REPUBLIC OF ESTONIA
MINISTRY OF JUSTICE

eRIK
Centre of Registers and Information Systems

Co-funded by the Justice
Programme of the European Union

IC RW Project

Feasibility Study

For a Secure Electronic Tool on Cross-Border Electronic Transmission of Certified Copies of Wills

Final Version

September 2016

The Foreword

The current feasibility study (hereinafter called the study) has been conducted within the project "*Further developments in the area of interconnection of registers of wills*" (hereinafter called IC RW), by Estonian Centre of Registers and Information Systems. Substantial input was provided by the Estonian Ministry of Justice and by the IC RW project partners and expert group members.

The major goal of the current study has been to explore the electronic possibilities for advancing the information exchange on the existence and content of wills between EU Member States, and to analyse the information security aspects related to the electronic cross-border exchange of digitized copies and certified digitized copies of wills in order to improve and fasten the cross-border communication in succession matters.

This study reflects only the authors' views and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

1 The Scope and Structure of the Study

One of the ground reasons for initiating the IC RW project and the current study is an understanding that it is extremely important that last wills and necessary information related to succession proceedings could be found in cross-border situations for ensuring that the last wishes of the testators are respected. Moreover, a contribution to the effective implementation of the Regulation (EU) No 650/2012 of the European Parliament and of the Council on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession (hereinafter referred to as the "Succession Regulation") was also a goal of the IC RW project.

Expectations for greater efficiency in the area of justice, particularly in cross-border situations, lead us towards the need to increase the use of electronic solutions. The development of well-functioning and interoperable electronic systems has already become one of the key issues both for the Member States as well as for the European Union.

The goal of this feasibility study is to explore and enhance the possibilities for exchanging succession related information and documents electronically between the Member States in order to improve and fasten the cross-border communication in succession matters. More precisely, the current study will focus on the possibilities of establishing wider networks of secure electronic cross-border data exchange channels for the delivery of data on the existence and content of wills and digitized copies of wills.

In order to improve and fasten the cross-border communication in succession matters, and to discover suitable tools with desired functionality and security levels, a study was conducted to provide the following:

1. An analysis of the needs for data protection, privacy, security, confidentiality and integrity in cooperation with stakeholders, and of recommendations from an information security perspective.
2. An overview of the available electronic cross-border data exchange solutions suitable for exchanging of copies (or certified copies) of wills and the possibilities of reusing already existing technical platforms and solutions (e-CODEX, STORK, e-SENS, EUFides, ENRW, etc.).
3. Recommendations for possible options of expanding the electronic exchange of succession related information between the EU Member States.

The current study could also be considered as a preparatory step for applying additional possibilities of implementing ICT tools for exchanging information on the existence and content of wills between persons and authorities involved in succession proceedings in Europe.

This study does not include recommendations regarding technical specifications on the preferable solutions, which is out of the scope of the IC RW project.

2 Earlier Related Studies

In order to avoid duplication of the work, the reports compiled and information collected during the previously conducted studies on the issues of cross-border succession have been reviewed. These documents have been a valuable source of information, and the results of this exercise have been reflected under the current chapter of this study. Also, the information on the succession factsheets of the European e-Justice Portal and at the homepage of the European Network of Registers of Wills Association (hereinafter referred to as "the ENRWA") has been considered.

2.1 European Commission's Survey 2016

In spring 2016, the European Commission conducted a *study on the electronic European Certificate of Succession, national registers of the European Certificate of Succession and wills, and their interconnection*, which involved a survey among the ministries of judicial affairs and the representatives of notaries in the EU Member States. The survey questionnaire also included questions regarding the national registers of dispositions of property upon death (including wills). The results of this study have not become public by the time of compiling the current IC RW feasibility study.

2.2 IC RW Project's Survey in 2016

The purpose of the IC RW project's survey[1] was to analyse the possibilities of advancing the cross-border exchange of data and files regarding wills in order to gain deeper understanding of the matters related to cross-border cases, and to discover current obstacles as well as development opportunities.

20 responses were received (19 Member States and CNUE). The respondents represented the ministries dealing with the matters of justice, the representative organisations of notaries, and other types of organisations, like registration offices, almost in equal numbers.

The survey revealed differences between the EU Member States in terms of exposure of data related to wills, after the death of a testator. While in some Member States the information about the existence of a will becomes public, then on the other hand some Member States reveal such information only to heirs or to authorities handing respective succession matters. In general, the Member States are able to provide information across borders, but different rules apply regarding persons who are entitled to receive the information about the existence or content of wills.

This survey indicated, that the most common way to exchange information about the existence of a will, besides the ENWR platform, is by e-mail or encrypted e-mail. Five of the responding Member States provide the information about the existence of a will via an Internet portal or a web-site. At the same time, there are some Member States that currently would not be able to provide such information electronically, mainly because of their national legislation, as well as because of the absence of widely used secure information networks in succession matters.

Regarding information exchange on the content of wills, it may be concluded, that the right to receive information is linked to the role of the enquirer. 14 Member States out of 19 respondents would reveal this information to another Member State's authority, while 13 Member States would reveal this information to an heir or a representative of an heir. Three Member States allow the widest circle of persons[2] to receive information about the content of a will after the death of a testator.

[1] 9660/2/16 REV2 EJUSTICE 112 JUSTCIV 205
[2] Heir or his representative, authority, persons with legitimate interest, anyone

11 Member States out of 18 that responded to the question about suitable digital file formats, indicated the ability to receive copies of wills in one or more digitized formats. Most commonly mentioned formats were documents with a digital signature (bdoc, edoc, ddoc, XAdES, CAdES) and files in the pdf or pdf/a formats.

Regarding the use of Internet-based communication channels, 11 Member States and CNUE responded that digitized copies of wills could be delivered to an enquirer abroad. The most preferable channels of communication would be interconnected secure networks or e-mail. Three Member States also indicated the option of giving access to a file through a web portal. On the other hand, four respondents indicated that no Internet means could be used for delivering copies of wills.

Regarding the authentication of an enquirer in the exchange of digital copies of wills, four Member States out of ten mentioned that authentication is conducted according to access rights based on profession, in three cases a digital signature or an electronic identification was mentioned, and in two cases receiving an e-mail was considered sufficient without the need for further identification.

Because of these differences discovered during the survey, it could be stated that more detailed information in a uniform and simple manner regarding succession matters should be presented via Internet to the parties involved, taking into account the possibilities offered by the available ICT tools.

2.3 IC RW Project's Survey in 2015

An initial IC RW project survey[3] was carried out among the EU Member States in 2015, in order to understand the overall position of the Member States and their current legal and technical situation on the topics discussed in the expert group on interconnection of registers of wills. Responses were collected from 24 Member States[4].

One of the topics reviewed was related to the Basel Convention on the Establishment of a Scheme of Registration of Wills. At the time of the survey there were 15 Member States who had not joined or not ratified the Convention[5], and the main reasons were related to the nature of registers for wills or a lack of those; the limitations on access to the data in registers; the nature of national legislation and the different ways of handling succession. An additional reason was stated as an understanding that joining the Convention would not fully solve the problem of exchanging data on wills, for various reasons, amongst them the fact that not all wills are registered.

One of the main concerns emerging from this survey was the realisation that many of the responding countries experience difficulties in locating the proper contact person or information source in the other Member State for receiving a timely response about the existence or content of a will.

It was also surveyed, who and under which terms could access the information held in the register of wills. According to the survey, before the death of the testator only the testator himself can see the data in the register or access the will. After the death of the testator there are great differences in legislation and culture in handling the information regarding wills. The rights to receive information about the existence of wills or their content vary from an appointed authority official only, to the public and anyone interested. Most commonly the persons demonstrating a legitimate interest would be considered eligible to receive information about the existence of a will.

The survey also studied the issues related to electronic access to the registers of wills. The results indicated that most commonly the registers are accessed based on the username and password given to a legal professional or notary in connection with their membership in a professional organisation or state institution,

[3] 11169/1/15 REV1 EJUSTICE 95 JUSTCIV 194; 13215/15 EJUSTICE 129 JUSTCIV 242
[4] AT, BE, CY, DE, DK, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, SI, SK, UK.
[5] BG, CZ, IE, EL, HR, LV, HU, MT, AT, PL, RO, SI, SK, FI, SE

or based on digital e-IDs. Also, country-specific digital access devises (employee cards, USB keys, etc.) are applied in several countries.

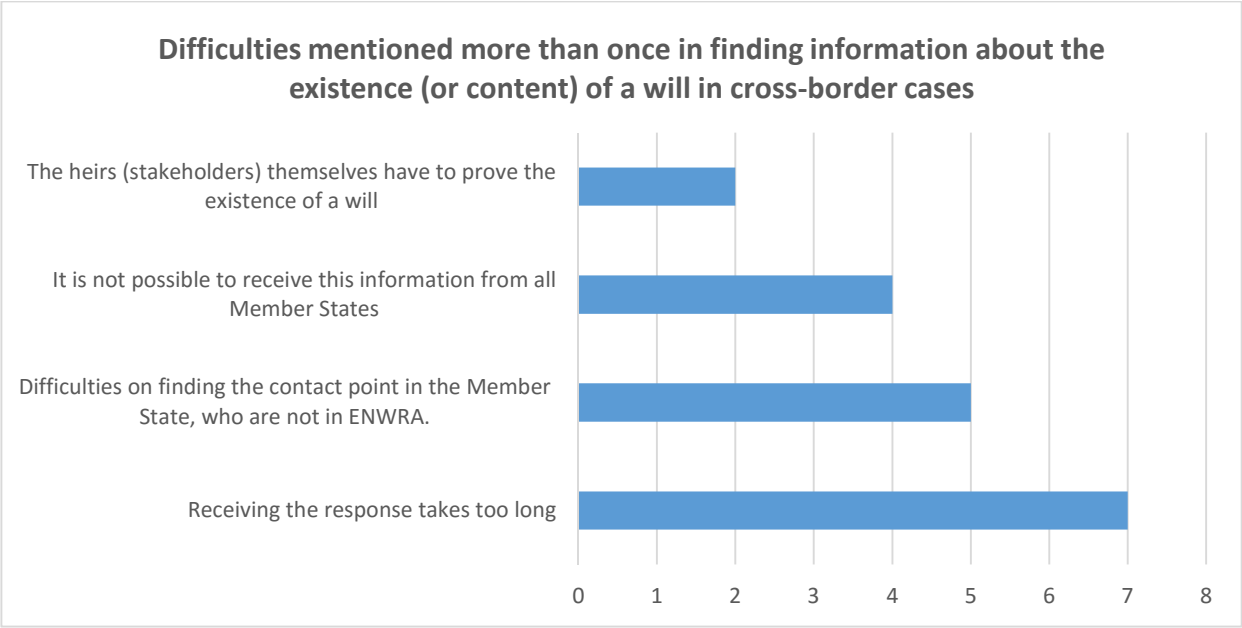

Figure 1. Responses received to the IC RW Survey 2015, question C.7: Please outline the difficulties you have faced if you needed the information about the existence (or content) of will in cross-border cases.

Regarding the matters of possible electronic exchange of the content of wills, the main obstacles detected were mostly related to the fact that the content of a will is not in a digital form or that it is not included among registered information. Copies of wills are also mostly made on paper form only, although in some countries a digital copy or a certified digital copy may be created for archiving needs.

2.4 "EUROPE WILLS" PROGRAMME

In 2008 the European Network of Registers of Wills Association (hereinafter called ENRWA) conducted a programme "Europe Wills", which was co-funded by the European Commission. One of the objectives of this project was to encourage the mutual recognition of last wills, by making it possible for legal professionals and also for European citizens to search for wills throughout the European Union.[6]

There were several conclusions drawn and suggestions given for the future activities in the "Europe Wills" project, which are important also for the current study. One of the statements outlined was that the future instrument of the European Community should explicitly encourage the interconnection of national registers of wills and not be aimed at establishing a European central register.[7]

Regarding the conditions for applying to obtain a copy of a will, it was mentioned most frequently that a death certificate needs to be provided as an essential prerequisite before communicating any information concerning the existence or the content of a will. It may be also necessary to prove one's status as an heir, or having justified interest in the matter, or both of these conditions may apply together.[8]

[6] ENRWA, 2010, p. 3
[7] Ibid., p. 7
[8] Ibid., p. 25-26

A suggestion was also made in the project report to investigate the possibility of interconnecting other national registers, like those containing information about marriages.[9] This might be an option especially for countries, where there are no registers designated to wills, but yet, the information related to succession matters might be present in other registers.

