a declaration of authenticity by the municipality in country H).

Only 2 out of 5 of persons registries are accessible to the public, the others are accessible by specified parties. The respondents remained however vague about the accessibility for parties located in other countries (such as municipalities in other EU Member States).

The legal framework of 4 out of 5 of persons registries defines how the registries can be accessible. The survey results however do not show if these methods are feasible for parties in other EU Member States or if these methods are similar in nature.

3 out of 5 of persons registries have legal rules guaranteeing confidentiality and privacy of stored information, which indicates that there are sensitivities in this area, but that not all countries have taken the same approach, which may hinder development of the trust required for interoperability.

Only 2 out of 5 of persons registries are subject to EU legislation and only 1 persons registry is subject to bi-/multi- lateral agreements at the EU level, which may indicate that little action has been undertaken on modern international information exchange in this area and new EU initiatives may not provide the right basis on which to continue.

There are legal obstacles to cross country interoperability such as the fact that a person registry only operates in one local language, as required by law.

Organisational aspects

3 out of 5 persons registries are potentially accessible by other public services and their operational processes are based on best practices. 3 out of 5 of persons registries' processes are fully documented and audited. Best practices and audit provide a transparent view on the organisation of the functioning of persons registries at present. This is a starting point of further cooperation and interconnection of these base registries in a cross border context.

Semantic aspects

All 5 persons registries have an interface and stored data accessible via one language only. This fact is a considerable obstacle to interconnecting base registries. 5 out of 5 persons registries have data accessible in a format for potential integrators. 3 out of 5 of the persons registries have an API available to use the persons registry functionalities in other applications. Only 1 persons registry has an API publicly available so that application developer can use it. Only 2 out of 5 have web services using the persons registry's API. Only 1 persons registry has a detailed taxonomy description available. 3 out of 5 persons registries have a standard applied on semantic and syntactic compliance.

It is highly likely that. the administrative clerk in country F will have a problem with the language of the base registry of country H.

In most cases, there will be no possibility to consult this base registry from his own system as there are no operational API's to make this happen, and if he can consult the data, there could be a problem to correctly interpret the information due to the different taxonomies.

Technical aspects

All 5 persons registries have an online portal, an interface enabling them to connect to other systems or base registries, and 4 out of 5 of persons registries have a fully documented interface. Only one persons registry has a governance model enabling editing of the interface. A

well-defined governance model facilitates further adaptations in terms of cross border interoperability.

Security aspects

All 5 persons registries have a security policy, however, only 3 out of 5 persons registries classify their information. Information classification is important as it enables the adoption of accurate security measures to protect sensitive data. All persons registries have user authentication and authorisation systems and 4 out of 5 have a security audit in place.

6.2.2 Starting a new business

The process of setting up a business varies greatly throughout Europe. The below scenario illustrates a simplified way of setting up a business in an interoperable world. This scenario involves a business registry and the sample contains 3 business registries related to registering a new company.

Scenario

Mr ABC, owner of the company 123 in a country H (home country), would like to open a new branch of this company in a country F (foreign company) (see Figure 25, below).

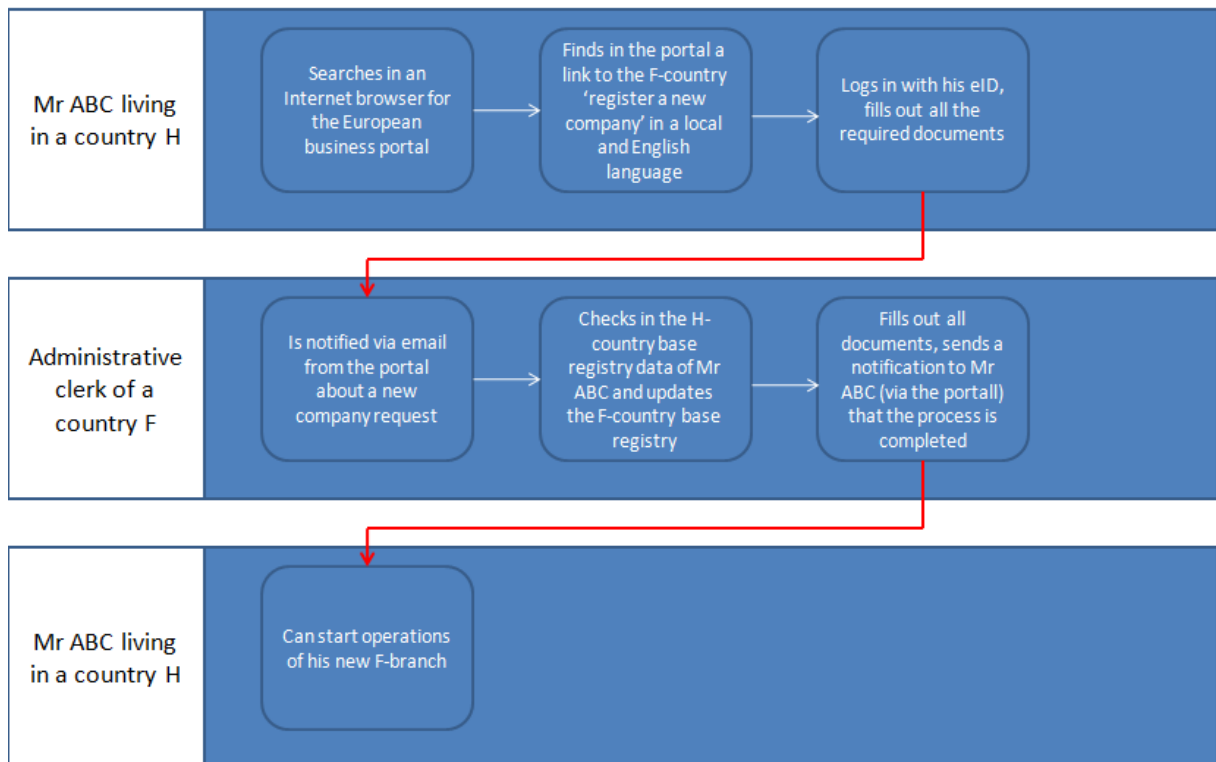


Figure 25. Registering a new company in an “interoperable world”.

Survey results

Legal aspects

The activity described in the above scenario may be hindered by a few remaining legal obstacles, even though there have been EU initiatives in this area. The main points from the survey are presented below.

All 3 business registries have a legal framework regulating their functioning, but only 2 out of 3 registries are subject to the legal framework at the EU level. 2 registries are accessible to the general public and one to government entities only. The survey results show, however, that the public does not get access to all of the data in the base registry, and it does not show the level of access granted to public administration in other EU countries. 2 out of 3 base registries' legal frameworks have a defined set of criteria to access the base registry. 2 out of 3 base registries' legal frameworks have control measures to guarantee the privacy and confidentiality of the entered data, which indicates that there are sensitivities in this area, but that not all countries have taken the same approach. Only one base registry is involved in a bi-/multilateral agreement on cross border interoperability at the EU level, which may indicate that little action has been undertaken on modern international information exchange in this area in practice. One base registry mentions the requirement of the eSignature as an obstacle for cross border interoperability.

Organisational aspects

According to the survey results, 2 out of 3 business registries have an online portal to register a company. 2 out of 3 registries can potentially be available for use/consultation by other services. However, these base registries do not function according to best practices, which is an obstacle from the cross border integration of processes point of view. The use of best practices contributes to transparency and a better understanding of processes in place in different countries. This in turn enables mutual adaption and, as a consequence, cooperation between different base registries.

Semantic aspects

The new company registration portals' interfaces are available in more than one language. For one base registry, the stored data is also available in other language. In the case of one base registry, the API is available to use the base registry functionalities in other applications (web – service). Only 1 base registry functions according to the semantic/syntactic standards.

Technical aspects

All 3 base registries have interfaces which are ready to be connected to other systems. Only 1 out of 3 has a governance model enabling the interface to be edited.

Security aspects

All 3 base registries have a security policy in place, but no audits are performed. 2 out of 3 base registries classify the stored information and have a system to authenticate and authorise the users.

6.2.3 Buying a property

The process of buying a property varies greatly throughout Europe. Buying a property involves many steps undertaken by a real estate agent, a lawyer and an administrative clerk. The below scenario illustrates a simplified way of buying a property in an interoperable world. This scenario involves a land and property registry and the sample contains 2 land and property registries.

Scenario

Mr ABC, residing in country H (home country), wants to buy a property in country F (foreign country). There are 2 land registries in the sample.

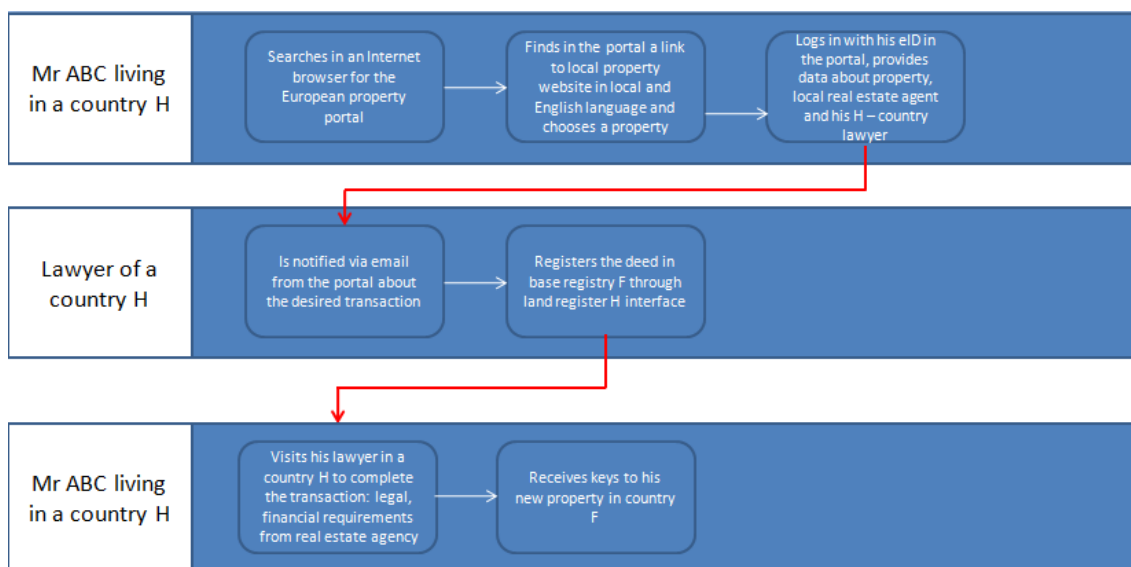


Figure 26. Buying a property in an “interoperable world”.

Survey results

Legal aspects

The activity described in the above scenario may be hindered by the legal obstacles which are presented below.

Both land registries are subject to the legal framework at national level, however it is not clear if the electronic data itself is recognised as 'official data' by other Member States. It may be that additional steps are required (such as a declaration of authenticity by the public administration). The data stored in base registries is available to legally authorised parties such as public administrations. The respondents remained however vague about the accessibility for parties located in other countries (such as municipalities in other EU Member States). The legal framework does not define the rules guaranteeing the confidentiality and privacy of stored data. Recent developments in public online geographic information systems have, however, shown that there are in fact privacy issues related to information in the real estate sector. Therefore, due to the lack of a clear legal framework, obstacles may arise on this area. The respondents from both land registries indicated that their base registries are subject to EU legislation (INSPIRE), which has triggered the move towards more harmonisation. It is however mainly related to geographic information aspects, not the personal or tax information aspects. The respondents also mentioned the legal obstacles to cross border interoperability: the cost of providing the information, edge matching (processing of spatial data) and semantics for geographical information.

Organisational aspects

According to the survey, only 1 land registry has a portal to deal with land properties. Both base registries are potentially accessible by multiple public services. Only 1 base registry's operational processes are based on best practices. However both base registries have their operational processes fully documented and audited.

Semantic aspects

Both land registries are accessible via one language only. The data format is, however, described in a document available for potential integrators. In the case of one base registry, an API enables the base registry's functionalities to be used by other applications. However, no web services use the API. Both land registries are subject of semantic/syntactic standards (e.g. ISO, INSPIRE, GML). Mr ABC, owner of the company 123 in a country H (home country) still has a limited possibility to proceed with the establishment of a new company in another European Member State online.

For Mr ABC, residing in a country H (home country), cross-border transactions concerning properties in a foreign country are still challenging and certain, locally based (meaning in the "foreign country) operations guided by a local representative are required.

Remark: please note that the above analysis is based on the results of the survey. As one will notice, Some EU initiatives, like EULIS, are mitigating on some of the above mentioned interoperability challenges.

Technical aspects

Both registries have an interface enabling them to connect to other system (one base registry has a partly operational interface). In addition, they have a governance model to modify the interface. For only one registry, the authentication technology is open for usage by other European countries.

Security aspects

Both land registries have a security policy in place. Neither applies an information classification system to manage sensitive data. Both registries possess a security policy and a system to authenticate and authorise users. Audit is in place for both.

6.2.4 Addressing speeding tickets

Addressing speeding tickets in the European cross border context contributes to the increase in the security on roads. The below Figure 32 shows a scenario of addressing speeding tickets in an interoperable world. There is only one vehicle registry in the sample.

Scenario

Mr ABC, residing in country H (home country), goes abroad, to country F, for a business trip by car. One day, he drives too fast in the country F and the road safety camera registers this fact by identifying Mr ABC's number plate.