2.5 "Cross-border Wills" Project

In 2012, with the benefit of co-financing from the European Commission, the ENRWA implemented the "Cross-Border Wills" project.[10] The objective of the project was to examine national procedures for opening wills, with a view to harmonising them while respecting their unique national characteristics.[11]

One of the areas of concern pointed out in the report was the difficulty of locating the professional or person with whom the will has been deposited abroad. The other issue of concern was related to the difficulties experienced in communicating the information contained in a will. The study revealed, that while there are no major legal difficulties with communicating the information contained in a will after the succession is completed, then in practice, that would be too late.[12]

It was also stated, that while in general, the legal professionals called to settle a cross-border succession would not be sufficiently familiar with the laws and practices in obtaining information from their European counterparts on the content of a will, it would be essential to identify and to acknowledge these practices more widely.[13]

[9] ENRWA 2010, p 28.
[10] ENRWA 2016.
[11] Ibid.
[12] ENRWA 2015, p. 7-8.
[13] Ibid., p. 15.

3 Patterns in Succession Proceedings

As European citizens are exercising their rights of free movement, it is of utmost importance to discover an existing will of the testator, whenever it is located nationally or abroad, for the succession to be carried out according to it.

The fulfilment of the last wishes of testators involves information exchange and communication between persons and authorities. Modern information systems could support the communication regarding the existence and content of wills between all the parties involved.

A desk research has been conducted for the purposes of current feasibility study on the nature and practices of succession proceedings in the EU Member States. It was studied, who the parties involved in a succession proceeding are and who would need to receive information about the existence of a will and the content of it. Based on the information discovered during the review of the Member States' information sheets at the e-Justice portal and ENWRA's web-site, similarities and also differences emerged in the way successions are conducted. The patterns discovered have provided important information for outlining the possibilities of developing ICT solutions suitable for all Member States for exchanging information on the existence and content of wills.

3.1 Settlement of Succession

There are different approaches taken in the EU Member States on how succession proceedings are carried out. Parties involved differ from country to country. In a number of Member States, succession proceedings are settled by courts and in a majority number of Member States, the succession matters are handled by notaries. There are some Member States, where succession matters are settled by heirs or by executors pointed in the will, and national authorities would become involved only in case of disputes, exceptions or complex matters.

3.2 Recording of Information on Wills

The registration of wills in the Member States may depend on the type of a will that is made by the testator e.g. on whether it is a domestic will or a will authenticated by a notary.
There are differences in the type of data collected and recorded about wills, and the usage and access to the collected information. In some countries, besides the records on the existence of a will, information on the content of a will is also registered or the will is stored in a digital format.

3.3 Access to the Information on Wills

The differences in the practises of handling succession proceedings in the Member States result also in differences in gaining access to the information about the existence and content of wills. There are Member States, where anyone interested may receive information on the existence of wills, and the state is providing web-based access to registries containing information on the existence of wills. In some Member States, only the authorities handling succession may search information about the existence and content of a will through professional data exchange tools, which are not accessible to other persons. In such a case, the person with a legitimate interest should address the information request to the authorized officials.

Based on the results of the IC RW survey 2016, the right to be informed of the existence and content of a last will does not depend on the nationality or country of residence of the enquirer, but rather on having a justified legitimate interest.

3.4 Conclusions for Further Planning Activities

Various options for communication should be analysed in order to engage both the authorities as well as persons with legitimate interests into the electronic information exchange process.

Obtaining information on parties involved and practises used in succession proceedings in each Member State could be made easier and a path to the information shorter for persons from other Member States. For this purpose, ICT solutions could be applied in making the cross-border communication procedures more transparent and less time-consuming.

Additional secure channels for communicating information on the existence and content of wills could be provided for the Member States that do not register all wills or do not register wills in a digital form, considering the specific needs of each Member State.

The differences in the practises of settling successions create different patterns of communication in cross-border successions. The emergence of the typology is taken into consideration in the current feasibility study.

4 Digital Information Security

Information security is a multidisciplinary area of activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats.[14]

There are information security measures established in each EU Member State for managing digital information at national registers of wills or respective document management systems. However, the information security aspects, which have been designed for sharing digital information nationally might not always be suitable for cross-border proceedings. Also, expectations on information security measures may vary from country to country because of the different policies on the usage of information on wills.

In the process of developing cross-border e-services and information exchange, information security principles should be assessed from the point of view of all users, and common agreements on necessary measures established. Additional information security aspects should be evaluated, when information is shared with third parties, such as international and non-governmental associations.

In case of the interconnection of national databases and large-scale information systems, higher level of information security measures should be considered in order to prevent the risk of misuse of the information systems by malicious actors.

While seeking for suitable information technology tools for exchanging of data and documents, also information confidentiality aspects need to be considered, especially when personal data and information on sensitive matters is involved, like in case of wills.

There are three areas of concern related to the potential exchange of digital data and files, which are further discussed in the current study:

1) Information in Digital Form
One of the critical aspects, which should be taken into account in the information exchange in a succession proceeding is related to the electronic forms of documents and data. It would be necessary to gain an overview of the various forms the digital information may appear during the information exchange process, in order to plan appropriate information security measures.

2) Access to Information and User Roles
The next area of concern is related to confidentiality matters. A closer look has been taken regarding the participants, user authentication and applicable access rights in the electronic exchange of data and documents in cross-border successions. The respective levels of access to the information and different user roles have been defined.

3) Delivery of Digital Information
The third area of concern is related to secure delivery, integrity and authenticity of transmitted information. Procedures should be established for confirming that the delivered digital data has not been compromised and altered during the transmission process.

[14] Hilton & Cherdantseva, 2013, p. 37.

4.1 Digital Information on Wills

The majority of the Member States keep digital registers of wills, but digital information exchange has many opportunities for advancement. In some Member States a digitized copy of the content of a will or a certified digitized copy of a will may be created during its registration or archival process. Also, other documents of the succession proceeding may contain information on wills and may be created and exchanged in a digital format.

In the IC RW project survey conducted in summer 2016 it was asked, which digital formats would be accepted in the succession proceeding for conveying information on the existence or content of wills. The terms *digitized copy of a will* and *certified digitized copy of a will* were defined for the purposes of the survey, as follows:

- A digitized copy of a will – a copy of a will, which has been photographed or scanned into an electronic file, based on the original will on paper.

- A certified digitized copy of a will – a copy of a will in digital form, which has been certified by electronic means, as a true copy of an original will on paper. The certification may have been given via a digital signature or other electronic means of verification.

Today, both of these forms of copies of wills are in use by some of the Member States and therefore it would be necessary to make a clear distinction between these two types for the purpose of better understanding issues related to creation, exchange and storage of such digital documents.

12 Member States indicated in their responses to the above mentioned survey the ability to receive copies of wills in various digitized formats. Most commonly mentioned formats were documents with digital signature (bdoc, edoc, ddoc, XAdES, CAdES) and pdf or pdf/a files. Also jpeg/jfif, tiff and doc file formats were mentioned. One Member State responded that any format is suitable, as long as the source is reliable.

For general understanding of the ways the information on existence or content of wills may be presented and shared in a digital format, a sample list has been created based on the survey results mentioned above:

- Data on the existence of will:
    a. Excerpts of records and data on wills from an electronic register, saved in an independent file or delivered to an output device.
    b. Digitized copies made from paper-based original records or documents.
    c. Messages about the existence of a will, in various digital formats.

- Data on the content of will:
    a. Digitized copies of a will
    b. Certified digitized copies of a will
    c. Digital abstracts or excerpts from the two previous formats
    d. Digitized copies of a protocol of opening the will
    e. Messages referring to the content of a will, in various digital formats.

4.2 Access to Information and User Roles

As it is necessary to protect digital data on wills from becoming exposed to persons to whom it is not intended, limitations on access should be determined and respective user roles and rights defined.

The current feasibility study addresses following questions:

1. What type of confidentiality levels need to be set on data on the existence as well as on the content of wills after the death of a testator?

2. Who would be the possible users of such information participating in an electronic transmission of the data and copies of wills in cross-border succession?

In the EU Member States different levels of confidentiality apply to the information on the existence and content of wills. While all Member States have established that before the death of a testator the will needs to be covered with the high level of confidentiality then after the death of a testator the required confidentiality levels differ from country to country. Also, higher levels of confidentiality and more restricted access rights apply to the information on the content of a will compared to the information on the existence of a will.

Depending on a national legislation, there are different groups of persons with different levels of access given to information on wills. This results in a need to determine the information confidentiality levels applied to each user group. In addition, access to the digitized copies or certified digitized copies of will should be determined on the case bases as access is granted to individuals and not to the user groups. For identifying the persons and their eligibility to access information on wills, proper authentication methods should be applied according to the information confidentiality requirements.

4.2.1 Access to Information on the Existence of Wills

In the IC RW survey 2016, the respondents were asked to indicate the possible options for confirming the identity of an enquirer, who receives information about the existence of a will by means of Internet, outside of the ENRW Platform. Among of the 16 respondents, three Member States indicated no necessity for the identification of an enquirer in case he/she would present a death certificate of the deceased or a copy of it. Five countries require certain data about the enquirer. Four countries provide information by public Internet means which require authentication by an e-ID or a digital signature. In countries, where the existence of wills or the content of it is public after the death of a testator, in would not be necessary to identify an enquirer.

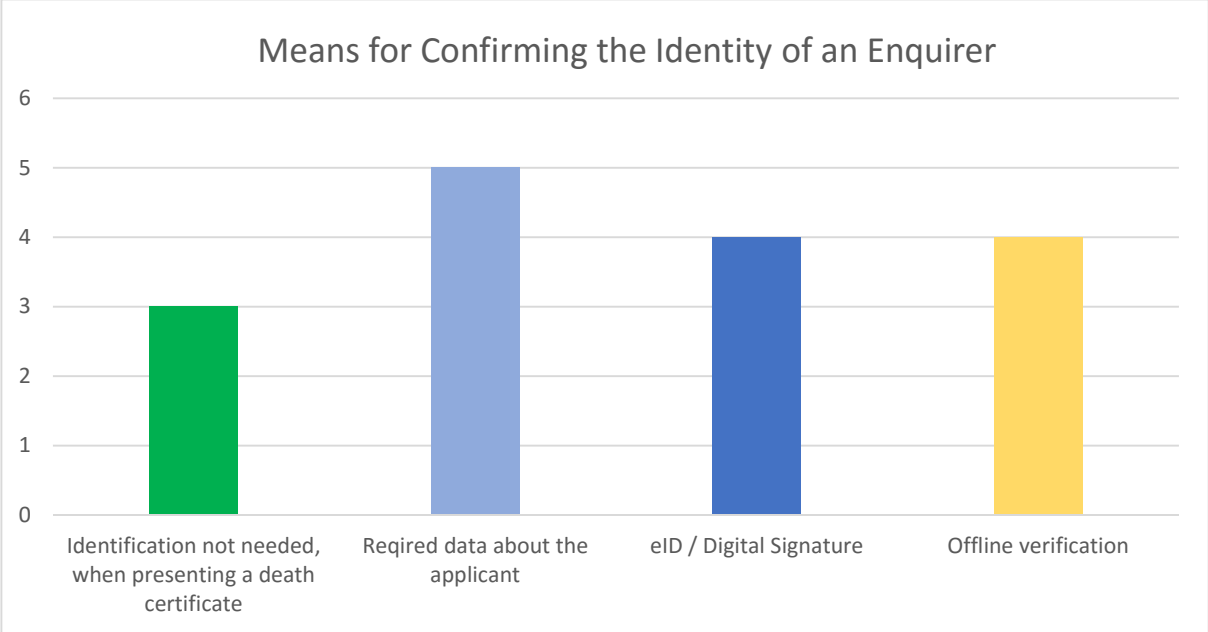

Figure 2. Means of identification of an enquirer on Internet-based enquiry, in case the ENRW Platform would not be available.

The responses indicate the possibility to propose standardised user groups and determine limits on access to the information on the existence of wills. This in turn would enable selecting sufficient and justified means for enquirer identification methods in cross-border data exchange process.