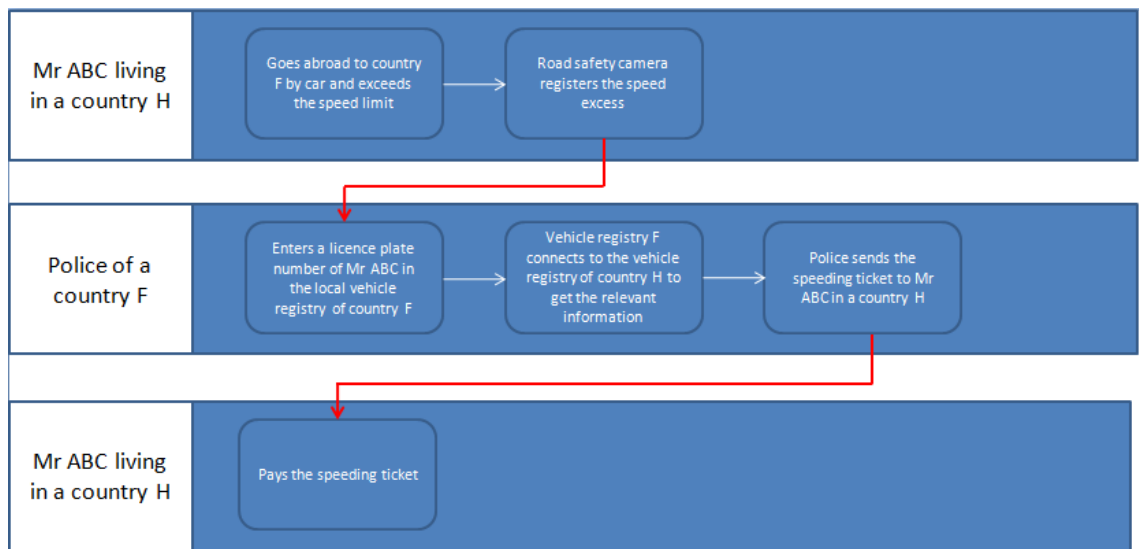


Figure 27. Addressing speeding ticket in an “interoperable world”.

Survey results

Legal aspects

The main legal issue from the survey that would hinder the activities in the above scenario is the lack of an EU framework for cooperation and the recognition of information held by other Member States (even though there are already bilateral agreements in this area), and the obstacles in the area of privacy and personal data protection where the administrations lack a clear legal framework.

Organisational aspects

The vehicle registry has a transport/vehicle portal. It does not have the potential to be accessed by other public services. The vehicle registry operational processes are based on best practices and are well documented.

Semantic aspects

The vehicle registry is accessible via more than language contributing in this way to cross border interoperability. The data is also stored in more than one language. Data is not described in a document available for potential integrators. No other services use the base registry API. No detailed taxonomy is available. No standard on semantic and syntactic compliance is applied to the vehicle registry.

Today, there is a low probability that Mr ABC, residing in a country H (home country), has to pay his speed ticket once back home. There is a legal structure in place but the operationalisation of data interchange remains a hurdle.

Technical aspects

The vehicle registry has an interface available to connect to other systems. This interface has a governance model enabling the necessary modifications. The vehicle registry interface and data are available in English but there is no API available and on the semantic level, no taxonomy defined.

Security aspects

The vehicle registry has a security policy as well as an information classification system in place. The registry has a system to authenticate and authorise users and security audits are performed.

6.2.5 Doing business in another country

Doing business in another country is one of the opportunities offered by the Single Market. The below Figure 33 illustrates doing business in another country scenario in an interoperable world. There are two procurement registries in the sample.

Scenario

A private company 123 located in country H wants to build a new highway abroad and searches for calls for tender in countries F1, F2, F3 and F4.

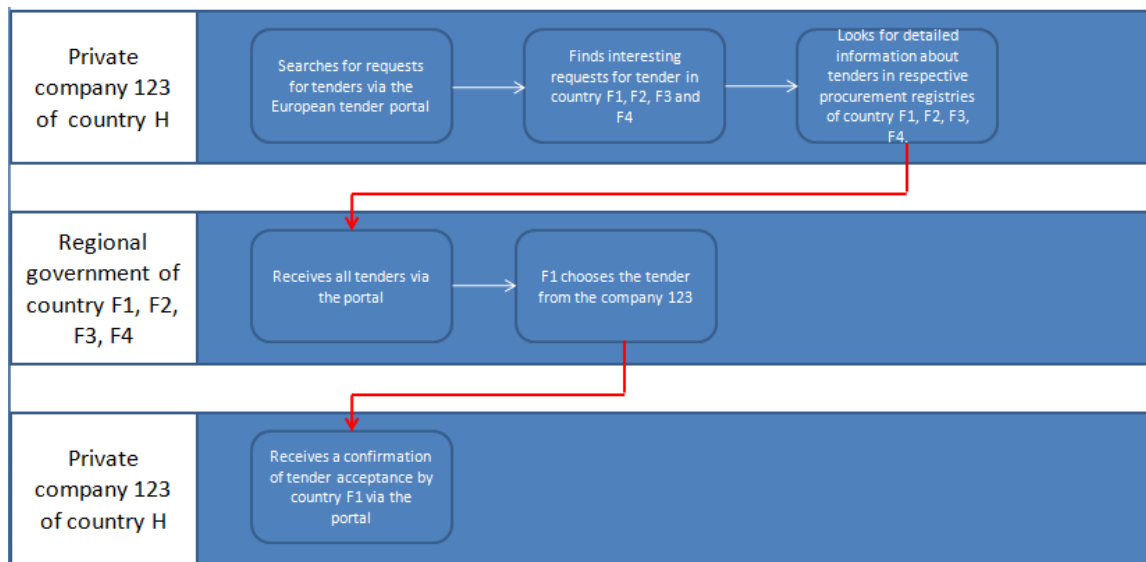


Figure 28. Doing business in another country in an “interoperable world”.

Survey results

Legal aspects

It appears that in this area, due to the initiatives undertaken by the EU, legal steps have been taken to enable the actions taken in the scenario to facilitate cross border procurement information services. The survey indicates the below legal environment.

The procurement base registries themselves are not regulated by a legal framework, but both procurement ‘information services’ are subject to a national legal framework. Due to this different approach, interoperability with other base registries that are regulated by a specific legal framework may prove to be hindered by legal obstacles.

One base registry is accessible to the public and another to parties defined by law.

None of the procurement registries have a legal framework that guarantees the confidentiality and privacy of stored/exchanged information, probably due to the nature of the information.

Only one correspondent indicated the applicability of the EU legal framework and none of the 2 registries are subject to bi-/multi- lateral agreements within the EU.

Organisational aspects

Only 1 out of 2 base registries is accessible online, however both registries are potentially accessible by other services. Both base registries function based on best practices.

Semantic aspects

Only one base registry is accessible via more than one language (both interface and data). The data format of this procurement registry is described in a document available for potential integrators. The API is not available to use base registry functionalities in other applications. 1 procurement registry has a detailed taxonomy description available. No single standard is applied on semantic and syntactic compliance.

Technical aspects

Both procurement registries have interfaces, partly or completely documented, enabling the procurement registry to connect to other systems or base registries. However, no governance model to edit/manage the interface is in place.

Security aspects

The security policy is in place for both procurement registries. Only one procurement registry has information classification in place. Both registries have a user authentication and authorisation system in place, however only one base registry has regular audits.

7. EU INITIATIVES RELATED TO BASE REGISTRIES

This section provides a summary of several EU initiatives and conclusions in terms of recommendations and quick wins that are closely linked to the five types of Base Registers subject to this study. For each type of base registry we highlight those initiatives that have significant impact on these Base Registries in Europe. As explained in annex 2, those initiatives are a subset of the high-level EU initiative inventory, shown in the table below.

Base registry type	EU initiative
Business	Proposal for a Directive as regards the interconnection of central, commercial and companies registers
	Consultation on Green Paper: The interconnection of business registers
	Green Paper: The interconnection of business registers
	Business register - Interoperability throughout Europe -BRITE
	Internal Market Information System - IMI
	The European Business Register - EBR
	Regulations 2157/2001 (on the Statute for a European Company (SE)) and 1435/2003 (on the Statute for a European Cooperative Society (SCE))
	European Parliament legislative resolution of 10 March 2009 on the proposal for a Council regulation on the Statute for a European private company (SPE)
	Multi-Industry, Semantic-based Next Generation Business Intelligence - MUSING
	Services Directive (2006/123/EC)
	First Company Law Directive (68/151/EEC) and 2003 amendment
	11th Council Directive 89/666/EEC on disclosure requirements with respect of branches
	Council Regulation (EEC) No213/85 of 25 July 1985 on the EEIG
	Transparency Directive 2004/109/EC
Cross-border mergers Directive 2005/56/EC	
Citizen, business	STORK - Secure Identity Across Borders Linked
	Effective problem solving across Europe - SOLVIT
Citizen	International Commission of Civil Status (ICCS)
	RISED ID Services GmbH - Electronic Address Verification Services

Base registry type	EU initiative
	e-Justice initiative
	Professional Qualifications Directive (Directive 2005/36/EC)
	European Civil Registry Network -ECRN
Land and property	European Land Information Service - EULIS
	Project LINE
	Cross - borders eConveyancing - CROBECO
Vehicle	Council Decision 2008/615/JHA of 23 June 2008 and Council Decision 2008/616/JH1 of 23 June 2008 and Council Decision 2008/617/JHA of 23 June 2008
	European CAR and driving licence Information System - EUCARIS
Procurement	Commission's 2004 "Action Plan for the implementation of the legal framework for electronic public procurement"
	Green Paper on expanding the use of eProcurement in te EU [COM(2010) 571 final]
	eCertis
	Pan-European Public Procurement Online project - PEPPOL
	Electronic Procurement, Invoicing ad Ordering - Open e-Prior
	Information System for European Public Procurement - SIMAP

Table 9. The five types of base registries and the corresponding EU initiatives.

7.1 BUSINESS REGISTRIES

Proposal for a Directive on the ‘Interconnection of Central, Commercial and Companies Registers’ and related initiatives

Concerning business registries the most recent initiative is the proposal of the European Commission concerning the ‘Interconnection of Central, Commercial and Companies Registers’¹³ that would require the Member States to connect their business registries electronically in order to facilitate cross border exchange of business information. The proposal amends the following Directives:

- Directive 89/666/EEC¹⁴ “to ensure that the business register of a company provides up-to-date information on the status of the company to the business register of foreign branches all across Europe”, through a requirement of an update of data stored in business registries within 15 calendar days from the moment a change occurred.
- Directive 2005/56/EC¹⁵ with the “aim to improve a cooperation framework between business registers in cross-border merger procedures”.
- Directive 2009/101/EC¹⁶ to facilitate “cross-border access to official business information by setting up an electronic network of registers and determining a common minimum set of up-to-date information to be made available to third parties by electronic means in every Member State”.

In addition, the proposal mentions Regulations 2157/2001¹⁷ and 1435/2003¹⁸ that require cross border cooperation between business registers concerning “the transfer of the registered office of European Companies (SEs) and European Cooperative Societies (SCEs)” and refers to a possible amendment of these as part of the review of Regulations. Also access

¹³ Proposal for Directive of the European Parliament and of the Council as regards the interconnection of central, commercial and companies registers, European Commission (COM(2011)).

http://ec.europa.eu/internal_market/company/docs/business_registers/20110224_proposal_en.pdf

¹⁴ Eleventh Council Directive 89/666/EEC of 21 December 1989 concerning disclosure requirements in respect of branches opened in a Member State by certain types of company governed by the law of another State, OJ L 395, 30.12.1989

¹⁵ Directive 2005/56/EC of the European Parliament and of the Council of 26 October 2005 on cross border mergers of limited liability companies, OJ L 310, 25.11.2005

¹⁶ Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent., OJ L 258, 1/10/2009

¹⁷ Council Regulation (EC) No 2157/2001 of 8 October 2001 on the Statute for a European company (SE), OJ L 294, 10.11.2001

¹⁸ Council Regulation (EC) No 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE), OJ L 207, 18.8.2003

to legal information and registers concerning businesses should be fostered by the proposal complementary to the European e-Justice Portal¹⁹.

The proposed Directive provides a number of specific amendments pertaining to business registers, including:

- Member States shall “take the necessary measures to ensure that the registers [...] are interoperable and form an electronic network (hereinafter referred to as the electronic network)”;
- The Commission shall adopt delegated acts concerning: a) the rules concerning the governance, management, operation and representation of the electronic network, [...] d) the minimum security standards for the electronic network, e) the use of a unique identifier, g) the method of transmitting information between the registers ensuring cross-border access to information in accordance with Article 3a, including the choice of the single European electronic platform, h) the interoperability of the information and communication technologies used by the members of the electronic network, including a payment interface, i) the definition of standards on format, substance and limits for storing and retrieving the documents and particulars that enables automated data exchange;
- Unique identifiers for companies and branches “that allows for their unequivocal identification in the European Economic Area”;
- Registers to notify registration and changes in documents and particulars (listed in Article 2 of the Directive) through the electronic network (referred to in Article 4a of Directive 2009/101/EC), and for MS to determine the legal procedure following the receipt of these notifications to ensure that “branches of companies that have been dissolved or otherwise removed from the register are closed without undue delay”;
- Member States shall “take the measures required to ensure that any changes in the documents and particulars referred to in the first paragraph is disclosed within 15 calendar days”;
- Member States shall ensure that these documents and particulars “can be obtained, on application by any applicant, by electronic means through a single European electronic platform accessible from every Member State”, and that “for each document and particular kept in their register ... clear information is attached explaining the provisions of national law according to which third parties can rely on those documents and particulars” (and that fees for this shall not exceed the administrative costs);
- The Commission shall adopt delegated acts concerning: “a) the method of identifying the link between a company and its branch”, and “b) the method of and the technical standards for the transmission of information between the register of the company and the register of the branch”;

¹⁹ See: <https://e-justice.europa.eu/home.do>

- Each MS will determine by law the arrangements for “publicising completion of the cross-border merger in the public register in which each of the companies is required to file documents”;
- The Commission shall adopt delegated acts concerning: “a) the technical standards for the transmission of information between the registries”, and “b) the standard forms of notification of the cross-border merger to be used”.

As noted in the preceding Green Paper²⁰, this has the potential to enhance the cross border trade, facilitates setting up of foreign branches and provision of services across borders in the EU. The Green Paper describes the existing cooperation framework between business registers and considers possible ways forward to improve access to information on businesses across the EU and more effective application of the company law directives. A public consultation exercise was launched by the European Commission in 2009 on possible ways to enhance co-operation between business registers. The result of the consultation showed substantial support for the improvement of interconnected business registries in the EU. The Member States supported the idea of interconnection of business registries but insisted that the added value would only come from interconnecting of all the 27 Member States. In addition, the MS suggested the need for legal requirements of the participation of all MS and a legal basis on the data exchange. The MS also expressed the necessity of updated, reliable and standardised data available in relevant language in order to address the uneven data quality across MS. Substantial appraisal was provided for the Business Register Interoperability Throughout Europe (BRITE) and Internal Market Information System (IMI) initiatives, as well as for the creation of strong legal basis for cross border data exchange.

Clearly, the Directive will, if adopted, have implications for the interoperability of the business registers across the EU on legal, organisational, technical and semantic level. At the technical level, the competent authorities in charge of keeping the business registers in the Member States will need to implement measures to ensure that the registers are interoperable and form an electronic network. The Commission will, under this proposal, have the power to adopt acts that deal with the governance, management and operation of the network as well as the definition of standards for storing and retrieving documents and particulars, security standards, methods and technical standards of information exchange (including the choice of the platform), interoperability of the information and communication technologies used by members of the network, and the method to identify the link between a company and its branch. This delegation of power would foster interoperability by enabling the Commission to determine these legal, technical, operational, semantic, and security elements in relation to the electronic network or single European electronic platform. In addition, the proposal if adopted would require Member States to provide access to the documents and particulars in electronic format to any applicant (through this platform), attach clear information to each document or particular

²⁰ Green Paper, The Interconnection of business registers, European Commission, 4 April 2009, COM(2009) 614 final. http://ec.europa.eu/internal_market/consultations/docs/2009/interconnection_of_business_registers/green_paper_en.pdf

explaining provisions of national law, determine by law the means to publish cross-border mergers and keep information up-to-date and disclose changes within 15 days. Adopting the proposal therefore means that both the Commission and Member State will commit to establishing interoperable business registers on the European level through a single European platform, with a common governance, management and operation as well as shared standards, interoperable technologies and methods for data exchange as well as a shared data model concerning unique identifiers and links between branches.

The two projects mentioned in the Green Paper on the Interconnection of Business Registers, namely Business Register Interoperability Throughout Europe (BRITE) and Internal Market Information System (IMI), are highly relevant for the interoperability for business registers in Europe.

Internal Market Information System (IMI) and Business Register Interoperability Throughout Europe (BRITE) and European Business Register (EBR)

The impact assessment conducted for the proposal of the Directive compared three different cost scenarios for a technical solution that could support the aims of the interconnection of business registers, involving the use of the results of three existing initiatives at EU level:

- 1) building on the EBR and BRITE project,
 - 2) developing a solution combining the EBR with IMI, and
 - 3) building a new network of registers.
- The European Business Register (EBR)²¹ is a network of business registers and information providers from 26 countries whose objective is to offer reliable information on companies all over Europe. It allows citizens, businesses and public authorities to search for a company name or, in certain countries, a natural person through all the member business registers by submitting a single query in their own language. As a result of the search, the requested information becomes available in the language of the query.
 - The 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”²², developed under the IDABC programme (Interoperable Delivery of European eGovernment Services to public administrations, businesses and citizens) during 5 years (2005-2009). The IMI helps user to find the right authority to contact in another country and communicate with them based on translated sets of questions and answers. The Commission has adopted a proposal for a Regulation on administrative cooperation

²¹ See also: <http://www.ebr.org/>

²² See also: http://ec.europa.eu/internal_market/imi-net/about_en.html

through the Internal Market Information System (IMI)²³ on August 29 2011, intended to establish a comprehensive legal framework for IMI, including:

- a set of common rules to ensure that IMI functions efficiently, including clarification of the roles of the different actors involved in IMI;
 - a framework for the processing of personal data in IMI;
 - a list of legal provisions supported by IMI;
 - a list of areas to which IMI could be expanded in the future.
- BRITE is a Sixth Framework Programme research project on integrated register-to-register communications that ran from 2006 to 2009 and aimed to implement novel ICT engineering to establish a new European cooperation instrument for public administrations to effectively respond to changes imposed by EU law and new market requirements, particularly business registers are subject to changes in EU company law. The European Business Register (EBR), a network of business registers kept by the registration authorities in most of the European countries, was the driving force behind this project. The aim of BRITE therefore was to set out, develop and pilot ICT and organizational cross-border solutions for public administrations active in cross-border business registration and related eGovernment areas²⁴. It has thus developed several technical elements allowing business registries to communicate and exchange data.

BRITE developed the BRITE model and platform that aims to help Business Registers to address changes that derive from EU-wide Company Law. The platform that was designed under BRITE for the integration of services (such as: the branch disclosure service, the transfer of seat and a central company names index) will be taken up by the EBR to further offer services in the field of interconnection of business registers in order to offer added value services to the market and to business registers. EBR plans to migrate the current EBR service (providing users with a one-stop-shop service to access the Business Registers databases) on the new platform in 2011 and provide for additional services through 2012²⁵. BRITE has developed a number of key deliverables:

- The BRITE interoperable workflow model: could enable the exchange of information and data in the EU;
- Registered Entity Identifier (REID): enables to identify a business registry via a worldwide unique number;
- An innovative interoperability model, ICT platform and data management instrument for business registries;
- BRITE's infrastructure system should meet high reliability and privacy standards. Several services are related to long term transactions (records) so the system should prevent data loss, data corruption (e.g. by digital signature, document certification).

These deliverables are highly relevant to the interconnection of base registries as they will provide relevant input for establishing the necessary standards, unique identifiers and interoperability model. The results of BRITE could therefore form quick win as a starting point for the implementation of the proposed Directive.

²³ Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('the IMI Regulation'), COM(2011) 522, 29-08-2011

²⁴ See also: http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=78387

²⁵ See also: <http://www.ebr.org/section/68/index.html>

These projects clearly have something to offer in terms of ready developed and tested solutions linked to the interconnection of business registers. In the impact assessment, the third scenario (the 'from scratch' scenario) is discarded on financial and political grounds. Leaving the first and second options for EBR and IMI as well as EBR and BRITE with their respective pros and cons. Quick wins here are the fact that IMI provides a useful electronic tool for cooperation between public authorities without having to invest in software development (it is therefore a highly economic option), however it would provide public access to business information and will not have the automates services developed under BRITE. Opting for EBR however would mean that changes have to be made in its organisation and management to give Member States sufficient control over the network and data transmission²⁶.

The European e-Justice Action Plan 2009-2013, also makes note of the intention to integrate the e-Justice portal²⁷ with the EBR; on the mid to long-term the possibility for a partial integration of EBR into the portal itself will be investigated.

7.2 CITIZEN REGISTRIES

Green Paper on the effects of Civil Status Records

The European Commission published a green paper on 14 December 2010 calling for "less bureaucracy for citizens"²⁸ aimed at "promoting free movement of public documents and recognition of the effects of civil status records". The green paper was also subject to a public consultation. The main issues at hand is the fact that two studies published by the Commission in 2007 and 2008 showed that citizens run into problems concerning civil status records when face with a requirement to legalise documents used between Member States. In the framework of the Stockholm programme the European Commission envisages two legislative proposals in 2013 concerning the "free movement of documents by eliminating legalisation formalities between Member States" and "recognition of the effects of certain civil status records (for instance relating to filiation, adoption, names), so that legal status granted in one Member State can be recognised and have the same legal consequences in another":

- Concerning the free movement of documents of public documents, the green paper notes that the legal framework is fragmented "because it is based on several sources: national laws that differ considerably from one another; a number of international multilateral and

²⁶ Commission Staff working document, Impact Assessment accompanying document to the Proposal for a Directive of the European Parliament and of the Council amending Directives 89/666/EEC, 2005/56/EC and 2009/101/EC as regards the interconnection of central, commercial and companies registers, 2010, http://ec.europa.eu/internal_market/company/docs/business_registers/20110224_impact_en.pdf

²⁷ See also: <https://e-justice.europa.eu/home.do?action>

²⁸ European Commission, GREEN PAPER, Less bureaucracy for citizens: promoting free movement of public documents and recognition of the effects of civil status records, COM(2010) 747, 14-12-2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0747:FIN:EN:PDF>

bilateral conventions which have been ratified by a varied and limited number of countries”, resulting in a lack of clarity and regulation that does not provide legal certainty. Four possible solutions are put forward: a) “The abolition of administrative formalities for the authentication of public documents”, b) “Cooperation between the competent national authorities”, c) “Limiting translations of public documents” and d) and “the European civil status certificate”. Option 1 considers the entire abolition of the apostille and legislation for all public documents, so that citizens could present any original document issued by an MS authority without taking additional steps. Option 2 concerns the effective exchange of information between public administrations in the Member States to foster awareness of records and keeping information up-to-date. Suitable electronic means would be required for this, the IMI system is listed as a possible electronic tool (it would also limit the need for translations of documents) as well as the CIEC platform (resulting from a Commission co-financed research project) concerning the use of electronic means in relation to judicial matters and the organisation of a network of civil registrars. The third option would involve introducing standard forms at least for the most common public documents, which could be multilingual forms produced by the CIEC. The last option builds on the already existing European drivers’ licence passport and suggests the introduction of a European civil status certificate that would exist alongside national civil status records (not replacing national civil status certificates) based on a standardised certificate.

- Concerning the mutual recognition of the effects of civil status records the green paper highlights the major issues that particularly derive from semantic differences between Member States due to different history, culture, and legal systems. Also here different options are explored including: a) “Assisting national authorities in the quest for practical solutions”, b) “Automatic recognition” and c) “Recognition based on the harmonisation of conflict-of-law rules”. These options particularly deal with legal issues and harmonisation of rules.

CIEC/ICCS Platform

The Commission Internationale de l'Etat Civil (CIEC) / International Commission on Civil Status (ICCS) has developed a prototype platform for the exchange of some civil status forms among registries in Member States²⁹. The automated electronic platform allows the form to be sent between public administration in a Member States or by a civil status officer of one Member State to the civil status officer of another Member State (e.g. on the basis of a bilateral agreement). The exchange platform adopts encryption for the communication protocols. Furthermore, secure access is guaranteed by a hardware token. The legal basis of the CIEC platform consists of 32 Conventions, of which 28 are in force and 9 are Recommendations. They can be signed by a Member State of CIEC and by any MS of the Council of Europe and the EU. A comparative law study in the field of personal status “Guide pratique international de l'état civil” was undertaken for civil registrars in different CIEC MS and serves as guide.

²⁹ See also: <http://www.ciec1.org/SommaireAnglais.htm>

European Civil Registry Network (ECRN)

European Civil Registry Network (ECRN)³⁰ is a project co-funded by the European Union under the ICT Policy Support Programme (PSP) that started halfway 2008 and ended in November 2010. It deals with the establishment of a pilot among the Civil Acts Registry of National Administrations to allow safe transmission and certain identification of the Civil Acts and Civil Status exchanged among Local Governments of European administrations. Additional services include information and guidance services for actors of the Civil Registry sector. The developed system is composed of a software framework (the ECR-Platform) that provides the basic functionalities of ECRN and a web application that is the only access point to all these functionalities and enables the secure exchange and authentication of a certificate (e.g. birth- or marriage certificate) from one Member State to another within 2-3 working days through a web-platform whereas this may take up 2-3 months through traditional routes. The specific objectives of the project were to 1) strengthening the administrations' ability to use new technologies to increase the efficiency of local administrative actions; 2) shortening delays for the public bodies to manage procedures and enabling citizens to reply in due time to requests for certification; and 3) enable the public authorities to gain immediate knowledge in case of any changes in a Citizens Civil status. The ECRN project investigated the common requirements for interoperability related to such key enablers such as e-Signatures and e-Identity (concerning the latter it has recently linked up with STORK, a CIP Large Scale Pilot aimed at providing interoperability between electronic identification systems across Member States) and investigated legal rules and obstacles, as well as the principles upon migration from document based to electronic submission of civil status information (e.g. use of XML) and proposes legislative requirements for interoperability.

Registry Information Service on European Residents (RISER)

The project Registry Information Service on European Residents (RISER)³¹ started in 2004 as an innovation project within the European Commission eTEN Programme. The project ended 2010. Since then a company has developed the service, and is now firmly positioned in the market. The RISER ID Services GmbH acts as a data processor on behalf of its customers (e.g. businesses and administrations) who submit inquiries about official address information from several member states of the European Union. RISER provides verification addresses and age to its customers, after verifying that they have proof of their legal interest for that information. The result of inquiry consists of full names and full addresses (and age in some cases) as listed in the respective official register or electoral roll register. Towards the end of 2010 RISER provided information from the official citizen registers of twelve European countries

³⁰ See also: <http://www.ecrn.eu/BBB/>

³¹ See also: <http://www.riserid.eu/home/>

for a total of 250 million inhabitants. RISER was awarded the European Privacy Seal (EuroPriSe) for its data protection and data security measures.