4.2.2 Access to Information on the Content of Wills

The respondents of the IC RW project survey 2016 were also asked to indicate sufficient means of authentication of an enquirer, when providing information about the content of a will via Internet. Out of ten respondents four Member States indicated that the sufficient authentication is based on the profession referring to the enquiries made by the representatives of authorities (as presented in figure 3 below). In three cases a digital signature or an electronic identification was mentioned, and in two cases receiving an e-mail was considered sufficient, without the need for further authentication.

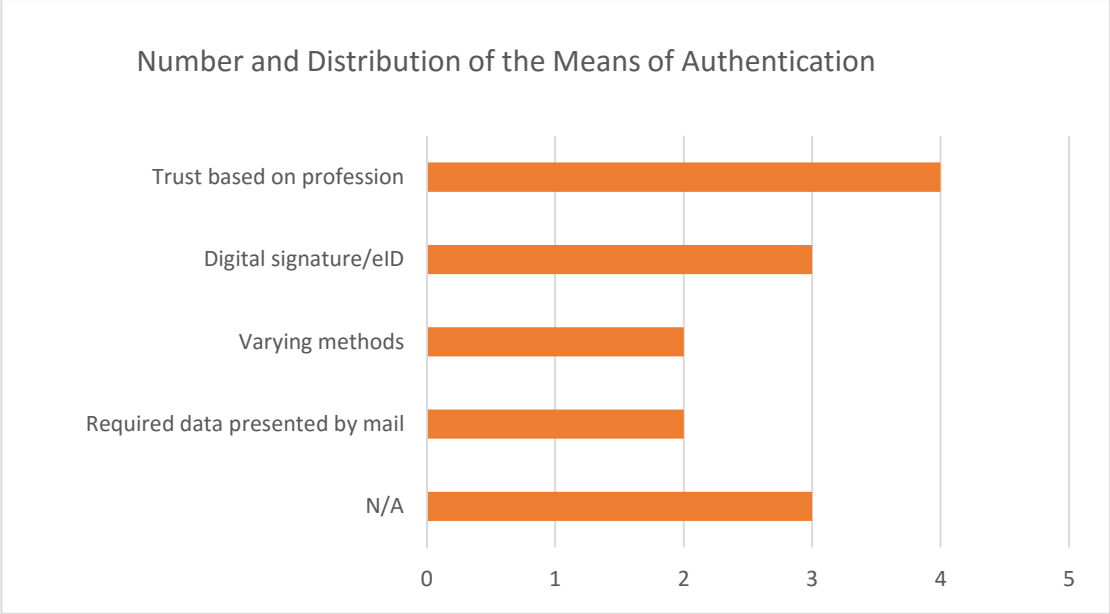

Figure 3. Means of authentication of the enquirer on the content of a will as indicated by the respondents of the IC RW project survey 2016.

The results of the IC RW 2016 survey demonstrate that Member States have set higher restrictions on access to the content of wills, and therefore more sophisticated authentication means should be applied for these cases compared to the enquiries on the existence of wills.

4.2.3 User Roles and Information Privacy

In general, there are some major groups of persons gaining access to the information on wills. In the current study these groups are viewed as user groups having different access levels to the information.

Therefore, two major user groups would be as follows:

- State authorities and other professionals or persons authorised to manage the succession proceeding,
- Heirs and other beneficiaries of the deceased.

These groups may also contain smaller sub-groups, for example legatees and other beneficiaries and persons with legitimate interests, executors of wills, administrators of the estate, notaries or court officials or other state or local government representatives dealing with the succession case.

As data privacy is about protecting a person's right to decide, who could or should not become aware of data related to his/her personal life, the functionality of the information systems should enable posing restrictions on the usage and visibility of data also on a case-by-case bases.

This concern stresses the need for ICT solutions, which would allow setting restrictions on the usage and visibility of data, according to the rights for privacy of referred persons. Therefore, whilst planning the methods for exchanging information on the content of wills or digitized copies of wills, the issues of personal data

protection may arise and may need to be specifically considered. Especially in situations, where different definitions of sensitive personal data are applied in the Member States.

4.3 Delivery of Digital Information

Among other information security measures it is as important to address the issues related to accidental or malicious alteration or deletion of digital data during the information transmission process. Respective measures should be applied to protect data integrity and authenticity of information on the existence and content of wills in digital form.

4.3.1 Protecting the Original Source of Information

In order to provide satisfactory information security levels, both organisational and technical measures should be determined. As a starting point, it would be necessary to take measures for protecting the integrity of original data source. Once the original data has been produced and a final version of a digital document compiled, all actions to modify the original document or presentation of information should be limited and logged. One solution available for such a functionality could be the requirement to seal the digital file with a digital signature, recording simultaneously the date and time of signing.

4.3.2 Safe Information Delivery

There are several aspects in the process of digital information delivery, which should be considered in digital information exchange practices and e-services. In order to provide trustworthy delivery of information, the security risks involved in the communication channels should be evaluated. As Member States have different expectations on security requirements concerning the Internet based delivery channels, it would be practical to group countries according to standardised security requirement classes. It would not be feasible to attempt to apply the same kind of security requirements across all EU Member States, as it would create unnecessary access restrictions from the perspective of the states with more liberal requirements of information delivery methods. However, all means possible should be applied to provide sufficient levels of confirmation of safe and protected delivery of information on wills, taking advantage of already existing and proved technologies and procedures.

The IC RW 2016 survey included questions on the Internet channels perceived acceptable for delivering information on the existence and content of wills abroad. 19 Member States provided their response to a question *´How could an heir or a legal authority from abroad, who does not have an access to the ENRW platform, receive information about the existence of a will in your country, via Internet means?´*.

There were four Member States which indicated two types of viable means of Internet delivery. Altogether 15 countries indicated some of the viable options for Internet-based provision of information on the existence of wills, besides the ENRW platform. Seven Member States indicated that the preferred Internet channel for providing information on the existence of a will would be by using e-mail or encrypted e-mail. Six Member States are providing information on the existence of a will via an Internet portal or a web-site.

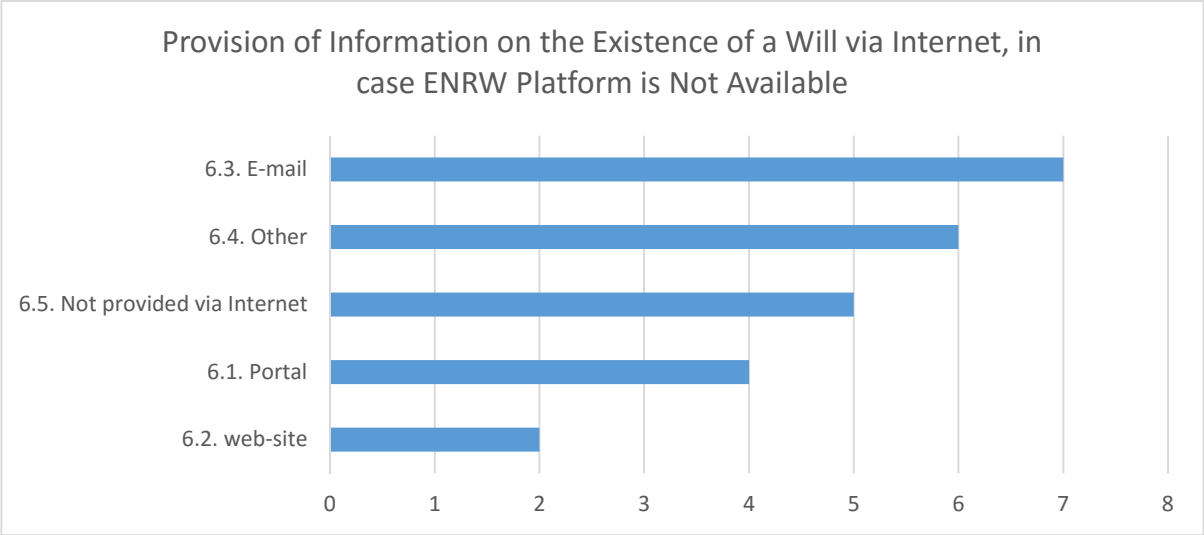

Figure 4. Means of Internet communication (besides ENRW platform) for providing information on the existence of a will to an enquirer from abroad (IC RW Project Survey 2016).

It was also surveyed, by which means of Internet a digitized or certified digitized copy of a will could be forwarded to the entitled persons or authorities from another EU Member State.

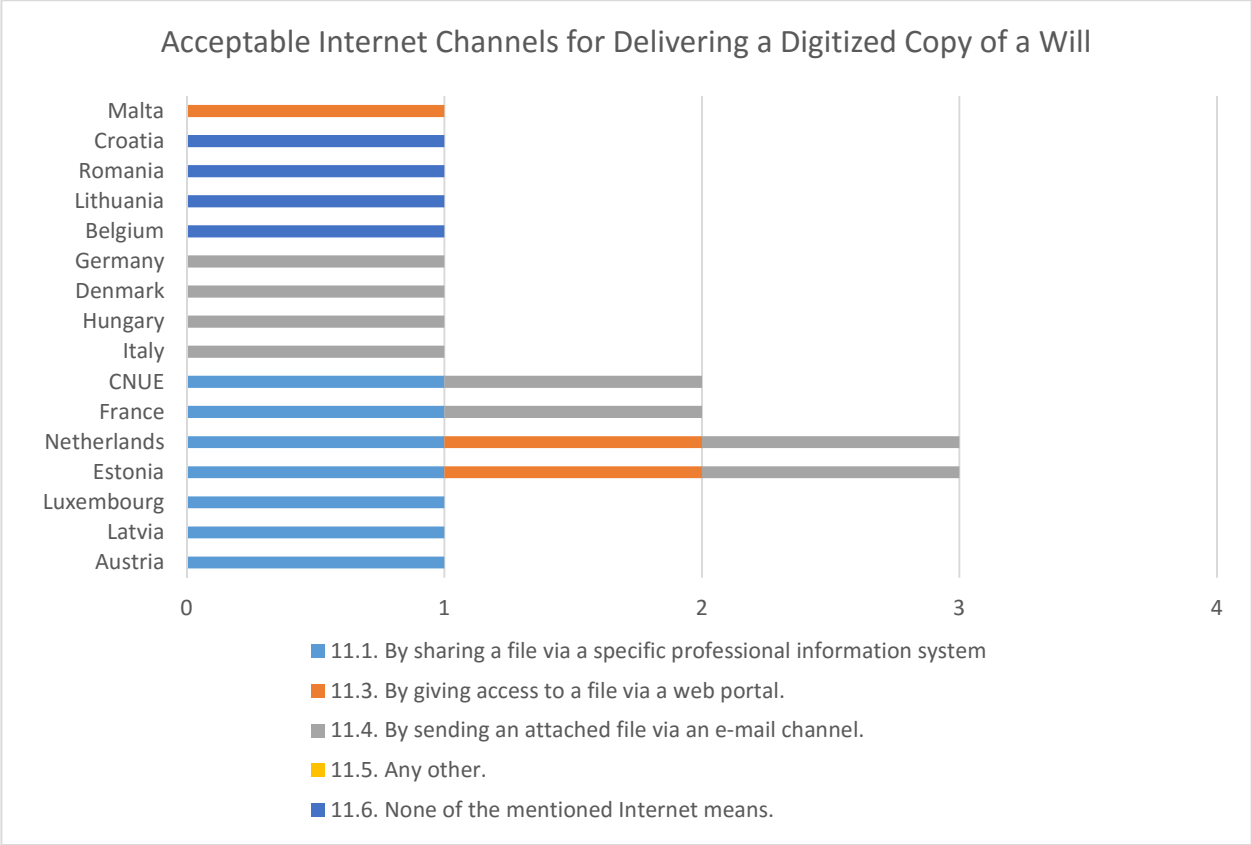

Figure 5. Acceptable Internet channels for the delivery of a digitized copy of a will to abroad (IC RW Project Survey 2016).

12 Member States and also CNUE responded, that the digitized copies of wills could be delivered to another Member State by one or more Internet channels. The most commonly indicated responses show that digitized

copies of wills could be shared by e-mail and through a professional information system. Three Member States also indicated the option of giving access to a file through a web portal.

The IC RW 2016 survey results indicate that some Member States are already using various digital channels for delivering information both on the existence as well as on the content of wills to enquirers nationally and abroad. Their experiences could provide valuable information for creating secure information delivery procedures and channels.
Yet, in case of some channels like e-mails, it would be necessary to re-consider whether higher levels of information security measures should be applied in order to achieve the delivery terms satisfactory for both or all Member States participating in the information exchange process.

4.4 Additional Information Security Risks

Besides the information security aspects covered previously there are some additional aspects outlined below, which also would be necessary to consider in cross-border exchange of information and data on wills, and suitable measures devised accordingly:

- Different practices in verifying an enquirer.
  - The definitions for eligibility of the enquirer should be published and made available to all interested enquirers.

- Lack of information in confirming the legal status of the heir/notary/court official.
  - Schemes for confirming the status of the enquirer should be designed and communicated.

- Insufficient certainty about the identity of the receiver, due to the lower level of authentication procedures.
  - Means for confirming the identity of the information receiver should be defined. The environments or conditions for confirming the sufficient level of authenticity should be established.

- Information about the death of a testator received from a secondary source.
  - Suitable means for establishing the fact on death of a testator, based on the original information source could be designed and respective procedures outlined.
  - Automated database searches should be preferred in case such functionality could be made available.

- Confirming the rights to act as a representative of an adult, a company or a minor.
  - A validation scheme of authorized representation should be agreed.

- Protection of the information systems from malicious users.
  - It would be necessary to log the minimal level of meta-data of user activities in the process of exchanging information on existence and content and of wills.

- Setting requirements on data retention.
  - Questions of data and document retention should be considered, specifically in cases, where information is uploaded into an environment other than national registers or national information systems.

- Outlined security requirements in systems specifications.
  - The information security aspects should be integrated into all elements of future technical specifications of ICT solutions prepared of modified for the exchange of information on the existence and copies or certified copies of wills.

5 Overview of Existing Solutions

Over the past years several large scale European projects have been carried out in order to develop solutions suitable for cross-border exchange of data and documents, authentication and integrated work flows. Below is a brief overview of the information systems developed for that purpose within the domains of e-Justice, e-Government and pan-European cooperation. Some of the solutions described are designed as a technical support services, for example, creating secure network connections, authenticating persons or providing and validating digital signatures. Quite a large number or environments described are intended for collaborative web-based work and file sharing. Some of these are intended for public administrations or specific circle of professionals only, while others are intended for any type of organisations or users.

5.1 STORK Project – Cross Border Authentication

A survey conducted by the European Commission in 2007 showed that a majority (28 out of 32) of the countries used or planned to use, an electronic ID scheme. While some countries had signed agreements on mutual recognition, eID systems differed from one Member State to another and interoperability across borders was almost non-existent.[15] For the period from June 2008 to May 2011 a Large Scale Pilot STORK (Secure idenTity acrOss borders linKed) was launched[16], which aimed at solving the issues of cross-border interoperability of electronic ID. The basic assumption was to build a modular technological infrastructure on top of national eID infrastructures.[17] The idea of Large Scale Pilots (LSPs) was to advance European key ICT policy areas by large scale projects driven by the Member States themselves and co-funded by the European Commission.

Among the six pilot Projects of STORK Project, the following three are of interest for the purposes of the IC RW Project:

Electronic Delivery (Pilot 4)
This pilot developed mechanisms for the secure online, cross-border electronic delivery of documents based on the existing domestic infrastructure in each Member State.[18] The objective of this pilot was to make national eDelivery portals accessible for citizens of foreign countries using their national eIDs. Furthermore, this pilot aimed to create a basic framework enabling countries and their public administrations to send documents to citizens of different countries directly through the citizen's domestic eDelivery portal.[19]

Cross-border Authentication Platform for Electronic Services (Pilot 1)
This pilot was to enable European citizens to access services in one country from any other participating country in a secure way, by using their own nationally issued electronic identity.[20] The STORK platform would not store any personal data and whilst the service provider might request various data items, the explicit consent of the owner of the data, the user, would be always required before his data could be sent to the service provider. This user centric approach taken was in line with the legislative requirements of all the various countries involved that oblige concrete measures to be taken to guarantee that a citizen's privacy would be respected.[21] As a result, a European eID Interoperability Platform was established, and STORK services became accessible by the end-users through their micro-sites linked to the STORK official site and also integrated into existing real live portal services of the underlying STORK interoperability platform.[22]

[15] European Commission. STORK Project, 2010, p. 1.
[16] Leitold, 2010, p. 2.
[17] European Commission. CEF Digital, 2016.
[18] European Commission. STORK Project., 2010, p. 2
[19] STORK Project, 2016.
[20] European Commission. STORK Project, 2010, p. 2.
[21] STORK Project, 2016
[22] STORK Project, 2016

ECAS Integration (Pilot 6)
Since the European Commission operates numerous electronic services that require user authentication, this pilot was to integrate STORK with the European Commission Authentication System (ECAS) in order to facilitate citizens from various Member States accessing the EC services with their electronic identities.[23]

5.2 STORK 2.0 – Cross-Border Authentication with National ID

STORK 2.0 was an EU co-funded project under the ICT Policy Support Programme of the Competitiveness and Innovation Framework Programme carried out during 2012 – 2015, involving 55 organizations, both public and private, across 19 European countries. STORK 2.0 built on the STORK framework for cross-border electronic identification and authentication (eID) of citizens and businesses in the EU and Associated Countries, allowing citizens to authenticate at foreign portals on behalf of themselves or on behalf of other natural or legal persons. It also enabled the use of powers (for digital signatures) designed to verify that signatories of documents have powers enough to present such documents on behalf of the person indicated in the document.[24]

The piloted identification technology of STORK and STORK 2.0 became the basis for e-IDAS technical specifications, and have not been further developed as STORK solutions, but instead, after the ending of the STORK 2.0, the Connecting Europe Facility (CEF) eID and the EU co-funded LSP e-SENS (Electronic Simple European Networked Services) have continued to work together to address the integration of the functionalities of STORK 2.0 into the e-IDAS technical specifications.[25]

5.3 E-CODEX Project – Secure Back-End Delivery

A large scale pilot project e-CODEX (*e-Justice Communication via Online Data Exchange)*, co-funded by the European Commission and the Partners, has been conducted during 2010 – 2016, with the goal to improve the cross-border access of citizens and businesses to legal means in Europe, and also to improve the interoperability between legal authorities within the EU.[26]

As part of the project deliverables for facilitating secure cross-border information exchange are the e-CODEX National Connector platform, Gateway, e-Delivery Platform, and Standalone Connector, which provide an opportunity to connect servers securely, and to issue a trust certificate for a safe delivery of information on the connection from a sender to a receiver.

E-CODEX Tools for Secure Connection

The eDelivery platform (see the Figure 6 and 7 below) enables creating secure connections between national information systems of the Member States or service portals, where the e-CODEX National Connector (adds/checks the Trust-OK token, is responsible for all semantic mapping) and the e-CODEX Gateway (establishes a secure and standardized connection with any other Gateway)[27] are applied on both ends of the connection either the national or portal side.[28]

There is also an E-CODEX Standalone Connector available, which is an independent and secure solution for a digital transmission of sensitive data. This solution would be also suitable for small states that have low volumes of cross-border cases and therefore do not have their own dedicated application to process these transactions. [29]

[23] European Commission. STORK Project, 2010, p. 2.
[24] STORK 2.0 Project, 2015
[25] STORK 2.0 Project, 2015, p. 3.
[26] E-CODEX Project, 2016.
[27] Steigenga, 2016.
[28] Ibid.
[29] Malta Information Technology Agency, 2015.

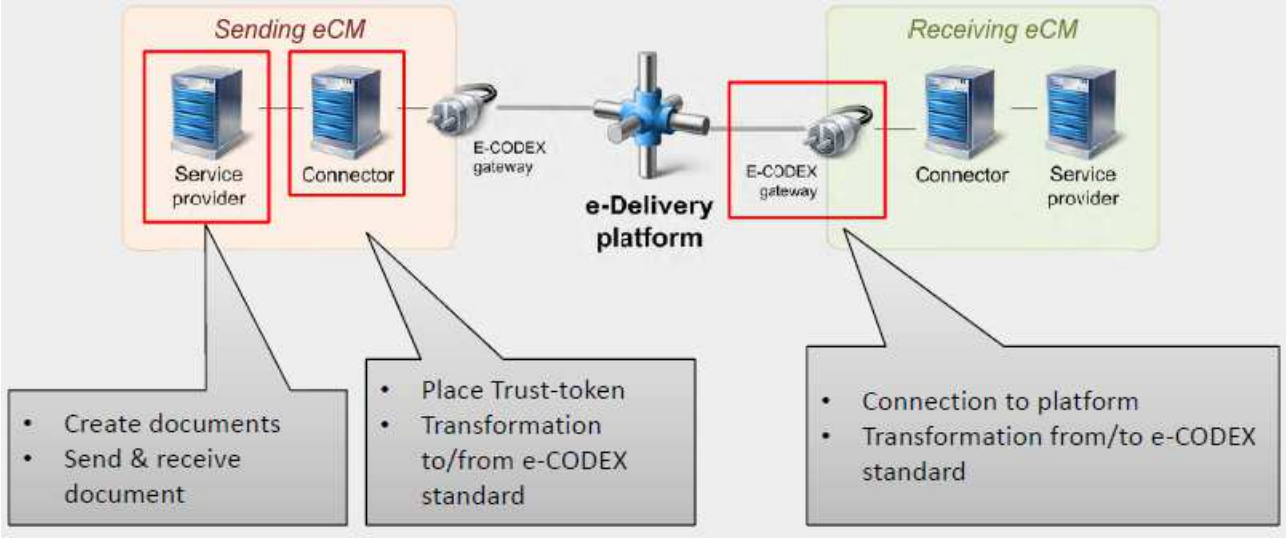

Figure 6. E-CODEX e-Delivery Platform[30]

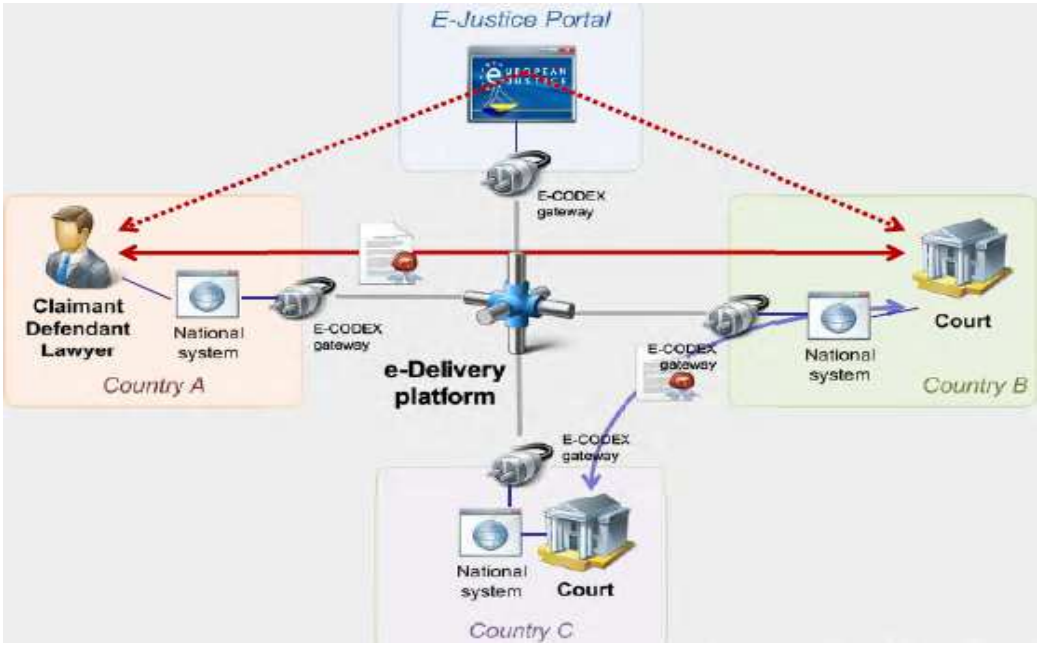

Figure 7: E-Delivery platform with connections to national systems and to the e-Justice Portal.[31]

5.4 E-SENS – Authentication and Delivery of Cross-Border Digital Services

With the understanding, that most EU policies require the exchange of data and documents between citizens, businesses and administrations across borders, the ICT Policy Support Programme sponsored the piloting of eDelivery solution in several policy domains during the period of 2007 and 2016 within the following LSPs:

- PEPPOL (The Pan-European Public Procurement Online) - the LSP of eProcurement, now transferred to the non-profit international association OpenPEPPOL.