7.3 LAND REGISTRIES

EU level projects: EULIS, Project LINE and CROBECO

The European Land Information Service (EULIS)³², established in 2006, is an online portal enabling access to land registries across European borders. It provides easy access to land and property information for professional customers in Europe, e.g. subscribed land registry customers such as banks, lenders, estate agents and lawyers. It is also a hub of information about different land registration conditions in each country. Its long-term mission is to underpin a single European property market through cross border lending. The service is aimed at professional customers who use land registry information to assist them in their day-to-day work life. It helps with access to land and property information, via computer applications. It is not a database itself, but simply to facilitate excess and retrieval of information through direct access to official land registers in Europe. Currently, 6 land registers are connected to the EULIS service and 15 are pending. Three criteria need to be fulfilled before being able to connect as a land registry: 1) having an online service, 2) provide information to professional users and administer these users, 3) provide 'reference information' about the local land registration environment.

EULIS provides glossary and reference information to understand the terminology used in local environments. Access to land registry information may vary as in some countries one can search the land registry by the name of a person, in other countries by object information (e.g. address). This results in a difference of the extent of information provided across countries.

Related to EULIS is the Project LINE³³ (started in September 2010 for a 2 year period), supported by the Official Justice Programme 2007-2013, and lead by the EULIS initiative, the project aims to develop a sustainable and financially viable solution, to enable new land registry organisations to cost-effectively connect to the next generation EULIS 2.0 platform. EULIS 2.0 is intended to be flexible and future proof in order to cope with the evolving national technical land register systems. Facilitating cross border access and use of legal property, improving the technical results of the EULIS platform is only a part of the project objectives. They also include compliance and alignment with the European e-Justice portal. Further developments will increase data exchange functionalities, by integration features such as e-Signatures and e-Registration.

³² See also: <http://eulis.eu/>

³³ See also: <http://eulis.eu/project-line/>

Cross-Borders eConveyancing (CROBECO)³⁴, is a research project funded by the European Commission and carried out by the European Land Registry Association (ELRA). The leading principle of the project is to take existing circumstances as given and respects these (including legislation, responsibilities or registrars and conveyancers, and existing conveyance systems) and the aim is to set up a European framework for obtaining foreign property (e.g. the sale and transfer or ownership of land between two parties from different Member States). The project has developed a draft of a Cross border Conveyancing Reference Framework (CCRF). The framework is based on electronic communication supporting the need for timely receipt of information from the land registry by conveyancers and of conveyance documents by registrars.

7.4 VEHICLE REGISTRIES

Council Decisions on stepping up cross-border cooperation, particularly in combating terrorism and cross-border crime

In June 2008 the Council published three Decisions³⁵ related to the cross-border cooperation with a particular aim of combating terrorism and cross-border crime. As stated in Decision 615 the provisions of the Decision are designed to improve the exchange of information related to, among others, vehicle registration data. The Decision provides for automated searches on vehicle registration data relating to owners and operators as well as vehicles, on which searches can be conducted only based on the full chassis number or a full registration number. Each Member State should designate a national contact point for incoming requests. Details of the technical implementation and administrative provisions are laid down in the Decision 616 on the implementation of Decision 615. According to Decision 616 the Member States should make vehicle registration data available 24/7 through automated data exchange, and in the event of technical failure agreements on temporary data exchange solutions shall be made through national contact points. Vehicle registration data is described in the data-set specified in chapter 3 of the Annex to the Decision, which provides mandatory and optional data and the search triggers (by chassis Number (VIN), reference data and time by time or license plate number, chassis Number (VIN), reference data and time). For the

³⁴ See also: http://www.elra.eu/?page_id=636

³⁵ Council Decision 2008/615/JHA of 23 June 2008 on stepping up cross-border cooperation, particularly in combating terrorism and cross-border crime, 6 August 2008

Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up cross-border cooperation, particularly in combating terrorism and cross-border crime, 6 August 2008

Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between special intervention units of the Member States of the European Union in crisis situations, 6 August 2008

exchange of data common technical specifications are also laid down in annex to the Decision, the electronic exchange shall take place through the Trans European Services for Telematics between Administrations (TESTA II). Automated searches shall take place using the European Vehicle and Driving Licence Information System (EUCARIS) within a decentralised structure. Secure communication of the data that is handled through EUCARIS using TESTA by sending encrypted XML-messages, the security design is based on a combination of HTTPS and XML signature through an SSL connection. The Decision further specifies authentication of users, user roles, logging and tracing of message exchange and further technical conditions as well as functional and non-functional requirements including security, standards, support and maintenance.

European CAR and driving licence Information System

As mentioned, the European CAR and driving licence Information System (EUCARIS)³⁶ is used for exchange of vehicle registration data between Member States; the legislative provisions discussed above make EUCARIS an integral part of the EU legislative framework. EUCARIS is a communications network (developed within the i2020 Agenda) which allows participating countries to consult and exchange data relating to motor vehicles and driving licences kept in the national registers of affiliated countries. It doesn't make use of a central European database. Each country is responsible for its own registry of vehicle and driving licence information and its own registration procedures, the country pages in EUCARIS provide details of organisations and contact persons in the Member States that handle the vehicle and driving licence registration.

7.5 PROCUREMENT REGISTRIES

Green Paper on expanding the use of eProcurement in the EU, Action plan for the implementation of the legal framework for electronic public procurement,

The Commission's 2004 Action Plan for the implementation of the legal framework for electronic public procurement³⁷, provided a roadmap, establishing a strategy designed to accelerate the adoption of e-Procurement whilst safe-guarding the core principles and

³⁶ See also: <https://www.eucaris.net>

³⁷ Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Action plan for the implementation of the legal framework for electronic public procurement, 13-12-2004
http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf

provisions of existing EU procurement legislation and Treaty. It was intended to encourage the development and use of convergent, accessible, secure but commercially viable solutions and disseminate examples of best-practice. Action was also required to stimulate and orientate the work of the first movers in the field, who had already introduced e-Procurement elements in their legislation or practices, or set up e-Procurement systems. The Action Plan was evaluated in 2010³⁸ and a green paper was published on expanding the use of e-Procurement in the EU³⁹ which was subject to a public consultation⁴⁰. The objective of the consultation was to gather input and ideas on ways to:

- Simplify and improve public procurement administration through ICT.
- Accelerate the transition to e-Procurement: Avoid a new generation of barriers to cross-border procurement, having their origins in different ICT solutions or e-Procurement processes.

The main cross-border barriers to public e-Procurement identified in the consultation relate to: “1) clarifying authentication and identification requirements; 2) enhancing interoperability; 3) providing general requirements for e-Procurement and; 4) standardising and simplifying certificates and requirements”. Particularly concerning enhanced interoperability between e-Procurement systems a call for guidance on minimum requirements is expressed, for example in the form of an interpretive communication, coordination between different existing interoperability initiatives (e.g. the German ‘XVergabe’ cross sector project that enables interoperability between German e-Procurement platforms). Providing general requirements and basic principles concerning the operation and interaction between e-Procurement systems, is also called for. For example the technology should be web-based thereby requiring fewer investments from suppliers, and provide more user-friendliness and be non-discriminatory. In addition, an EU law concerning the Virtual Company Dossier (VCD)⁴¹ (making it legally binding to encourage cross-border recognition), a more uniform technology for e-Procurement and eliminate requirements from Member States for suppliers to be established within the respective Member State. Also administrative barriers to cross-border e-Procurement relating to the submission of documents and certificates could be tackled by “standardising forms and certificates, simplifying rules for certificate requests and facilitating access to existing

³⁸ European Commission, Commission Staff Working Document, Evaluation of the 2004 Action Plan for Electronic Public Procurement, Accompanying document to the Green Paper on expanding the use of e-Procurement in the EU, SEC(2010) 1214, 18-10-2010, http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/evaluation-summary_en.pdf

³⁹ European Commission, Green Paper on expanding the use of e-Procurement in the EU, SEC(2010) 517, 18-10-2010, http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/green-paper_en.pdf

⁴⁰ DG MARKT, Services Working Document, Summary of the responses to the green paper on expanding the use of e-procurement in the EU, http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/synthesis_en.pdf

⁴¹ The Virtual Company Dossier (VCD), developed by the PEPPOL project, is intended to enhance interoperability and simplification of electronic tendering offering, as well as transparency and electronic monitoring of supplier qualifications in public procurements.

certificates". In support of this, some respondents feel that e-Certis⁴² should be established as the central location for pre-qualification documents. Cooperation between VCD and e-Certis is also encouraged.

The consultation showed a clear preference to establish EU-wide standards to support e-Procurement in seven main areas: "1) standardising attestations and selection criteria; 2) standardising e-signatures; 3) standardising e-Procurement platforms; 4) using PEPPOL standards; 5) standardising product classification; 6) further developing e-Certis5; and 7) using CEN standards (European Committee for Standardization)". In addition, the use of open-source solutions for e-Procurement should be encouraged according to 77% of the respondents in a flexible and modular way, 90% of respondents indicated that the Commission should continue to make its own solutions available by for example building on open source e-Prior.

Additional challenges identified include user-friendliness of systems and legislation, language barriers, legal uncertainties and difference across Member States at technological, legal and procedural levels. Concerning language barriers, automatic translation of tender documents, and standardisation of all documents could provide a solution as well as the use of e-Catalogues and improving the Common Procurement Vocabulary (CPV)⁴³.

Related initiatives: e-Certis, PEPPOL, Open e-PRIOR

e-CERTIS⁴⁴ is a free, on-line source of information to help companies and contracting authorities to cope with the different forms of documentary evidence required for cross-border tenders for public contracts. It presents the different certificates frequently requested in procurement procedures across the EU. For each country, information on the most common certificates is organised under common headings, corresponding to the types of documentary evidence mentioned in the EU Procurement Directives. For each heading, each national dataset contains a record broken down into a number of standard fields. This record describes in detail, consistently across the national datasets, the certificates issued in a given country for a specific type of evidence. The system matches equivalent documents across the different national datasets.

The Pan-European Public Procurement OnLine project (PEPPOL)⁴⁵, started in 2008, the project aims at expanding market connectivity and interoperability between eProcurement communities. PEPPOL enables access to its standards-based IT transport infrastructure through access points, and provides services for eProcurement with standardised electronic document format. As an open standardised platform, PEPPOL's infrastructure has been

⁴² E-Certis is an online information tool that provides details of the different certificates and attestations that are frequently requested for public procurement in the 27 Member States.

⁴³ The CPV is designed to meet the requirement of the public procurement sector and provides a multilingual and broad classification covering products, works and services.

⁴⁴ See also: http://ec.europa.eu/internal_market/publicprocurement/e-procurement/e-certis/index_en.htm

⁴⁵ See also: <http://www.peppol.eu/>

designed to interconnect existing networks and bridge individual eBusiness islands in Europe. PEPPOL increases business opportunities for participants and supports interoperability across borders. It facilitates electronic communication among European companies and government institutions in the pre-award and post-award procurement process.

Open e-PRIOR (Electronic Procurement, Invoicing and Ordering)⁴⁶ is an Open Source e-Procurement platform for all Public Authorities wishing to pilot e-Procurement, including its cross-border aspects. It has been developed by the Directorate General for Informatics (DIGIT) in the context of the IDABC e-Invoicing and e-Ordering project. The project aims at a practical implementation of interoperable electronic services at a pan-European level, predominantly within the post-awarding phase of Public Procurement.

In the EU e-Procurement has been on the political agenda already for quite a few years. A recent green paper and consultation on expanding the use of e-Procurement in the EU shows that there are still steps to be taken to encourage more interoperability between e-Procurement systems used by public administrations in the Member States, in particular there is a need for further simplification and to accelerate the transition towards e-Procurement. In the consultation a number of existing project were identified that can provide solutions that can form quick wins to further interoperability of e-Procurement systems and underlying registers.

⁴⁶ See also: <http://www.osor.eu/projects/openeprior>

8. CONCLUSION

The objective of the study is to propose recommendations on cross border data exchange between base registries based on the assessment of the maturity of the interoperability of base registries with regards to the EIF framework.

The assessment of the maturity of the interoperability was performed for each of the EIF interoperability levels (legal, organisational, semantic, technical) and the security dimension, as well as per base registry type (business and citizen registry). The main finding within the analysis per interoperability level comes from the survey results and indicates many weaknesses in terms of the readiness for cross border interoperability across all four interoperability levels as well as within the security dimension. The best performing is the security dimension, which does not reveal significant drawbacks. However, within the legal level, not all base registries are established by a legal act. Moreover, only 10 base registries are subject to the EU legal framework and only 6 are subject to bi-/multilateral legal agreements. As far as the organisational level is concerned, the main finding is that most base registries (12) are not aggregated data repositories (there is no evidence of established communication with other parties). In addition, base registries mostly do not have defined operational processes and generally no audit is performed. Within the technical level, nearly 50% of respondents indicated the existence of a licensing model that enables the sharing of technology. In addition, around 50% of respondents declare openness towards other countries in terms of the utilisation of standard authentication mechanisms and openness in case a European third party invests in a PKI infrastructure. Concerning the semantic level, the worst performing, the main findings suggest that no multilingual framework is in place (base registries are mostly accessible in one language only). Most base registries do not have a detailed taxonomy and only two base registries function in the EU context. To summarise, the EIA, a sequence schema indicating the order in which a base registry should be enabled/created, is proposed. The precondition of cross border interoperability is the legal level followed by the organisational, semantic and technical levels respectively. The results of the survey are in line with the sequence schema as far as the legal and organisational levels are concerned. The security dimension relates to the four interoperability levels. The main conclusions of the analysis per level are:

- legal level: an overarching or specific cross border interoperability framework is required,
- organisational level: the enhancement of transparency and further alignment of best practices is required,
- semantic level: taxonomy alignment is required,
- technical level: an improvement in reusability and opening up of the Identity and Access Management environment to work in cross border context is needed,
- security dimension: a further alignment on best practices and need for security awareness is required.