[30] Steigenga, Presentation at European Police Congress, 2016.
[31] Ibid.

- SPOCS (The Simple Procedures Online for Cross-Border Services) - the LSP of simplified administrative procedures.
- e-CODEX (the e-Justice Communication via Online Data Exchange) - the LSP of e-Justice.

The piloting of eDelivery in these different domains was quite successful and as a result, a dedicated eDelivery 'convergence' track was launched under the last LSP e-SENS (Electronic Simple European Networked Services) within ICT Policy Support Programme.[32]

E-SENS has been carried out during 2013 to 2016 and it focuses on strengthening digital single market and on facilitating public services across borders. E-SENS is invoked to consolidate and solidify the work done in previous LSP projects, and to extend the solutions to new domains[33], aiming to provide the foundation for a platform of "core services" for the eGovernment cross-border digital infrastructure foreseen in the regulation for implementing the Connecting Europe Facility (CEF).[34]

5.5 CEF Building Blocks Digital Service Infrastructures

The European Commission CEF Building Blocks Digital Service Infrastructures (a.k.a. CEF BB DSIs) provide basic and sector-agnostic digital services, which could be reused to enable more complex digital public services. All the CEF BB DSIs provide a set of core services, enabling services and enhancing services:

A. **Core Services** deliver the basic outcomes and objectives of the CEF Building Blocks, i.e. facilitate cross-border/cross-sector technical interoperability among heterogeneous information systems.

B. **Enabling Services** deliver the core services and the outcomes/objectives that these core services support. It includes the technical and organizational services to enable the implementation of the Standards and Technical Specifications as defined by the core services.

C. **Enhancing Services** are added on top of the core services to create additional value for the users and promote the uptake and reuse of the Building Blocks.[35]

5.5.1 eID Building Block – Secure Cross-Border Authentication

The main goal of CEF eID is to enable secure cross-border authentication between the Member States, whose eID systems apply various security mechanisms for verification and authentication, and which are based on different philosophies, while lacking cross-border recognition and validation.[36]

The CEF eID building block is indented to help public administrations and private online service providers to easily extend the use of their online services to citizens of other EU Member States, making national electronic identification systems interoperable. Once this building block is deployed in a Member State, the mutual recognition of national eIDs becomes possible, and in line with the e-IDAS (electronic Identification and Signature) legal framework (e-IDAS Regulation (EU) 910/2014) and with the privacy requirements of all the participating countries.[37]

5.5.2 e-IDAS Network – Requesting and Providing Authentication

[32] CEF Digital, 2016.
[33] e-SENS Project, 2013, p. 1.
[34] e-SENS Project, 2016.
[35] CEF Digital, 2016.
[36] CEF Digital. Goals, (27.06.2016)
[37] CEF Digital, 2016.

The 'e-IDAS-Network' consists of e-IDAS-Nodes, which can either request a cross-border authentication via an e-IDAS-Connector or provide such authentication via an e-IDAS-Service. In the case of the e-IDAS-Service Node, this may be operated in two different ways:

- e-IDAS-Proxy-Service: an e-IDAS-Service operated by the Sending Member State and providing personal identification data.
- e-IDAS-Middleware-Service: an e-IDAS-Service running Middleware provided by the Sending Member State, operated by the Receiving Member State and providing personal identification data.[38]

5.5.3 eDelivery Building Block - Electronic Delivery of Documents

The eDelivery building block helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens across borders. eDelivery is based on a distributed model, allowing direct communication between participants without the need to set up bilateral channels. Through the use of this building block, every participant becomes a node in the network using standard transport protocols and security policies. As a result of this, organisations that have developed their IT systems independently from each other can start to securely communicate with one another once they have connected to a eDelivery node.[39]

It is important to note that there is no single eDelivery node per Member State but several ones. Each one of these nodes is deployed for a specific Pan-European Project within a given policy domain: eJustice, eProcurement, etc. Typically, the nodes of eDelivery are uni-domain and uni-project. The eDelivery nodes can be implemented at any administrative level (national, regional, local) or by single organisations.[40]

CEF eDelivery is based on a four-corner model, backend systems (corners one and four) exchange messages via Access Points (corners two and three), not directly. The users of the Access Points are the backend systems which need to exchange documents and data cross-borders in an interoperable way. The Access Points use digital certificates, either through a Public Key Infrastructure (PKI) or through mutual exchange, to secure the data during its transmission across two Access Points. The Access Points of CEF eDelivery are not operated centrally, but are deployed independently by public authorities or businesses in a distributed fashion. Also a third-party service provider may be used.[41] CEF eDelivery offers a sample implementation of the e-SENS AS4 Profile, known as Domibus, which was developed in collaboration with the e-SENS and e-CODEX LSP projects.[42]

5.5.4 eSignature Building Block – Signature Creation and Validation

CEF eSignature's main goal is to ensure that public administrations and businesses could create and validate electronic signatures across borders, supporting public authorities in automating the validation of interoperable eSignatures and eSeals coming from any EU Member State, based on the Member States' "Trusted Lists" (the public lists of supervised qualified trust service providers).[43] There is a SD-DSS software which allows performing the automated validation of eSignatures, checking them against the Member States' Trusted Lists. In addition, with SD-DSS the electronic signing of documents may be enabled at the portal of any organisation.[44]

[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] European Commission, 2016, p. 5.
[42] Ibid., p. 11.
[43] European Commission. CEF Digital, 2016.
[44] European Commission, 2013, pp. 3-4.

5.6 X-Road Europe

X-Road Europe is a distributed service-based architecture designed to enable the quick and inexpensive development, provision and use of new electronic services. X-Road Europe enables data exchange in fields that do not yet have a pan-European technical solution, and it could be used by public as well as private sector organisations to transfer electronically any information (documents, metadata) securely from one point to another (between persons or machines). X-Road Europe is based on the Estonian e-government backbone X-road, which was commissioned by the Republic of Estonia in 2001, and operates like a service bus where all services are available in case authorization is given. X-Road Europe is fully compliant with the European Interoperability Framework and it is based on open source, on the EUPL licensing. It has a complex security system: authentication, multilevel authorisation, a high-level log processing system and encrypted data traffic with time stamps. These security solutions ensure that all information systems connected to the environment are identified, that access to services is regulated in the agreements between organisations and that data traffic is logged and provable.[45]

5.7 e-TrustEx – Electronic Trusted Exchange of Documents

e-TrustEx is a project of the Directorate-General for Informatics of the European Commission under the ISA Programme (Action 1.8), under which an e-TrustEx platform is offered to public administrations at European, national and regional level to set up secure exchange of natively digital documents or scanned documents from system to system via standardised interfaces.[46] E-TrustEx may be installed by a public administration or used as a service on the cloud, and it enables mechanisms to ensure integrity, authenticity, confidentiality and non-repudiation of information.[47]

As more and more digital documents containing sensitive information are exchanged between Public Administrations, EU institutions, businesses and citizens, instead of sending these through via simple email, Public Administrations could add an extra layer of security by adopting e-TrustEx.[48]

5.8 EUFides – Cloud Service for Notaries

EUFides is a secure notarial cloud that makes it easier for European notaries to work together on cross-border files. The EUFides platform is governed by an international non-profit association under Belgian law (AISBL), the founding members of which are the Belgian, French, Italian, Luxembourg and Spanish notarial organisations. User interface is available in five languages: English, Dutch, French, Italian and Spanish.[49]

Access Control:
EUFides is described as meeting the highest security standards and guaranteeing absolute confidentiality of files. Notaries from the member notarial organisations can use the platform and also invite a civil law notary from another European country, which is not yet a member to work on a cross-border file. Access rights are issued by the national notarial authorities, and only practising notaries could have access to this service, but it is possible to give access to one's files also to colleagues.[50]

Functionality:
1. Connect using the access right issued by your notarial organisation.
2. Contact a colleague using the European Directory of Notaries.

[45] Estonian Information System Authority, 2013.
[46] European Commission, 2016, p. 2.
[47] Ibid., p. 3.
[48] Ibid., p. 2.
[49] CNUE, 2012.
[50] Ibid.

3. Implement the cooperation contract, governing fees and the sharing of tasks between the notaries.
4. Create files and add documents.
5. E-mail notifications to inform a colleague about the created file or shared document.
6. Downloading and deleting documents from the platform.[51]

5.9 ENN Platform

In July 2016, according to a CNUE's press release an online platform of the European Notarial Network has been opened for the notaries in Europe, who are listed in the directory www.notaries-directory.eu. The ENN Platform allows notaries to contact with the national interlocutors electronically, and to access various legal databases, provides bilingual forms, and facilitates participation in thematic forums and conducting online discussions.[52]

5.10 Bartolus - Signature Verification Platform

The Bartolus platform has been developed as a verification service of electronic notarial signatures for the notaries to conduct checks on any authentic instrument issued in electronic format. In the current state, the verification of notarial signatures is possible for the notaries of Germany, France, Italy and Spain.[53] The verification confirms whether the document has been indeed signed by a practising notary, and whether or not the document has remained unaltered during its transfer.

5.11 ENRW Platform – Search and Exchange of Registry Information

ENRWA has developed a specific tool for exchanging information on the existence of wills abroad. The intermediary ENRW platform is interconnecting Member States´ registers, through a client software. An additional version ENRW Light makes it possible for registers that have not yet been computerised to be queried and to query the other registers, operating through a correspondent, appointed by the register administrator, who will take charge of processing inquiries from and to other registers.[54]

5.12 iSupport - Electronic Case Management

In September 2014, the iSupport project was commenced by the support of the European Union grant under the "Civil Justice" Programme. The objective of the iSupport project has been to develop an electronic case management and secure communication system to facilitate the fast, efficient and cost-effective cross-border recovery of maintenance obligations. iSupport system is intended to facilitate communication between central authorities, to ensure consistent practices at both the European and global level, alleviate translation problems by operating in different languages, provide for electronic transfer of funds and their monitoring, and allow the states to implement paperless case management.[55]

[51] Opstal, 2016.
[52] CNUE, 12.07.2016.
[53] CNUE. Demo Server, 2016.
[54] ENRWA, 2010, p. 17.
[55] Hague Conference on Private International Law (HCCH), 2014.

In 2015 the development of iSupport 2.0 was launched, lasting for a period of two years. The iSupport 2.0 will have a functionality for connecting to the EU e-Justice Portal,[56] based on eDelivery. The outcome might be of interest also for the purposes of designing solutions for exchanging information on wills.

5.13 CIRCABC - Collaborative Spaces

CIRCABC (Communication and Information Resource Centre for Administrations, Businesses and Citizens) supports the creation of collaborative groups, distribution and management of documents in any format, several languages and with version control, and user management and access control.[57] The web-based CIRCABC application is used to create collaborative workspaces, and is freely available for any public or private organisation. It is divided into categories and interest groups, allowing people to manage content, users and communication features. It can also be deployed as a standalone alternative. There is also an open-source software version of CIRCABC under European Union Public Licence 1.1.[58]

5.14 IMI - Administrative Cooperation Platform

IMI (The Internal Market Information System) is a flexible administrative cooperation platform for authorities, which provides a multilingual online tool and facilitates the exchange of information between public administrations across Europe involved in the practical implementation of EU Law. The functionality of IMI allows to identify counterparts in another EU country, ask each other questions with the help pre-translated questions, answers and forms, send notifications, and store and share information that is secure and data-protection friendly.[59]

[56] HCCH, 2016.
[57] European Commission. ISA Programme, 2016.
[58] Ibid.
[59] Ibid.

6 Recommendations on the ICT Solutions

Back in 2010, it was envisioned in the final report of the "Europe Wills" project that in future, we could look into the possibility of directly connecting the persons with whom the wills are deposited, thereby increasing co-operation between the professionals entrusted with this matter.[60] Today we can say that it is technically already possible.

In honouring and fulfilling the last wishes of the testators with the priority to ensure that succession proceedings can be carried out without unnecessary delay, it would be important to develop effective and fast mechanisms for the cross-border exchange of data on the existence and content of wills, focusing equally on providing information to heirs, respective authorities as well as all other parties concerned. In order to take advantage of the technological solutions that support the secure delivery of information according to the expected levels of privacy and confidentiality, good and clearly communicated practices could be agreed between the Member States, together with the uptake of suitable technological applications.

At the beginning of the study, the following questions were posed:

1. Are there any suitable tools existing, that could be applied for communicating information regarding the existence of wills and the content of wills, or would it be necessary to create a new exchange channel?

2. What enhancements to the process of document and information exchange could be suggested, in order to facilitate greater interconnection of registers of wills and to enable more effective succession proceedings?

For outlining recommendations and possibilities for the advancement of the use of existing ICT solutions, the following aspects are addressed in this chapter:

1) information access roles and rights;
2) functionality description;
3) secure networking options.

6.1 Information Access Roles and Rights

According to the IC RW 2016 survey, it is evident that different confidentiality levels apply to the information on the existence of a will, and to the information on the content of a will. There are also great differences between the Member States, regarding who may access and receive such information. This results in the necessity to determine several classification levels of confidentiality and access rights according to the roles in which the enquirers of information would act. Therefore, the ICT solutions exchanging information across borders should be equipped with a possibility to distinguish between the different roles of information enquirers and to provide access to the information based on that.

6.1.1 Information Access Levels

In search for a solution for exchanging information on the existence and content of wills, the authentication of an enquirer could be conducted according to the information confidentiality levels, derived on the basis of information collected with the current study. The table below describes the suggested information access levels to be supported by an ICT solution for cross-border data exchange on wills.

Access level	User group	User group description

[60] ENRWA, 2010, p. 28.

Level 1	Devices	ICT devices and systems that are allowed to proceed after presenting certain amount of technical data for user identification.
Level 2	Anyone	Individuals and systems, who/that may search or enquire information about the existence of a will, after providing certain data about the deceased.
Level 3	Provider of personal data	Individuals, who may receive information after providing required personal data. The confirmation on the payment of an access fee may also be requested.
Level 4	Holder of the copy of the certificate	Persons, holding a copy of the death certificate of the deceased, who might have made a will.
Level 5	Holder of the original death certificate	Persons, holding the true original of the death certificate or a copy of such certificate of the deceased, who might have made a will.
Level 6	Authority representative	Persons, identified based on their professional position and hold access rights to a certain professional information system, or who are listed among the acknowledged professionals of their country.
Level 7	Identified person	Individuals, who will receive information after digitally authenticating themselves.
Level 8	Identified person with legitimate interests	Individuals, whose identity has been digitally authenticated and their legitimate interest for information has been established.
Level 9	Individuals	Individuals, who would be allowed to receive a specific data set of information according to their unique role or need, after digitally authenticating themselves, and providing additional data clarifying their role.

In the case of representatives of any of the persons mentioned in the previous levels, the rights to act as a representative would also need to be confirmed.

The following confidentiality and access levels may be suggested in connection with the expected models of authentication:

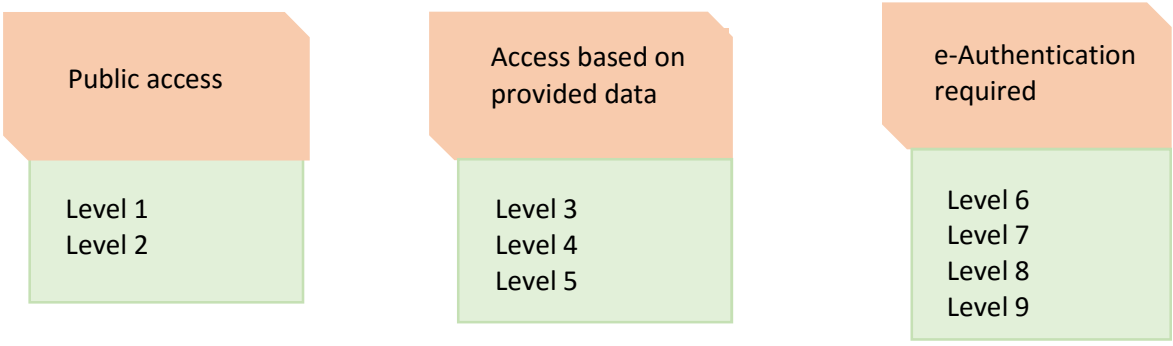

Figure 8. Confidentiality levels linked to the type of access to e-services.

Based on the general information confidentiality rules, the following recommendations could be given for establishing user control levels:

- The access to the data on wills should be determined based on the role and legitimate interests of the enquirer, while the rights to further exploit the received data should also be established, including further sharing with third parties.

- In case the access to data on wills is based on certain data provided by the enquirer, mechanisms should be established for verifying the reliability of input data.

- In case the identity of an enquirer is confirmed on the basis of controlled and trusted lists of professional users, the lists of eligible users should be made publicly available.

- In the case of access based on controlled and trusted lists of professionals, a policy of user administration should be established at national level and made publicly available. The registration of users could be based on electronic IDs, where available, for speedy and reliable update of these lists.

- For authenticating an individual or an organisation, the most reliable source of information should be consulted, typically provided by the state of residence or registration.

- ICT solutions for exchanging information on the existence as well as on the content of wills between the Member States should be available for auditing by an internationally recognised third body authorised to conduct information security audits for ensuring that information security aspects and policies are followed.

6.2 Expectations on Functionality

In order to gain a perspective where information technology could enhance data and document exchange, an initial list of functionality expectations based on the desk research and surveys conducted within the IC RW project, has been drafted and outlined below. These functionalities are a basis for envisioning and describing the solutions suggested.

F1. **Finding an appropriate contact point, that could give information on the existence and content of wills in due time.**

- Describing the steps to be taken by the enquirer, based on their role.
- Providing a list of first contact points, both physical and digital, for enquiring about the existence of a will in other countries.
- Listing suitable options of authentication and means of communication.

F2. **Enquiring information regarding wills located abroad, and receiving responses.**

- Establishing legitimate interests and authentication, if necessary.
- Listing authentication options, and personal data or documents required for successful enquiry.
- Providing access to or delivering the required information and documents according to the terms of the information owner.
- Ensuring the possibility to obtain information and documents from national registers for verifying the enquirer abroad, his/her legitimate interest or right to receive information.
- Compiling an enquiry to be delivered according to the needed level of security.
- In the case of authorities, direct contacts via professional networks would be established for communicating on wills.
- Ensuring the possibility to verify the authenticity of the information received.
- Ensuring the possibility to store the received reply in a secure manner.

F3. **In response to an enquiry from abroad, sharing information and a copy of the will on the terms needed for the receiver.**

- Ensuring the possibility to store the data in a commonly shared workspace and giving access to the files based on individual or user group access rights according to the security principles.
- Creating a reply with data extracted from the registry or entered manually.
- Ensuring the possibility to digitally sign the reply message.

- Ensuring the possibility of setting the retention period of the information or the document, in case it is uploaded in a system other than the national professional register.
- Forwarding all necessary files to selected persons or authorities.

6.3 A Layered Solution for Exchanging Information on Wills

A possible solutions for tackling the concerns related on the necessary steps to be taken for receiving information on wills is described below. This possible ICT solution is based on a layered build-up solution, with connections to the related national and international environments, where the information on the existence and content of wills may be found and shared. The purpose of such layered solution is to consider all user groups and available communication channels together with the necessary authentication methods, according to the requirements of each Member State or owners of the specific connected ICT solution.

A three-layered approach is suggested for the process of acquiring information on wills located abroad. Each layer may contain multiple activities.

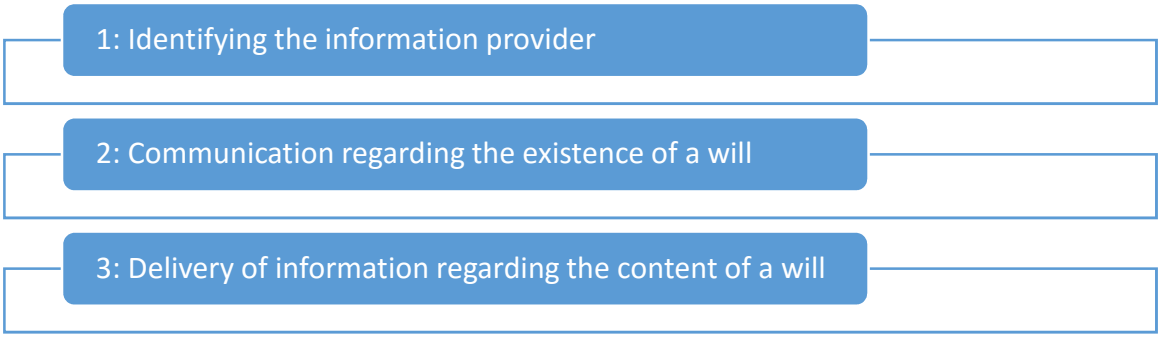

Figure 9. Three layers of activities, which can be supported by ICT solutions suited to each layer.

As indicated by the IC RW 2015 survey, one of the concerns of the authorities handling successions is difficulties experienced in finding the quickest path to the persons dealing with successions or holding a will.

Therefore, the first layer would be an informative layer dealing with finding the persons, authorities or digital services in other Member States to whom an enquiry could be addressed. It would provide an initial overview of the steps to be taken for receiving information on wills from each Member State in a clear, standardised and structured manner. Information would be presented in the form of a decision-tree, accessible at a web site available to all interested persons, such as the e-Justice portal.

At the same time links to the first contact points, including digital access points, would be provided together with the description of conditions under with the information on wills would be released.

The second layer would concern the establishment of facts regarding the existence of a will located abroad. The applicable confidentiality levels would be described for each user group, and when needed, the options for user authentication would be provided.

The third layer would involve communication between the persons and authorities with legitimate interests on the content of a will, and on the transferral of the copies or certified copies of wills or other documents related to the enquiry. The access to information would be determined and the necessary confidentiality levels established based on the user group or an individual.

Each of these layers of activities will be specified further in the sections below.

6.4 Entry via the Information Portal

The first layer of the web-portal would describe the steps to be taken by an enquirer. Together with each step there would be a standardised descriptions of the general practises providing information about the existence and content of wills, along with the specifications on applicable access rights. The enquirer could make a selection presented in the decision tree, which would produce links to the information systems for conducting a search in public portals, or presenting an enquiry to the appropriate contact point through a digital authentication environment or any other suggested communication channels.

The following activities and further information could be presented by the decision tree:

1. the selection of the EU Member State;
2. the description of steps to be taken for receiving information on the existence and content of wills;
3. the indication of the role in which a person is acting when seeking information on the existence or content of a will;
4. the options available for contacting the appropriate contact person, service or institution for receiving the desired information;
5. the specifications on applicable access rights and the listing of available authentication options;
6. the description of fees if applicable, or documents that would need to be presented for searching information on wills.

After determining the appropriate contact point and becoming familiar with the conditions necessary for receiving information on the existence of a will, the enquirer could have a choice of options to proceed, depending on the applicable confidentiality levels and authentication methods. In these cases, where the access to information on the existence of wills would not be public and user authentication would be required, it might be feasible to provide several authentication options. The selection of these options could meet the enquirer verification and authentication requirements of the provider, and at the same time provide the information enquirer with an option to choose the most suitable method.

In the case of the Member States, where the functionality of searching for the existence of wills could not be provided, a information portal could provide a standardised e-mailing facility for sending an enquiry to the first contact point of the Member State over a secure network connection. This would enable to set commonly agreed security standards on e-mail communication, to log the metadata of user activities, and to provide automatic translations of the format or perhaps also of the content of the exchanged messages. In addition, a secure channel of delivery could be provided for forwarding any required electronic documents to the national contact point, along with the message, if required.

In order to establish an approach described above, a collaborative effort could be taken by the Member States. The standardised structure of the decision tree together with the links to the national first (digital) contact points and information on the access rights and user authentication options should be displayed, where needed. Common agreement on access levels could enable information enquiry based on same principles across EU.

6.5 Entry via Professional ICT Solutions

Besides searching information through the information portal, the authorities may also enquire information on the existence of wills through a professional network (e.g. ENRW platform) or ICT solution. The direct gateway for judicial authorities would enable bypassing the information portal. In that case, the search could start directly from the second layer and therefore an initial authentication of the user would be carried out by logging in to a professional ICT platform.