In order to overcome the gaps, issues and drawbacks identified above, a series of recommendations were provided in the form of best practices per interoperability level and within the security dimension and aspects respectively.

As far as the analysis per type of base registry is concerned, the main findings, based on the survey results, are the following. For the business and citizen registries, the main

drawback within the organisational domain is the lack of simple governing body and a governance model, as well as processes based on best practices and the lack of an audit. Within the technical level, the citizen registries lack a legal framework regulating to whom the stored data is made available. The drawback of citizen registries is that they are mostly not subject to the EU legal framework. Business registries mostly do not have a framework regulating correction of wrongly introduced data, consultation of stored data and the confidentiality and privacy of information. With regards to the security dimension, citizen and business registries mostly lack a security governance model. For citizen registries, attention must be paid to the introduction of a security policy and a disaster recovery plan.

At the semantic level, both types of registries lack a detailed taxonomy and semantic/syntactic standards. In addition, the citizen registries lack the possibility provided by the base registry to be accessible in more than one language and also lack semantic interoperability agreements between interconnected base registries. The business registries do not have a data format described in a document available for potential integrators and also lack an API enabling the use of base registries by other applications or web services and an API publicly available for other developers.

The next part of the study on the life events, provided evidence that in order to reach cross border interoperability, significant improvement is still necessary. The five scenarios analysed (for each of the five base registry types) enabled examples of obstacles to be listed which the base registries face at present within the five interoperability levels. To summarise, none of the five life events scenarios (moving to another country, starting a new business, buying a property, addressing speeding tickets, doing business in another country) is possible nowadays (based on the survey results).

The last part of the study listed all of the EU initiatives relevant to the project scope and the sample of base registries. All but one initiative had a neutral impact or fosters cross border interoperability.

Based on the results, which state that the maturity level is not sufficient to ensure interoperability, recommendations on how to overcome the obstacles that base registries face with regards to cross border interoperability are presented in detail in the deliverable “Final report”.

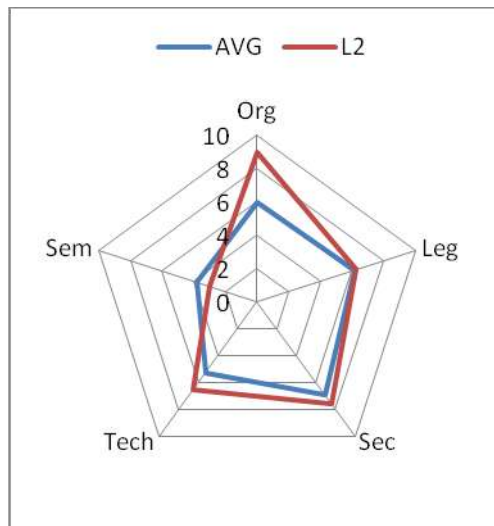
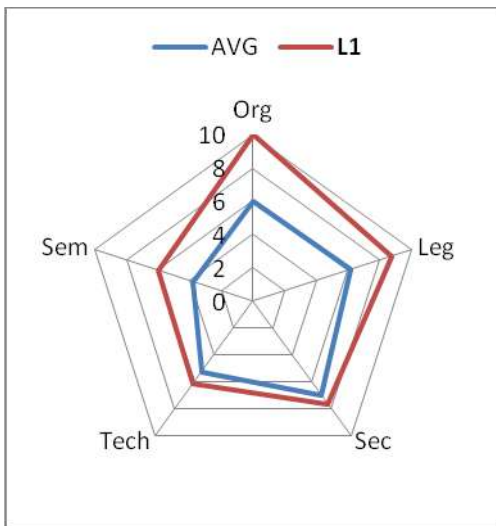
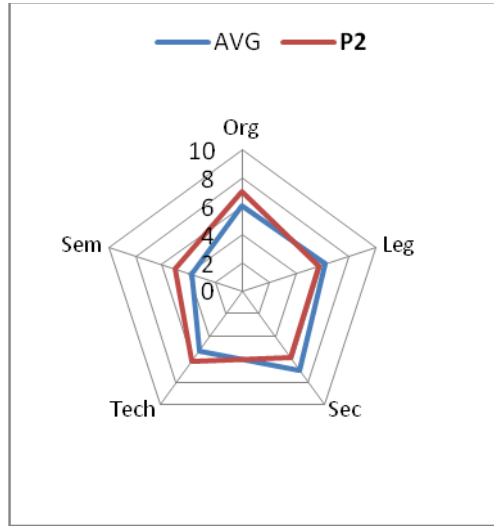
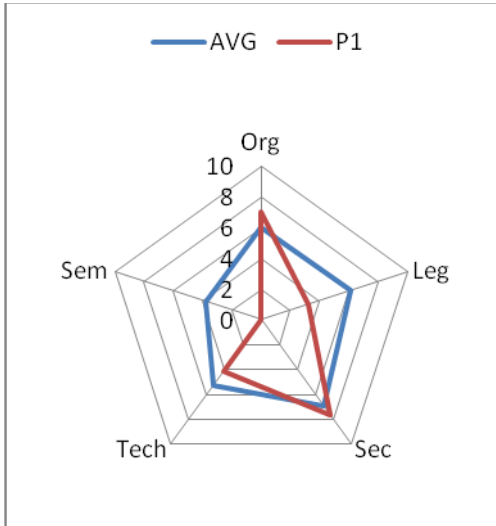
Referring to the online survey itself, it can be concluded that it represents a good instrument with which to start measuring the maturity of base registries. The Member States can use it as a benchmark instrument to assess their base registries’ degree of maturity with regard to cross border interoperability. It can also be said that the quality of results was not homogeneous but depending on the insights of the respondent on the related topics. Therefore, the respondent and the type of questions needs to be carefully selected and matched. Moreover, the European Commission should support the coordination of information gathering by the Member States.

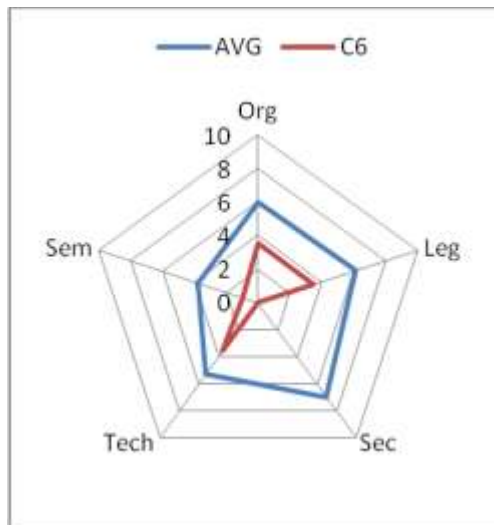
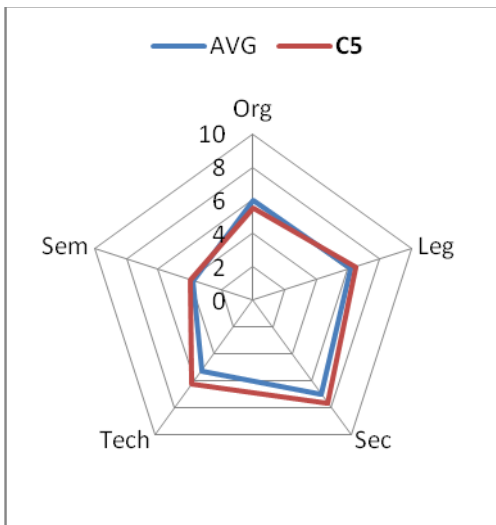
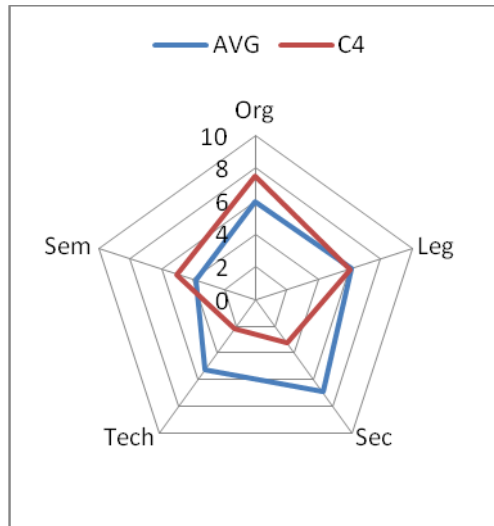
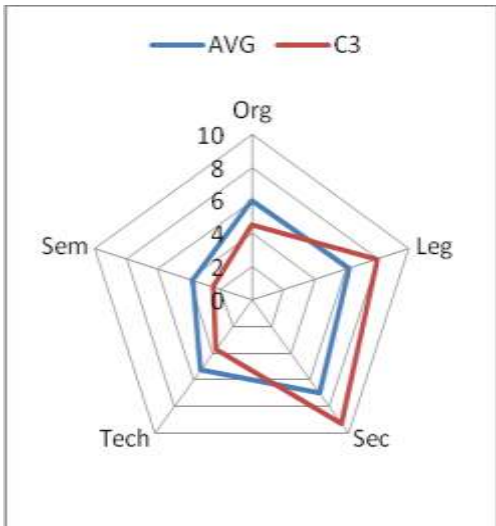
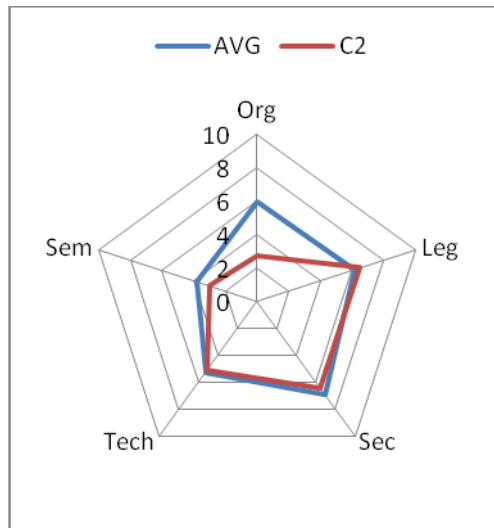
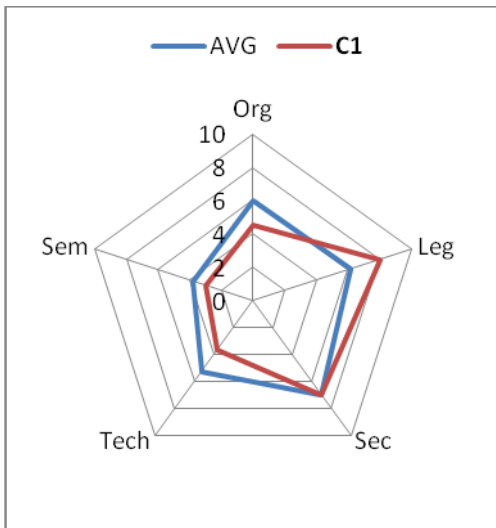
To summarise, based on the survey results, several drawbacks were identified at all four interoperability levels and within the security dimension. It can be concluded that today, cross border interoperability is not mature enough. It should be stressed that all of the obstacles to the cross border interoperability were identified solely based on the survey results within a sample of 19 base registries. This paper could be considered as a preliminary study