Both the entry through the portal and the entry through the profession-based platform are described in figure 10 below, together with the presentation of the subsequent steps towards receiving information on wills.

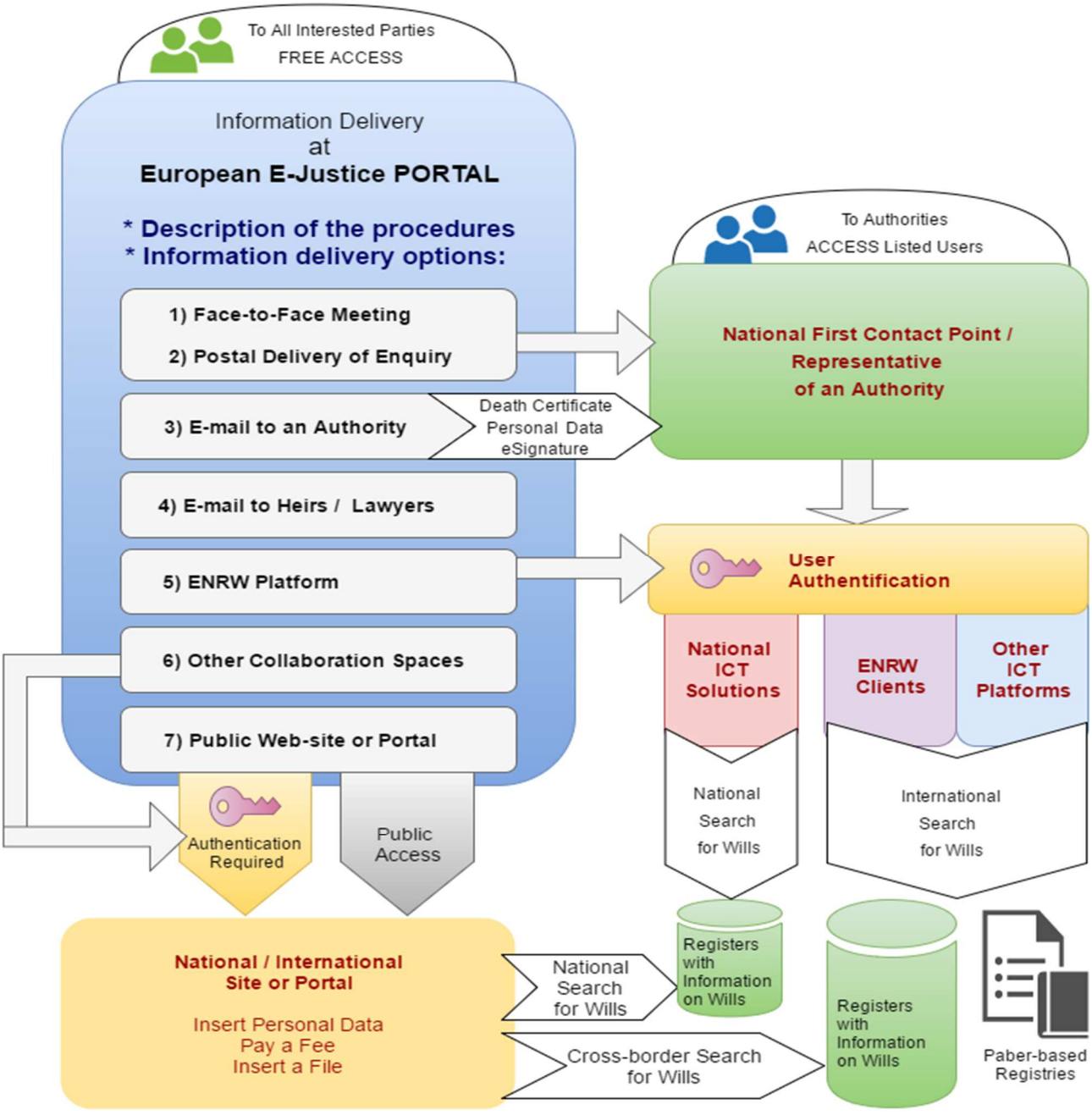

Figure 10. An overview of possible layout of an ICT solution for receiving information on wills.

6.6 Informing an Enquirer about the Existence of a Will

The second layer of activities is concerned with the communication about the existence of a will. There are several options used in the EU Member States for receiving or exchanging information on the existence of a will. For example, information may be received by conducting a search in a registry, without any intervention or involvement of persons at the location of the information. Or, as revealed from the IC RW survey 2016,

such information could be received by e-mail or via a professional collaboration network, like the ENRW Platform.

While moving from the layer of providing information about the necessary steps to the layer of providing information on the existence of wills, it would become necessary to apply higher levels of access control and enquirer authentication methods.

Therefore, a secure message delivery service could be in place at the information portal for sending standardised enquiries to the first contact points of the Member States. The commonly agreed delivery of the user information data set and authentication would be integrated into the security requirements. In addition, an automated message translation could be applied, or pre-prepared messages could be used. As a next step, a response to the enquiry could be provided in the pre-prepared form, delivered through a secure environment selected from a list of presented options.

Similarly, there were several ICT tools presented in chapter 5, which might be suitable for providing secure authentication and network connections for communicating information on the existence of wills and on the content of wills across borders. The ICT tools already previously co-funded by the European Commission should be re-used if possible and their suitability should be analysed in greater details together with the system owners, having the competence and knowing the possible necessity for further developments and investments.

6.6.1 Considerations on User Authentication

As the Member States require different levels of security for revealing information about the existence of a will and for providing digitized copies of wills, the requirements on enquirer authentication vary greatly from country to country. Therefore, it may not be feasible to attempt to provide a single solution for enquiring information from 28 Member States, but rather a combination of solutions could be applied, according to each country's succession practises, ICT readiness and information security requirements.

Based on the e-IDAS Regulation all Member States would be expected to complement their national public e-service environments with the ability to recognise the national electronic identification means of other Member States. Currently there are more than 20 Member States having e-ID systems in place already. In the upcoming years it may be envisioned, that Member States' national digital entry points would be made e-IDAS-compliant, enabling persons from other Member States to access the services currently available only to the residents or e-residents of the state. As the Member States are continuously making considerable efforts to provide secure and reliable e-services nationally, and enabling e-IDAS compliant authentication at national state portals or sites for searching information in the registries, it would be feasible to take advantage of the nationally developed e-IDAS compliant authentication means, also for authenticating the enquirers on the existence and content of wills. Once authenticated at the national digital entry point, the enquirer may be entitled to continue with the search on the data on wills in a national register, or to send an enquiry to the respective authority.

The e-IDAS e-ID building blocks for user authentication could be also integrated into non-governmental and international web-based collaborative spaces. This would allow using the national electronic identification tools also at the sites or ICT solutions developed independently from any specific Member State. As another option, these solutions could also apply the authentication services provided by trusted third parties. Eventually, the cooperation networks of the Member States and partnering organisations would definitely benefit from the mutually acceptable authentication methods and agreed types of secure networking channels.

There are also various tools available that authenticate users based on a username and a password. In the case of deploying such information systems for exchanging sensitive data, the user management policy could be made public and auditable, giving the possible users a basis for evaluating the security and suitability of that tool for cross-border communication. Regarding the professional networks, where the initial authentication of a user would not meet the requirements of other Member States' information providers, links to additional means of authentication could be provided, in order to allow users to continue to seek information they need,

seamlessly via the secure and controlled environments, meeting the security requirements set in each Member State or collaborative network.

6.6.2 Considerations on Network Security

Besides authenticating and verifying the persons involved in the communication process, it would also be necessary to establish a secure communication channel between the point sending the enquiry and the one receiving the enquiry, in order to secure data integrity during its transportation over networks.

The Figure 11 below proposes an overview of various possibilities for connecting information systems of the Member States or international collaboration spaces via a secure network.

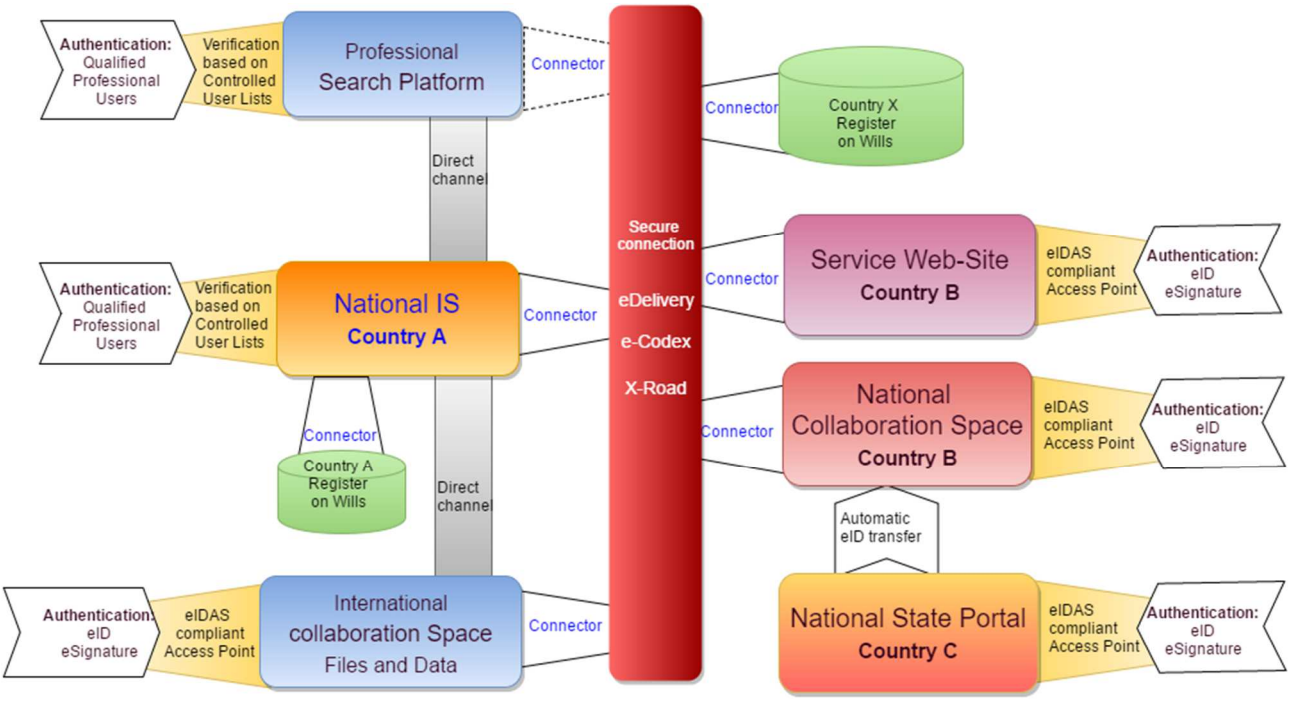

Figure 11. Overview of possibilities for connecting information systems over secure network connections, and for authenticating users of the network of interconnected systems.

For higher levels of network security in the information exchange process, tools like the e-Delivery, the e-CODEX or the X-Road may provide secure connection with the e-Justice portal and with other national or international (non-governmental organisation) information systems. As described in chapter 5, these solutions would provide authentication and multilevel authorisation and secure networking channels for information delivery from point to point. In the Member States, where a national digital access point is not available, the functionality of providing a secure connection between organisations or networks, could be provided by a trusted third party.

6.6.3 Digital Authentication vs e-Signature

There have already been a number of ICT solutions developed for checking national digital signatures. Some of the existing ICT solutions provide the functionality of placing digital signatures, together with the authentication functionality. In such cases it would be advisable to distinguish the situations, where digital authentication would be needed, and the situations where the placing of a digital signature would be needed.

If the digital signature would be applied only for confirming the authenticity of an enquirer, it would be sufficient to apply digital authentication instead, together with logging the activities performed.[61]

Some of the signature verifying solutions, like Bartolus, mentioned in chapter 5, are aimed towards verifying the signatures of different countries in a single service environment. The e-IDAS network solution and the SD-DSS software of the CEF e-Signature building block allow performing an automated validation of e-signatures, checking them against the Member States' Trusted Lists. Also, with SD-DSS, the electronic signing of documents can be enabled at the portal of any organisation.[62] This functionality would provide a new opportunity in the coming years to authenticate persons and verify signatures from all Member States having the respective e-IDAS building blocks integrated.