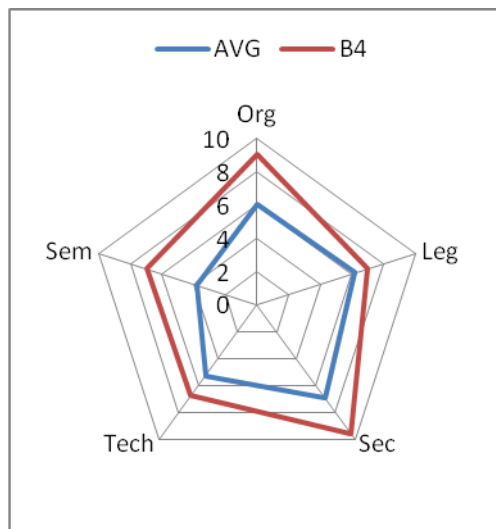
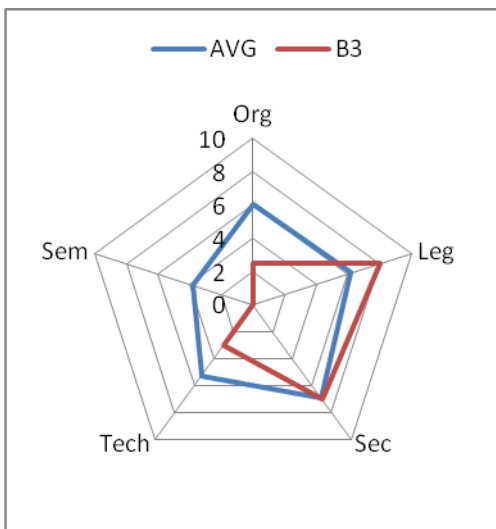
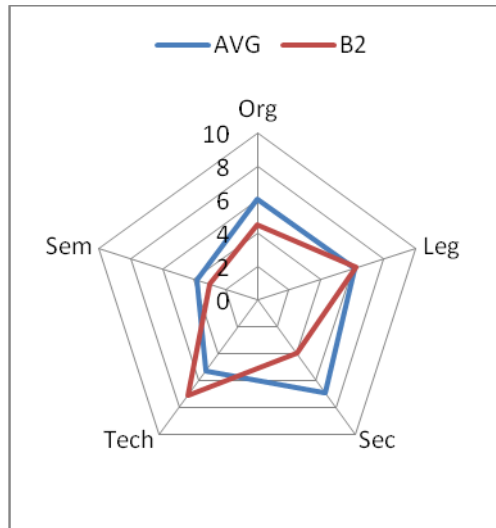
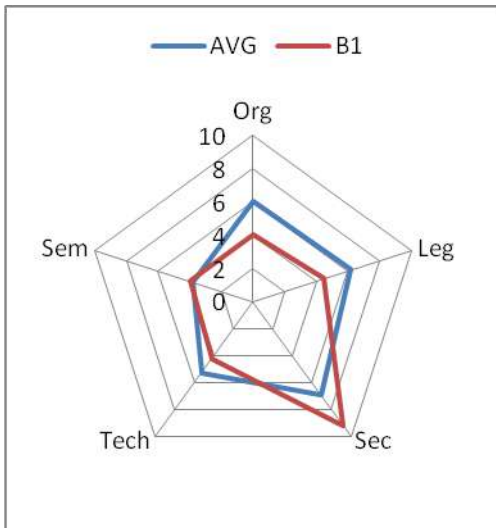
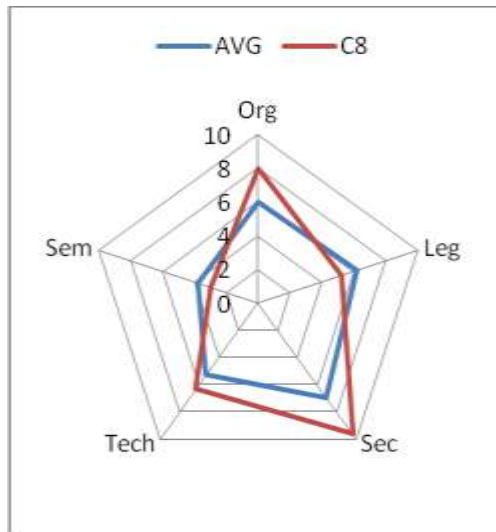
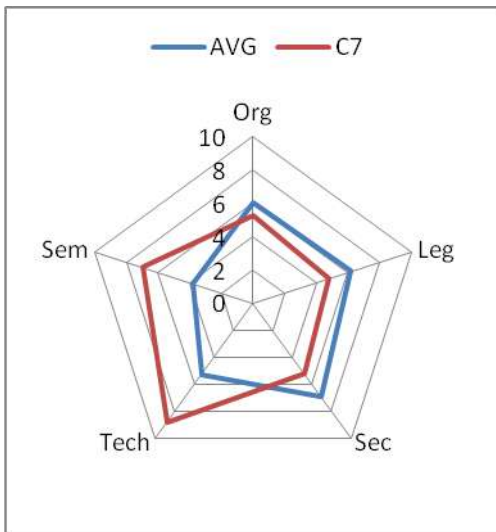
and further analysis of the phenomenon of cross border interoperability is recommended. In order to improve the credibility of the results, conclusions and recommendations, the size of the sample should be substantially increased to make sure a representative sample of base registries is chosen per each country. A representative sample does not only mean an increase in the number of base registries per country, but it also means a country-specific representative maturity. Therefore, more advanced research has to be performed in order to identify a bigger sample. In that context, desk research would be a more preferred method in order to reach a deeper understanding of the interoperability obstacles and nuances present in each country.

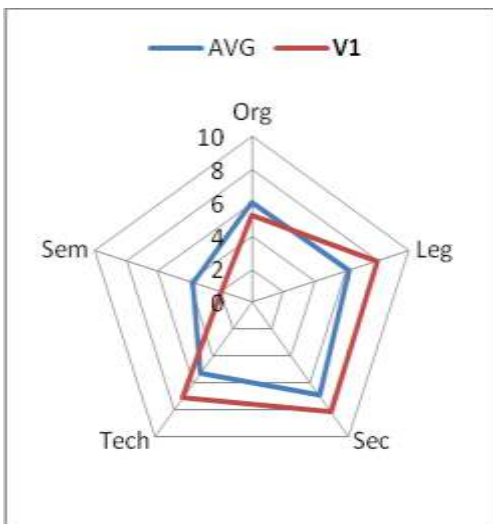
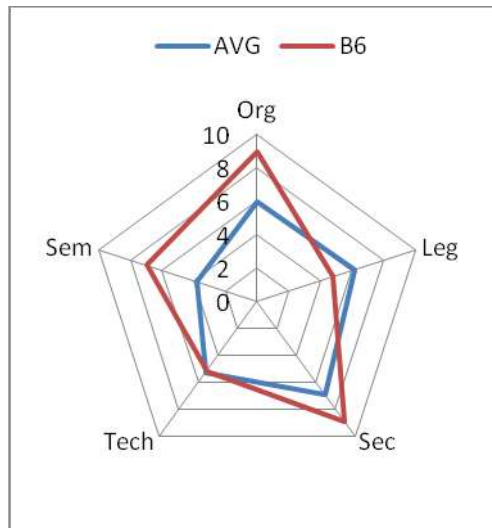
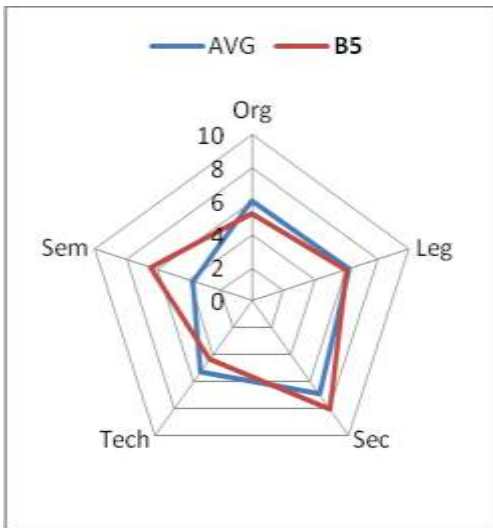
In addition, the types of base registries to be analysed have to be carefully chosen in order to focus on base registries that are related to the most common life events in a cross country context. Focusing in the first instance on “niche” base registries, such as, a list of citizens having a particular disease should be avoided. The “niche” base registries can be seen as the next step towards cross border interoperability.

ANNEX 1: SCORING PER BASE REGISTRY









ANNEX2: A DETAILED VIEW OF THE EU INITIATIVES ON INTEROPERABILITY OF BASE REGISTRIES.

This annex shows the inventory of EU initiatives that are related to the interoperability of base registries. The inventory is made based on a high-level “landscape” scan of EU initiatives. The purpose of this exercise was to produce a non exhaustive selection of relevant EU initiatives linked to the five types of base registries, as identified in the study. Out of that list, a more thorough selection was made of initiatives with an explicit and immediate impact on the interoperability of base registries. That subset has been analysed in further detail, in order to obtain recommendations and quick wins to enhance interoperability of base registries (see chapter 7).

The table below provides a short summary of each EU initiative, together with linkages to the interoperability levels.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
Proposal for a Directive as regards the interconnection of central, commercial and companies registers http://ec.europa.eu/internal_market/companies/docs/business_registers/20110224_proposal_en.pdf	On 24 February 2011 the European Commission adopted a proposal for a Directive with the aim of interconnecting Business Registers within the EU. The proposal amends a number of existing Directives (namely, Directive 89/666/EEC, Directive 2005/56/EC, and Directive 2009/101/EC).	The proposal would require all Member States to link up their business register electronically in order to facilitate cross border exchange of business information. MS should determine the legal procedure following the receipt of notifications. Each MS will determine by law the arrangements for “publicising completion of the cross-border merger in the public register in	As the proposal suggests a base registry would be accessible to multiple stakeholders. In addition, a governance model is proposed in order to provide up-to-date information on companies. Member States shall ensure that the documents and particulars “can be obtained, on application by any applicant, through a single European electronic platform	The proposal suggests that branches and all European limited-liability companies have a single European identifier allowing their clear identification and connection. The standard forms of notification of the cross-border merger to be used	Interoperability between business registries to form an electronic network, the Commission shall adopt delegated acts concerning: <ul style="list-style-type: none"> • method of transmitting information between the registers ensuring cross-border access to information in accordance with Article 3a, including the choice of the single 	The Commission shall adopt delegated acts concerning: <ul style="list-style-type: none"> • minimum security standards for the electronic network

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
		<p>which each of the companies is required to file documents”</p>	<p>accessible from every Member State”, and that “for each document and particular kept in their register ... clear information is attached explaining the provisions of national law according to which third parties can rely on those documents and particulars” (and that fees for this shall not exceed the administrative costs);</p>		<p>European electronic platform</p> <ul style="list-style-type: none"> • the interoperability of the information and communication technologies used by the members of the electronic network, including a payment interface • the definition of standards on format, substance and limits for storing and retrieving the documents and particulars • the method of and the technical standards for the transmission of information between registries. 	

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
<p>Consultation on Green Paper: THE INTERCONNECTION OF BUSINESS REGISTERS</p> <p>http://ec.europa.eu/internal_market/company/docs/business_registers/2010_consultation_final_report_en.pdf</p>	<p>Public consultation exercise launched by the European Commission in 2009 on possible ways to enhance co-operation between business registers.</p> <p>The result of the consultation showed substantial support for the improvement of interconnected business registries in the EU.</p> <p>Substantial appraisal was provided for the BRITE and the IMI initiatives, as well as for the creation of strong legal basis for cross border data exchange.</p>	<p>The consultation states that a legal requirement for the participation in interconnection of all Member States and a firm legal basis for the data exchange could be envisaged.</p>	<p>A governance agreement is confirmed in the consultation as a good solution to determine the terms and conditions of the cooperation. It is suggested that the base registries' exchanged information should be reliable and up to date across the MS.</p>	<p>It is suggested that the base registries exchanged information should be standardised and available in the relevant language across the MS.</p>	N.A.	N.A.
<p>Green Paper: THE INTERCONNECTION OF BUSINESS REGISTERS – COM (2009) 614 final</p> <p>http://ec.europa.eu/internal_market/consultations/docs/2009/interconnection_of_business_registers/green_paper_en.pdf</p>	<p>This Green Paper describes the existing cooperation framework between business registers and considers possible ways forward to improve access to information on businesses across the EU and more effective application of the company law directives.</p>	<p>The paper describes the existing cooperation framework between business registers. IT also and considers possible ways to improve access to information on businesses across the EU as well as a more effective application of the company law directives.</p>	<p>The paper provides possible ways of addressing business registers' cooperation and addressing the weakness of current policies and initiatives. In particular, it concerns access to the network of business registers (including all 27 Member States), whose characteristics need to be determined by a governance agreement.</p>	<p>The paper suggest the EBR to be a good starting point for across border access to information as it is available in several languages and could be extended to other MS.</p>	N.A.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
Business Register Interoperability Throughout Europe – BRITE http://www.ecgi.org/brite/index.php	BRITE is a research project on integrated register-to-register communications. It has thus developed several technical elements allowing business registries to communicate and exchange data.	The BRITE model and platform aims to help Business Registers to address the EU-wide Company Law. Business Registers are deeply affected by the EU Company Law.	The BRITE interoperable workflow model enables the exchange of information and data in the EU.	REID – Registered Entity Identifier enables to identify a business registry via a world unique number.	Technical objective of the project was to design and implement an interoperability model, an IT communication platform and data management instrument for business registries.	BRITE's infrastructure system complies with high reliability and privacy standards. Several services are related to long term transactions so the system prevents data loss, data corruption (e.g. by digital signature or document certification).

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
<p>Internal Market Information System – IMI</p> <p>http://ec.europa.eu/internal_market/imi-net/index_en.html</p>	<p>IMI was launched in November 2007 in support of the administrative cooperation provisions of the new Professional Qualifications Directive (2005/36/EC).</p> <p>It is a web-based application that provides competent authorities in Member States with a tool for finding relevant interlocutors in other Member States and communicating with them in an efficient and secure way, by using pre-translated sets of standard questions and answers.</p> <p>Because Member States have been closely involved in devising the system, IMI offers uniform working methods agreed by every EU country.</p>	<p>On 29 August 2011, the Commission has adopted a proposal for a Regulation on administrative cooperation through the Internal Market Information System. It is intended to set a legal framework for IMI, covering:</p> <p>a. a set of common rules defining the roles of the different actors involved in IMI, b. a framework for the processing of personal data in IMI, c. a list of legal provisions supported by IMI, d. a list of areas to which IMI could be expanded in the future.</p>	<p>There exists a defined governance model: national; regional or local authorities can find their counterparts abroad to find information. The disputes are resolved by national/regional IMI coordinator and help is provided by the EC's central helpdesk.</p>	<p>Information requests are handled within IMI, using a structured set of questions and answers. The questions have been pre-translated into all official languages by the European Commission translation services, thus providing reliable and legally certain language support.</p>	<p>A specific IMI application is developed to support the required exchange of information.</p>	<p>Data protection is assured by seven legal texts: Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995, Commission's report on the state of data protection in the Internal Market Information System (22/04/2010), European Commission's Decision of 02.10.2009 L(2009) 263, European Commission's Decision concerning the implementation of IMI (2008/49/EC), The Commission Recommendation of 26.03.2009 C(2009) 2041, The European Commission's Decision of 16.08.2009 C(2006) 3602, The Privacy Statement.</p>

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
The European Business Register – EBR http://www.ebr.org/	EBR is a network of business registers and information providers from 26 countries whose objective is to offer reliable information on companies all over Europe. It allows citizens, businesses and public authorities to search for a company name or, in certain countries, a natural person through all the member business registers by submitting a single query in their own language. As the result of the search, the requested information becomes available in the language of the query.	The legal aspects of the data transmission within the network and in particular the protection of personal data are governed by national law, including the provisions implementing the Community data protection rules.	Participation in the EBR network is voluntary for the registers and is realised on a contractual basis (Information Sharing Agreement). The European Business Register has also adopted the form of a European Economic Interest Grouping (EEIG), however, due to specificities of certain national laws, not all registers are authorised to participate.	The EBR It allows citizens, businesses and public authorities to search for a company name or a natural person through all the business registers which are members of EBR. This can be done by submitting a single query in one's own language. The requested information is available in the language of the query.	Registries in the member countries provide data which is accessible through the EBR in standardised reports. The distributors of information use the EBR software under specific technical conditions.	Information is retrieved from a country's official business registry and provided by a country relevant EBR Information Distributor. This model helps to early detect doubtful activity or information.
e-Justice initiative https://e-justice.europa.eu/home.do?action	The e-Justice project aims at assisting the work of businesses, legal practitioners and judicial authorities and facilitating the access of citizens to judicial and legal information. It is an electronic one-stop-shop for access to justice throughout the EU. The web site benefits citizens, businesses, lawyers and judges with cross-border legal questions and boosts mutual understanding of different legal systems by contributing to the creation of a single area of justice. The web portal provides information and links on laws and practices in all Member States.	N.A.	The European e-Justice action plan for 2009-2013 sets out how the e-Justice portal would deal with the integration of EBR. The project states that access to business registries takes place once (European) Authentication of: - Identity - Functions - Rights	N.A.	N.A.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
			are in place and mutually trusted by relevant stakeholders.			
European Land Information Service – EULIS http://eulis.eu/	<p>EULIS is an online portal enabling access to land registries across European borders. It provides easy access to land and property information for professional customers in Europe. It is also a hub of information about different land registration conditions in each country. Its long-term mission is to underpin a single European property market through cross border lending.</p> <p>The service is aimed at professional customers who use land registry information to assist them in their day-to-day work life. It helps with access to land and property information, via computer applications. It is not meant to be a database itself, but simply to facilitate excess and retrieval of information.</p>	N.A..	<p>Within the EULIS the information is retrieved online, directly from official land registers. Organisation visible in EULIS is not always the organisation responsible for deed or title registration.</p> <p>Three criteria need to be fulfilled before being able to connect as a land registry: 1) having an online service, 2) provide information to professional users and administer these users, 3) provide 'reference information' about the local land registration environment</p>	<p>EULIS provides a glossary and reference information to understand terminology used in local environments.</p> <p>Access to land registry information may vary as in some countries one can search the land registry by the name of a person, in other countries by object information (e.g. address). This results in difference of extent of information provided across countries.</p>	<p>EULIS helps with access to land and property information, via computer applications. It is not a database itself, but simply to facilitate excess and retrieval of information through direct access to official land registers in Europe.</p>	<p>The EULIS addresses the demand for reliable information on real property rights and requirement of restrictions to it. This is crucial for banks, notaries, tax administrators, financial institutions, surveyors as well as public bodies.</p>

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
Project LINE http://eulis.eu/project-line/	<p>Supported by the Official Justice Programme 2007-2013, and lead by the EULIS initiative, the project wants to develop a sustainable and financially viable solution, to enable new land registry organisations to cost-effectively connect to the EULIS 2.0 platform.</p> <p>Facilitating cross border access and use of legal property, improving the technical results of the EULIS platform is only a part of the project objectives. They also include compliance and alignment with the e-Justice programme, by gathering together officials and land registry organisations across Europe. Further developments will increase data exchange functionalities, by integration features such as e-Signatures and e-Registration.</p>	N.A..	<p>Governance of access to land registries will be done through a community of land registries organisations of EU MS.</p> <p>It also includes compliance and alignment with the European e-Justice portal.</p>	<p>EULIS provides glossary and reference information to understand terminology used in local environments.</p>	<p>The project aims to deliver the EULIS platform enabling access to land registries.</p> <p>EULIS 2.0 is intended to be flexible and future proof in order to cope with the evolving national technical land register systems.</p> <p>Further developments will increase data exchange functionalities, by integration features such as e-Signatures and e-Registration</p>	<p>Data protection is covered by:</p> <ul style="list-style-type: none"> EU Directive 96/9/EC (data right and copyright) · PSI Directive (2003/4/EY) · PSI Directive 2003/98/EC article 8.2 · EU Directive 95/46/EC (data protection: privacy) articles 7, 11, 25, 26 <p>On national level EULIS fits within the laws and regulations related to Land Registry, Cadastre, Privacy.</p>
Regulations 2157/2001 (on the Statute for a European Company (SE)) and 1435/2003 (on the Statute for a European Cooperative Society (SCE)) http://europa.eu/legislation_summaries/employment_and_social_policy/social_dialogue/126018_en.htm	<p>The <i>Regulation 2157/2001</i> enables a company present in different MS to be established as one entity under Community law instead of a number on national laws. This results in a central management and reporting system under Community law and as a consequence in reduction of administrative costs. The <i>Regulation 1435/2003</i> sets up a legal statute for a European Cooperative Society creating a level playing field for competition between cooperative societies and capital companies. This fosters cross border activities of cooperative societies at the EU level.</p>	<p>Cross-border cooperation of business registers is required explicitly by the Directive on cross-border mergers and by the Statutes for a European Company (SE) and a European Cooperative</p>	N.A.	N.A.	N.A.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
		Society (SCE).				
<p>European Parliament legislative resolution of 10 March 2009 on the proposal for a Council regulation on the Statute for a European private company (SPE)</p> <p>http://www.europarl.europa.eu/sides/getDoc.do?sessionId=C116582BFBBCF07E226B39F52E5DC2F2F.node1?pubRef=-//EP//TEXT+TA+P6-TA-2009-0094+0+DOC+XML+V0//EN</p>	<p>Article 46(2) of the proposal lays down obligations of authorities responsible for registers. According to the obligations, those authorities shall cooperate with each other to ensure that the documents and particulars of the SPEs listed in the draft Regulation are also accessible through the registers of all other Member States</p>	<p>Once the Statute for a European Private Company (SPE) is adopted, the number of cases that require cross-border cooperation may increase. The SPE could provide small and medium-sized enterprises (SMEs) with a simple and flexible way to expand their business in the Single Market. It is though necessary to ensure easy access to official information on these companies active in several Member States.</p>	N.A.	N.A.	N.A.	N.A.
<p>MUlti-Industry, Semantic-based Next Generation Business IntelliGence – MUSING</p> <p>http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=8506237</p>	<p>MUSING is a research project (co-funded by the EU under the FP6) which goal os to develop Business Intelligence (BI) tools and modules based on semantic knowledge and content systems. The project objective is to collect international company intelligence and country/region information</p>	N.A.	<p>The focus of the project was internationalisation by making evolve the local enterprises to international dimension , hereby expressly concentrating on the information acquisition about international</p>	<p>The technology designed within the project aims to help in searching for relevant semantic information (expressed in the ontology) within internationalisati on, among</p>	<p>MUSING services consultation platform can connect to business registries to enrich the data it provides.</p>	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
			partnerships, contracts and investments.	others.		
Professional Qualifications Directive (Directive 2005/36/EC) http://ec.europa.eu/internal_market/qualifications/policy_developments/legislation_en.htm	<p>The Directive came into force on 20 October 2007 and replaced fifteen existing Directives in the field of the recognition of professional qualifications.</p> <p>A number of changes have been introduced, including greater liberalisation of the provision of services, more automatic recognition of qualifications and increased flexibility in the procedures for updating the Directive.</p>	<p>The provisions of the Directive enhance the automatic recognition of Professional Qualifications across MS, in order to achieve the full potential of the Internal Market and of the citizens' freedom of movement. Cross-borders cooperation of competent authorities will have to be as fast and efficient as possible. Its application relies on the IMI for technical functioning.</p>	N.A.	N.A.	N.A.	N.A.
Services Directive (2006/123/EC) http://europa.eu/legislation_summaries/employment_and_social_policy/job_creation_measures/l33237_en.htm	<p>The Directive introduces provisions aiming explicitly at simplifying life and increasing transparency for businesses (including SMEs) and citizens. In particular, it requires Member States to remove burdens and facilitate cross-borders provision of services. It also sets the obligation to designate "points of single contacts" through which service providers can obtain all relevant information and deal with all administrative procedures. It also sets the obligation for the points of single contact to be accessible at a</p>	<p>Chapter VI of the Directive contains detailed provisions relating to the electronic exchange of information between MS administrations.</p>	<p>The most recent act: Commission proposal to interconnect business registers within the EU.</p>	N.A.	<p>A specific IMI application is developed by the Commission, in close cooperation with the MS, to support the required exchange of information.</p>	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
	distance and by electronic means.					
First Company law Directive (68/151/EEC), and 2003 amendment http://ec.europa.eu/internal_market/company/official/index_en.htm	The First Company law Directive (68/151/EEC) prescribes compulsory disclosure of a series of documents and particulars of limited-liability companies.	The 2003 amendment required the MS to put in place a system of electronic registers by 1 January 2007. This modernisation of the Directive was aimed at making company information more easily and rapidly accessible by interested parties and at simplifying significantly the disclosure formalities imposed upon companies.	N.A.	N.A.	N.A.	N.A.
11th Council Directive 89/666/EEC on disclosure requirements with respect of branches http://europa.eu/legislation_summaries/internal_market/businesses/company_law/26012_en.htm	It integrates the Company Law Directives by providing specific provisions for company branches.	This Directive concerns companies' branches that are located in a different MS than where it was originally established. Branches of companies are obliged to publish the following data: the address of the branch, the activities of the branch, the	N.A.	N.A.	N.A.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
		company's place of registration, registration number, particulars of the company directors.				
Council Regulation (EEC) No 2137/85 of 25 July 1985 on the European Economic Interest Grouping (EEIG) http://europa.eu/legislation_summaries/internal_market/businesses/company_law/26015_en.htm	It integrates the provisions of the Company Law Directives, with respect to EEIG.	The Regulation establishes that "any grouping establishment situated in a Member State other than that in which the official address is situated shall be registered in that State". This means that "a grouping shall file, at the appropriate registry in that Member State, copies of the documents which must be filed at the registry of the Member State in which the official address is situated, together, if necessary, with a translation which is in line with the practice of the registry where the establishment is registered".	N.A.	N.A.	N.A.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
Transparency Directive 2004/109/EC http://ec.europa.eu/internal_market/securities/transparency/index_en.htm	<p>The Directive requires that regulated financial information remains available to market participants at central depositories appointed nationally by Member States. Member States are encouraged to support the interconnection of these depositories.</p> <p>This network should be electronic and its members should respect some minimum standards of security, certainty as to the information source, time recording and easy access by end users. The recommendation foresees an important role for the Committee of European Securities Regulators (CESR) in launching the electronic network.</p>	The Directive on transparency obligations of listed companies (2004/109/EC) requires that regulated financial information to be available to market participants at central depositories appointed nationally by the MS.	Within the Transparency Directive a single electronic network/platform of electronic networks across the MS should be established for the "appointed storage mechanisms".	During the consultation process some participants were in favour of the use of XBRL (company that developed the taxonomy) for disclosures, in order to increase visibility and comparability to encourage cross-border investment but also to deal with the language problem.	N.A.	The Commission requires the electronic network (to exchange the regulated financial information) and its members to respect standards of security especially the information source, time recording and easy access by end users.
Cross-border mergers Directive 2005/56/EC http://ec.europa.eu/internal_market/company/mergers/index_en.htm	<p>The Directive will facilitate mergers of limited-liability companies on a cross-border basis, which at present are impossible or entail prohibitive costs. It sets up a simple framework drawing largely on national rules applicable to domestic mergers and avoids the winding up of the acquired company.</p> <p>Under the Directive on disclosure requirements in respect of branches opened in a Member State by companies governed by the law of another State, certain documents and particulars concerning the company have to be disclosed in the register of the branch. A direct exchange of information between the concerned registers could facilitate the task of keeping the relevant information always up-to-date.</p>	N.A.	The Directive envisages close cooperation of registries. The registration of the company that results from the cross border merger should inform the registry in which each of the companies was required to file documents about the cross border merger. In addition, the old registration should be deleted.	N.A.	N.A.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
<p>Council Decision 2008/615/JHA of 23 June 2008</p> <p>Council Decision 2008/616/JHA of 23 June 2008</p> <p>Council Decision 2008/617/JHA of 23 June 2008</p> <p>http://ec.europa.eu/transport/infringements/directives/road_en.htm</p>	<p>There are EU legislative provisions on several aspects of vehicles and driving licences use and circulation, whose implementation concerns each Member State.</p> <p>The creation of a European database is inserted into a broader counter-terrorism framework, approved by the Council and inserted into the Title VI of the EU Treaty.</p>	<p>These legislative provisions lead to wider range of application of the EUCARIS system. The system has thus become a part of the EU legislative framework</p>	<p>National points of contact are established and an obligatory process used for the search mechanism is defined.</p>	<p>Complete data set: mandatory and optional definitions are used to streamline the communication.</p>	<p>TESTAIL is used as a communication network and data is handled through EUCARIS using encrypted XML-messages. The Decision further specifies authentication of users, user roles, logging and tracing of message exchange and further technical conditions as well as functional and non-functional requirements including security, standards, support and maintenance</p>	<p>The security design is based on a combination of HTTPS and XML signature through an SSL connection</p>
<p>EUropean CAR and driving licence Information System – EUCARIS</p> <p>https://www.eucaris.net</p>	<p>EUCARIS is a communications network (developed within the i2020 Agenda) which allows participating countries to consult and exchange data relating to motor vehicles and driving licences kept in the national registers of affiliated countries.</p>	<p>EUCARIS contributes to prevention of violations of the law. Legal basis is the following:</p> <p>EU Council Decisions: 2008/615/JHA and 2008/616/JHA, bilateral/multilateral agreements for</p>	<p>EUCARIS uses a country's own registry of vehicle and driving licence information and its own registration procedures.</p>	<p>EUCARIS web client application is multilingual and enables administrative personnel, police-officers etc. to do inquiries in other countries via their browser.</p>	<p>EUCARIS's 'Core' application enables secure treating and communication of messages. Security is ensured by the use of: closed network, SSL, XML signing, logging, MS authorisation, authorisation of EUCARIS users.</p>	