6.7 Sharing Document Files and Copies of Wills

The third layer of the activities, which could be supported by an ICT solution is concerned with providing access to files and functionality of a secure file transfer, including exchanging copies or certified copies of wills. Once the authentication of the user and the secure information exchange channel has been established, files could be transferred in a controlled environment from the original information source to a secure collaborative workplace or directly to the enquirer.

For the highest security, the authentication of a user at such a file sharing environment could be based on the national e-ID, or conducted through national digital entry points and state portals, together with establishing the access rights based on the user groups or at an individual person's level. After the enquirer authentication at the national entry point, the person could either use national e-services or enter to the collaborative workspace.

6.7.1 Collaborative Spaces

Besides the secure file sharing areas provided by the Member States' national solutions, there are a number of environments described in chapter 5, which have been developed for the collaborative web-based work and file sharing. Some of these are intended for public administrations (e-TrustEx) or for a specific circle of representatives of same profession or area of activity (EUFides), while others are for all types of organisations or users. In each case, the purpose is the establishment of a common digital space, where the rules of conduct and practices may be commonly agreed, and the appropriate confidentiality and access levels determined.

For meeting the needs of higher levels of user authentication, an e-IDAS compliant third party authentication point could be established also at such a collaboration space owned by a commercial or non-governmental service provider. Similarly, such a secure collaborative environment for exchanging the copies of wills could be provided by the European Commission and its institutions, acting as a third party service provider or a hub between various national or European networks.

Environments like CIRCABC and iSupport described in chapter 5 may be considered as likely suitable for communication between organisations of different nature, or for communicating with heirs and their representatives. These environments could be taken into consideration and mutually tested by these Member States which would be seeking for a secure file exchange platform for exchanging the copies of wills with other states' authorities and also with private persons. Based on these tests more detailed recommendations could be provided.

As the Member States have different levels of readiness regarding the exchange of digital documents, then for any further developments the Member States could assess the possibility of following the recommendations of this study, based on their specific needs, future strategic visions and funds available.

[61] Erlich, M., Information System Authority. Estonia, 2016, p. 5.
[62] European Commission, 2013, pp. 3-4.

Also the suitability of the ICT platforms or solutions reviewed in the chapter 5 and suggested for consideration in chapter 6, should be analysed together with the system providers in more detail from the perspective of national needs and possibilities.

6.8 Other Development Opportunities

In addition to the solutions described above, a number of additional recommendations can be drawn for further steps to enhance the European collaboration in exchanging information regarding wills. These recommendation are presented in the sections below.

- **Standardized Enquiry Form**

A standardised enquiry form on the existence on wills or ability to deliver copies of wills could be prepared, with unified data fields and definitions of input options. This type of form would enable to exchange enquiries between the information portal and national information systems, or between professional networks. The form could be either multi-lingual or with the automatically translated form fields.

- **Synchronized Display of Information on Factsheets**

According to the IC RW survey 2015, there were some difficulties identified by the respondents in finding up-to-date information regarding the steps to be taken in the case of documents and information needed regarding wills made in other Member States. Therefore, it would be recommended that the e-Justice portal provide the necessary information for the decision tree solution on enquiring information regarding wills, in a precise and standardised way, which in turn could be usable for the development of a web-based solution for providing smoother paths.

- **Advanced Search Opportunities over Public Records**

The IC RW survey 2016 revealed that there are currently some Member States enabling public searches from their national register of wills. As an advanced opportunity, a simultaneous search could be considered made available by a wider circle of Member States based on standardised enquiry forms, together with the e-IDAS authentication mechanisms if needed.

7 Summary of the Feasibility Study

The current feasibility study has been carried out within the frame of the project "Further developments in the area of interconnection of registers of wills", with the goal of analysing conditions needed for establishing secure electronic cross-border channels for exchanging certified copies of wills.

The earlier studies regarding the cross-border succession and the practices of the Member States were reviewed for better understanding of the issues involved in the digital information exchange. The differences discovered in the practises of handling succession proceedings also result in different expectations on information confidentiality. This finding was taken into consideration in the recommendations proposed for possible further enhancement of digital information exchange on wills.

The IC RW 2016 survey results indicated that some EU Member States are already using various digital channels for delivering information both on the existence and on the content of wills to enquirers nationally and abroad. Their experiences could provide valuable information for creating secure information delivery procedures and channels.

The information security aspects as well as the functionality and confidentiality requirements were studied, together with the areas related to the information in digital form, access to digital data and files on wills and the safe delivery of information. The secure network connections and possibilities for enhancing the exchange of succession related information electronically between the EU Member States were explored, and the recommendations and alternatives presented.

As the sustainability and wider usage of already existing systems is essential in the area of e-Justice, various currently available ICT solutions were reviewed for establishing an overview of the current state of play and for avoiding possible overlap of the work done. However, a detailed analysis regarding technical requirements and possible costs should be carried out by the information system owners as the next step.

The study provided evidence that it would be possible to start moving towards the further application of modern ICT tools in the successions proceedings, especially in relation to the e-IDAS standardized solutions applicable to the public sector and governmental institutions in the following years.

More specifically, the possible steps for a wider delivery of information on wills and for greater access to the information available digitally, a multi-layered approach outlining concrete activities for each layer, an initial list of functionality expectations and an initial description of a user access classification were provided.

The interoperable ICT systems and a secure connection channel for linking different types of existing systems could be considered a flexible way for developing the area of interconnection of registers of wills further by involving all Member States and interested parties.

Member States are encouraged to analyse the possibilities for following the recommendations of this study in order to take further steps based on the specific needs, future strategic visions and funds available.

8 Bibliography

1. CEF Digital. (2016, July 1). *eDelivery Background*. Retrieved from eDelivery: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Background

2. CEF Digital. (2016, July 1). *Goals*. Retrieved from eID: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+Goals

3. CEF Digital. (2016, July 1). *Large Scale Pilots*. Retrieved from eDelivery: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Large+Scale+Pilots

4. CEF Digital. (2016, July 1). *Service Offering*. Retrieved from CEF building blocks: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Service+Offering

5. CEF Digital. (2016, July 1). *Solution description* . Retrieved from eID: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+Solution+description

6. CNUE. (2012). *EUFides. A collaborative workspace for European notaries*. Retrieved from Services: http://www.notaries-of-europe.eu/index.php?pageID=8033

7. CNUE. (2016, July 12). *ENN Platform opens to Notaries of Europe.* Retrieved from CNUE News: http://www.notaries-of-europe.eu//index.php?pageID=13885

8. E-CODEX. (2016). *Technical Background*. Retrieved from About the Project: http://www.e-codex.eu/about-the-project/technical-background.html

9. ENRWA. (2010, March 17). *"EUROPE WILLS" PROGRAMME. Final Report.* Retrieved from http://www.arert.eu/IMG/pdf/rapport-final-en.pdf

10. ENWRA. (2014, October 31). *"Cross-Border Wills" (CroBoWills) Project. „Review of national practices regarding the opening of wills in Europe".* Retrieved from http://www.arert.eu/IMG/pdf/etat-des-lieux-2014-10-31-en.pdf

11. ENWRA. (2015, March 12). *"Cross-border Wills" (CroBoWills) Project". Final Report.*

12. ENWRA. (2016, March 24). Retrieved from The communication of the information contained in wills – "Cross-Border Wills" project: http://www.arert.eu/-La-communication-des-informations-.html

13. ENWRA. CroBoWills Project. (2014). *Summary report of national practices related to the opening of wills in Europe.* Retrieved from http://www.arert.eu/IMG/pdf/synthese-2014-10-31-en.pdf

14. e-SENS Project. (2013, April 12). *e-SENS "Electronic Simple European Networked Services" launched.* Retrieved from "Electronic Simple European Networked Services" launched

15. e-SENS Project. (2016). *About the project*. Retrieved from http://www.esens.eu/content/about-project

16. Estonian Centre of Registers and Information Systems. (2016, July). IC RW Survey Report 2016.

17. Estonian Information System Authority. (2013). *X-Road Europe*. Retrieved from Data Exchange Layer X-Road: https://www.ria.ee/en/x-road-europe-en.html

18. Estonian Ministry of Justice. (2015). Results of the Questionnaire on Registers of Wills.

19. European Commission. (2013). *Cross-border eSignature Creation and Validation Made Easier.* Retrieved from http://ec.europa.eu/isa/documents/cross-border-esignature.pdf

20. European Commission. (2016, May). *CEF eDelivery Access Point. Component Offering Description.* Retrieved from https://encrypted.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiBivHqjYzOAhWCkywKHSMmC94QFggdMAA&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F23003387%2F(CEFeDelivery).(AccessPoint).(COD).(v1.04).docx%3Fv

21. European Commission. (2016). *e-TrustEx. Facilitating Digital Data Exchange.* Retrieved from http://ec.europa.eu/isa/actions/documents/e-trustex_brochure.pdf

22. European Commission. (2016, February). *Introduction to the Connecting Europe Facility eSignature building block.* Retrieved from Discover eSignature: https://ec.europa.eu/cefdigital/wiki/download/attachments/23003331/%28Building%20Block%20DSI_IntroDocument%29%20%28eSignature%29%20%28v0.0.20%29.pdf?version=1&modificationDate=1459425077091&api=v2

23. European Commission. CEF Digital. (2016, June 27). *Large Scale Pilots.* Retrieved from eID: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+Large+Scale+Pilots

24. European Commission. CEF Digital. (2016, july). *Background.* Retrieved from eSignature: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+Background

25. European Commission. Directorate-General for. Věra Jourová. (2016, June). *Fact Sheet. June 2016.* Retrieved from http://ec.europa.eu/justice/civil/files/fact_sheet_public_docs_en.pdf

26. European Commission. ISA. (2016). *IMI.* Retrieved from Our solutions for you: http://ec.europa.eu/isa/ready-to-use-solutions/imi_en.htm

27. European Commission. STORK Project. (2010, November). *Secure Electronic Identity Across Europe.* Retrieved from https://www.eid-stork.eu/dmdocuments/public/eID_Factsheet_FINAL%20v2_Nov10.pdf

28. Hilton, & Cherdantseva. (2013). "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing.

29. Hoyer, H. (2014). *Master Thesis: Planning of Cross-Border E-Services. The Case of Digital Prescription.* Retrieved from https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Uliopilaste_teadustoode_konkurss/h_hoyer.pdf

30. Information System Authority. Republic of Estonia; Erlich, Mark. (2016, June). *e-Signatures in Europe and Their Treatment in Estonia. Instructions and Advice for Handling e-Signatures* . Retrieved from https://www.ria.ee/public/PKI/EL_e-allkirjade_kasitlemine.pdf

31. Leitold, H. (2010). *Challenges of eID interoperability: The STORK Project.* Retrieved from http://dl.ifip.org/db/conf/primelife/primelife2010/Leitold10.pdf

32. Malta Information Technology Agency. (2015, June 10). *E-Codex General Assembly meets in Malta*. Retrieved from https://mita.gov.mt/en/News/Pages/2015/e-Codex-General-Assembly-meets-in-Malta-.aspx

33. Opstal, B. v. (2016). Cross Border Transactions In Europe (Presentation).

34. Steigenga, E. (2016, February 24). *E-CODEX in Cross Border Criminal Justice.* Berlin: European Police Congress. 3C: Electronic judicial file.

35. Steigenga, E. (2016, March 2). Working Party e-Justice, Expert group on registers of Wills. Presentation slides. Brussels.

36. STORK 2.0 Project. (2015, November 23). *Press Release*. Retrieved from https://www.eid-stork2.eu/images/stories/documents/stork%202.0_pressrelease_final2.pdf

37. STORK 2.0 Project. (2015, November 18). *STORK 2.0 Code is Available at JOINUP!* Retrieved from https://www.eid-stork2.eu/index.php?option=com_k2&view=item&id=2108:18-11-2015-stork-20%E2%80%99s-software-available&Itemid=130

38. STORK Project. (2016). *Home*. Retrieved from https://www.eid-stork.eu/index.php?option=com_content&task=view&id=297&Itemid=5

39. STORK Project. (2016, July). *Pilot 4. Electronic Delivery - To develop cross-border mechanisms for secure online delivery of documents*. Retrieved from https://www.eid-stork.eu/pilots/pilot4.htm

40. STORK Project. (2016, July). *Stork at a Glance*. Retrieved from https://www.eid-stork.eu/