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
		the information exchange via File Transfer or Owner/Holder application, EUCARIS Treaty.				
Cross-Borders eConveyancing – CROBECO http://www.elra.eu/?page_id=636	<p>Carried out by the European Land Registry Association, the project aims at setting up a European framework for obtaining foreign immovable property.. In the deed, the law of the country where the plot is located is made applicable to the contract. This helps to protect the buyer against unknown consequences of a foreign legal system.</p> <p>The aim of the project is to develop a Draft of a Cross border Conveyancing Reference Framework (CCRF). Because timely receipt of information from the land registry by conveyancers and of conveyance documents by registrars is essential for cross-border conveyance, the framework is based on electronic communication. It is also expected that this new procedure will boost confidence in a protected legal position and encourage purchases of foreign immovable property.</p>	<p>The leading principle of the project is to take existing circumstances as given and respect these (including legislation, responsibilities or registrars and conveyancers, and existing conveyance systems)</p>	<p>The project has developed a draft of a Cross border Conveyancing Reference Framework (CCRF): CCRF provides and explains generic rules for governance and a uniform process.</p>	<p>The process is based on a bilingual (mother tongue of the buyer and the official language of the foreign country) approach.</p>	<p>Authorisation of a user is done via a digital signature to confirm that the conveyance is a real public notary, authentication is done via qualified digital certificates belonging to digital signatures.</p>	<p>Security aspects are based on ELRA best practices and projects on the European projects and legislation.</p>
Commission Internationale de l'Etat Civil (CIEC) - International Commission on Civil Status (ICCS) http://www.ciec1.org/SommaireAnglais.htm	<p>The Commission Internationale de l'Etat Civil (CIEC) / International Commission on Civil Status (ICCS) has developed a prototype platform for the exchange of some civil status forms among registries in Member States.</p> <p>Please note: this is an initiative applied at the MS level.</p>	<p>The legal basis of the ICCS are 32 Conventions, of which 28 are in force and 9 Recommendations . They can be signed by an ICCS MS and by any MS of the Council of Europe and the EU.</p>	<p>An automated electronic platform exists for exchange of civil-status data between authorities of within the same MS and between MS (e.g. on the basis of a bilateral agreement).</p>	<p>“Guide pratique international de l'état civil” is a comparative law study in the field of personal status written for civil registrars in different ICCS MS and serves as guide.</p>	<p>The platform allows the form to be sent by a civil status officer of one MS, and the form to be safely received by the civil status officer of another MS.</p>	<p>The exchange platform adopts encryption for the communication protocols. Furthermore, access is guaranteed by a hardware token.</p>

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
RISER ID Services GmbH - Electronic Address Verification Services http://www.riserid.eu/home/	<p>RISER started in 2004 as an innovation project within the European Commission eTEN Programme. The project ended 2010. Since then a company has developed the service, and is now firmly positioned in the market.</p> <p>The RISER ID Services GmbH acts as a data processor on behalf of its customers es. Customers (e.g. businesses and administrations) submit inquiries about official address information from several member states of the European Union. RISER provides verification addresses and age to its customers, after verifying that they have proof of their legal interest for that information. The result of inquiry consists of full names and full addresses (and age in some cases) as listed in the respective official register or electoral roll register.</p>	<p>Customers of RISER are obliged to ensure that processing of query has a legal basis and a privacy compliant process.</p>	<p>RISER does not store data and inquiries are passed to official registries in the EU MS.</p>	<p>RISER, at present, is available in German, English, Estonian and Hungarian.</p>	<p>Data flows only between a customer and the relevant registry and is not made available to third parties.</p>	<p>A transparent data processing procedures exist and personal data is not kept in the database. RISER was awarded the European Privacy Seal (EuroPriSe) for its data protection and data security measures.</p>
Commission's 2004 "Action Plan for the implementation of the legal framework for electronic public procurement" http://ec.europa.eu/internal_market/public_procurement/e-procurement/index_en.htm	<p>The Commission's 2004 Action Plan provided a roadmap, establishing a strategy designed to accelerate the adoption of e-Procurement whilst safe-guarding the core principles and provisions of existing EU procurement legislation and Treaty. It was intended to encourage the development and use of convergent, accessible, secure but commercially viable solutions and disseminate examples of best-practice. Action was also required to stimulate and orientate the work of the first movers in the field, who had already introduced e-Procurement elements in their legislation or practices, or set up e-Procurement systems.</p>	<p>EU policy was designed to play a complementary role in support of national or regional efforts to put procurement on an electronic footing. Tenders submitted online are published on the EU TED (Tenders Electronic Daily) within five days of being sent.</p>	N.A	N.A	N.A	N.A
Green Paper on expanding the use of eProcurement in the EU [COM(2010) 571	<p>After the evaluation of the 2004 Action Plan for eGovernment, a consultation process was</p>	<p>Responses to the consultation called</p>	<p>It suggests coordination</p>	<p>Administrative barriers to cross-</p>	<p>Some respondents feel</p>	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
<p>final] and Consultation</p> <p>http://ec.europa.eu/internal_market/public_procurement/e-procurement/consultations/index_en.htm</p>	<p>launched in the form of a Green Paper addressed to all relevant stakeholders. The objective of the consultation was to gather input and ideas on ways to:</p> <ul style="list-style-type: none"> • Simplify and improve public procurement administration through ICT. • Accelerate the transition to e-Procurement: • Avoid a new generation of barriers to cross-border procurement, having their origins in different ICT solutions or e-Procurement processes. 	<p>for an EU law concerning the Virtual Company Dossier (VCD) making it legally binding to encourage cross-border recognition) and to eliminate requirements from Member States for suppliers to be established within the respective Member State.</p>	<p>between different existing interoperability initiatives (e.g. the German 'XVergabe' cross sector project that enables interoperability between German e-Procurement platforms). Providing general requirements and basic principles concerning the operation and interaction between e-Procurement systems</p>	<p>border e-Procurement relating to the submission of documents and certificates could be tackled by "standardising forms and certificates, simplifying rules for certificate requests and facilitating access to existing certificates.</p>	<p>that e-Certis should be established as the central location for pre-qualification documents. Cooperation between VCD and e-Certis is also encouraged</p>	
<p>eCertis</p> <p>http://ec.europa.eu/internal_market/public_procurement/e-procurement/e-certis/index_en.htm</p>	<p>e-CERTIS is a free, on-line source of information to help companies and contracting authorities to cope with the different forms of documentary evidence required for cross-border tenders for public contracts. It presents the different certificates frequently requested in procurement procedures across the EU.</p> <p>For each country, information on the most common certificates is organised under common headings, corresponding to the types of documentary evidence mentioned in the EU Procurement Directives. For each heading, each national dataset contains a record broken down into a number of standard fields. This record describes in detail, consistently across the national datasets, the certificates issued in a given country for a specific type of evidence. The system matches equivalent documents across the different national datasets.</p>	<p>The information coming from different countries (tender documents) provided by the system is based on the knowledge of local legal procedures. The authenticity of documents is proved by official certificates by national authorities or statements by tender's representative certified in various</p>	<p>N.A.</p>	<p>A standard list of tender specific documents is provided in the eCertis system.</p>	<p>N.A.</p>	<p>N.A.</p>

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
		ways.				
Pan-European Public Procurement OnLine project – PEPPOL http://www.peppol.eu/	<p>Started in 2008, the project aims at expanding market connectivity and interoperability between eProcurement communities. PEPPOL enables access to its standards-based IT transport infrastructure through access points, and provides services for eProcurement with standardised electronic document format.</p> <p>As an open standardised platform, PEPPOL's infrastructure has been designed to interconnect existing networks and bridge individual eBusiness islands in Europe. PEPPOL increases business opportunities for participants and supports interoperability across borders. It facilitates electronic communication among European companies and government institutions in the pre-award and post-award procurement process.</p>	N.A.	N.A.	To ensure an efficient communication between MS, the Common Procurement vocabulary is used as well as CPV codes.	The platform consists of a number of access points to access a standard-based IT transport infrastructure. National technology solutions are not changed, but aligned with the European standards.	From the security point of view eSignatures based on electronic certificates are issued by relevant authorities.
Electronic Procurement, Invoicing and Ordering – Open e-Prior http://www.peppol.eu	<p>Open e-PRIOR is an Open Source e-Procurement platform for all Public Authorities wishing to pilot e-Procurement, including its cross-border aspects. It has been developed by the Directorate General for Informatics (DIGIT) in the context of the IDABC e-Invoicing and e-Ordering project.</p> <p>The project aims at a practical implementation of interoperable electronic services at a pan-European level, predominantly within the post-awarding phase of Public Procurement.</p>	N.A.	N.A.	N.A.	Technological solutions can be reused from business to administration processes and used for the administration to administration process.	N.A.
Information System for European Public Procurement – SIMAP http://simap.europa.eu/index_en.htm	A web portal providing access to most important information about public procurement in Europe.	N.A.	N.A.	Information is available in all EU languages. In addition, standard forms for public procurement and CPV codes are used.	SIMAP is a system that supports the EU TED platform.	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
European Civil Registry Network – ECRN http://www.ecrn.eu/BBB/	ECRN is a project co-funded by the European Union under the ICT Policy Support Programme (PSP). It deals with the establishment of a pilot among the Civil Acts Registry of National Administrations to allow safe transmission and certain identification of the Civil Acts exchanged among Local Governments of European administrations. Additional services include information and guidance services for actors of the Civil Registry sector.	The exchange of civil registry data is compliant with the Wien Convention 1976 on Multilingual Documents.	Governance model describes connection to base registries and a process to update them.	Exchange of civil registry certificates is done with a use of multilingual documents.	The system is composed of a software framework that provides the basic functionalities of ECRN and a Web Application that is the only access point to all these functionalities.	A certified and secure platform guarantees exchange of an authentic civil registry certificate between the MS.
STORK - Secure Identity Across Borders Linked https://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1	<p>The STORK project is co-funded by the European Union under the Competitiveness and Innovation Programme (CIP). The STORK project seeks to make it easier for citizens and businesses to access online public services across borders by developing and testing common specifications for mutual recognition of national electronic identity (eID) between participating countries.</p> <p>After developing and testing rules and specifications to support mutual recognition of eIDs across Europe, it would be possible to use cross-border services over the Internet exploiting secure eID authentication. It would then be easier, quicker and cheaper for citizens to live and work in different EU countries, and for business to operate across Europe.</p> <p>The cooperation of the project with other EU initiatives on interoperability is also foreseen, as well as a possible future integration.</p> <p>Remark:</p> <p>STORK affects the interoperability of business registries indirectly, as it aims at developing mutual recognition of national eIDs, which are a prerequisite for more secure electronic</p>	N.A.	N.A.	N.A.	The STORK project enables communication between citizen or business registries between the MS through a platform. The Quality Assurance Authentication Framework “describes how national authentication levels would be mapped with STORK QAA levels to ensure eID interoperability” (see: www.eid-stork.eu)	N.A.

EU Initiative	Short Description	Impact on Interoperability Criteria				
		Legal	Organisational	Semantic	Technical	Security
	transactions among registries.					
<p>Effective problem solving across Europe – SOLVIT</p> <p>http://ec.europa.eu/solvit/site/index_en.htm</p>	<p>Active since 2002, SOLVIT is an on-line problem solving network in which EU Member States work together to solve without legal proceedings problems caused by the misapplication of Internal Market law by public authorities. It deals with cross-border problems between a business or a citizen on the one hand and a national public authority on the other, where there is possible misapplication of EU law in several policy areas. It is coordinated by the European Commission which provides the database facilities, and by the Member States, which set up SOLVIT centres in their territory. It processes requests from citizens and businesses.</p> <p>A case is submitted to the local SOLVIT centre and is then entered into an on-line database. It will be forwarded automatically to the SOLVIT Centre in the other Member State where the problem has occurred (known as the "Lead" SOLVIT Centre). The Lead SOLVIT Centre should confirm within a week whether or not it will take on the case. If a solution is found, the citizen/business will be advised on what they need to do to benefit from the proposed solution.</p> <p>This initiative aims at improving the application of the Internal Market, and at speeding up the process when a dispute arises from a simple misapplication of EU Law, without costs for citizens and businesses.</p>	<p>According to the EU Data Protection legislation only data related to a concrete case is entered in the SOLVIT database. The data base is managed by the DG Internal Market with conformity to the IDA security policy.</p>	<p>Home and Lead Coordination Centres choose a language to communicate with each other (Commission Recommendation of 7.12.2001 on principles for using "SOLVIT").</p>	<p>Access to relevant registries is done via a dedicated web-interface.</p>	<p>N.A.</p>	

