

FEASIBILITY ANALYSIS FOR AN EU DIGITAL DEPOSIT SYSTEM



June 2018

ISBN 978-92-9156-250-3 doi:10.2814/666851 TB-04-18-147-EN-N

© European Union Intellectual Property Office, 2018

Reproduction is authorised provided the source is acknowledged

TABLE OF CONTENTS

CONTEXT AND BACKGROUND OF THE FEASIBILITY ANALYSIS	4
EXECUTIVE SUMMARY	6
1. INTRODUCTION	10
2. SUMMARY ANALYSIS OF VOLUNTARY REGISTRATION AND DEPOSIT SYSTEMS IN SELECTED EU MEMBER STATES.....	12
3. STRUCTURE OF THE DIGITAL DEPOSIT SYSTEM FOR THE FEASIBILITY ANALYSIS.....	16
4. LEGAL FEASIBILITY	31
5. TECHNICAL FEASIBILITY	41
6. IMPACT.....	46
7. COSTS	49
ANNEX I: SUMMARY OF REPLIES TO QUESTIONNAIRE FOR SURVEY ON REGISTRATION/DEPOSIT SYSTEM(S)	50
ANNEX II: QUESTIONNAIRE ON REGISTRATION/DEPOSIT SYSTEM(S)	70

CONTEXT AND BACKGROUND OF THE FEASIBILITY ANALYSIS

It was brought to the attention of the European Observatory on Infringements of Intellectual Property Rights (the Observatory) that in various EU Member States, public bodies such as ministries or intellectual property (IP) offices manage IP deposit systems. This includes Benelux, Spain, France, Italy, Hungary, Portugal and Romania. However, most EU Member States do not have a publicly managed IP deposit system. At the same time, a number of private systems exist in the EU market. These systems offer ‘registration’ or deposit of content as a competitive commercial service.

Against that background, the European Union Intellectual Property Office (EUIPO) decided to look into the feasibility and possible benefits of establishing an EU Digital Deposit System. Such a system would provide simple and inexpensive access to a deposit service in all EU Member States through a central tool administered by a public authority, with clarity for users as regards the (legal) value of the deposit obtained. It would fulfil significant evidentiary functions.

In particular, individual creators, inventors and small businesses would benefit from an EU Digital Deposit System. It could be a significant first step in the innovation process, that is, in the preliminary phase of an application for a design or a patent. It would be useful in conflicts where the anteriority of ownership or the priority of the claim must be resolved. A deposit could help rights holders to deliver evidence when they submit a take-down notice to an online platform, particularly in relation to enforcement of intellectual property rights (IPR) in the online environment. Evidence generated by the EU Digital Deposit System could also facilitate the work of online platforms (including smaller ones), and help them to take down illegal content more quickly.

Alongside the Feasibility Analysis, the Observatory dealt with the deposit of (digital) content in two other publications. First, the Oxford Intellectual Property Research Centre conducted a research study on the functioning of voluntary registration and deposit systems in the United States of America (USA) and in the People’s Republic of China¹ (China). The study concluded that voluntary copyright registration and/or deposit can be of considerable practical use, including in the context of national and possibly in international litigation, online enforcement or commercial activity.

¹ Gangjee, D.S., Dinwoodie, G.B., Mogyoros, A., Zhao, B., Study on voluntary registration and deposit systems: United States and China, conducted for the EUIPO by the Oxford Intellectual Property Research Centre, November 2017, European Union Intellectual Property Office, 2018. The study will be available on the Observatory’s website, <https://euiipo.europa.eu/ohimportal/en/web/observatory/observatory-publications>

Second, the EUIPO, in collaboration with the European Audiovisual Observatory, produced a report on deposit systems for audiovisual works². The report shows, inter alia, that there is a variety of systems in the 12 Member States analysed³, covering different territories, users and types of content. Systems that were established for the main purposes of facilitating IP enforcement and the preservation of cultural heritage coexist in the market.

² Arias Burgos C., Cabrera Blázquez F.J., Cappello M., Fontaine G., Poch A., Schönherr F., Valais S., Deposit systems for audiovisual works, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2017, available at https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Deposit_Systems_for_Audiovisual_Works/Deposit_Systems_for_Audiovisual_Works_en.pdf

³ The Benelux countries (Belgium, Luxemburg and the Netherlands), France, Germany, Hungary, Italy, Lithuania, Portugal, Romania, Sweden and the United Kingdom.

EXECUTIVE SUMMARY

A Digital Deposit System at EU level should enable authors, inventors, creators and individuals and businesses in general to keep evidence of the existence of their works or other information at a certain point of time through a central tool that operates in a secure and highly confidential manner, administered by a public authority. The Feasibility Analysis for the establishment of such a system consisted in the following four steps: **(1) gathering information on existing national practices concerning voluntary registration or deposit systems; (2) proposing different options for the structure of a Digital Deposit System; (3) performing a legal and technical feasibility evaluation of the proposed options; and (4) assessing the impact and costs of such a solution.**

As a first step, the European Observatory on Infringements of Intellectual Property Rights (the Observatory) of the EUIPO carried out a survey. The survey was distributed to the Observatory's public sector stakeholders in selected EU Member States, where there are publicly managed voluntary registration/deposit systems (digital or otherwise). The replies received from the following Member States were thoroughly analysed and compared: Benelux, Spain, France, Italy, Hungary, Portugal and Romania. In addition, the functioning, purpose and performance of a private company offering a digital deposit service was studied. The replies to the survey revealed, inter alia, that all publicly administered registration/deposit systems studied have their legal basis in national laws, often in national IP or copyright acts. According to the information obtained, the registration/deposit systems in all Member States analysed establish (or help to establish, in the event of a legal dispute) a rebuttable presumption of authorship/ownership. One of the essential features of both the public and the private registration/deposit systems is to provide evidence of the date of registration/deposit (in digital systems it is the date on the electronic certificate). Most of the electronic registration/deposit systems use some cryptographic methods; the qualified certificate provided by the Benelux i-DEPOT and the timestamp issued by the private sector initiative studied are of particular interest. With one exception, all of the public registries/depositories studied keep a fixed copy of the content to which the application relates. The timestamp used by the private sector initiative may be applied independently of a deposit of a copy of the content. A significant point of divergence among the systems studied is the confidentiality of the content and other information registered/deposited. Some registration/deposit systems are entirely confidential. In these systems, different types of content (IP related or not) can be deposited, the procedure for submitting content is the same for all applications, and the institution or company administering the depository/registry does not carry out any specific checks on the content or the applicant. In a few systems, there is a publication and public search function; the elements that can be accessed vary. As to the private sector initiative, users may decide if and to what extent they wish information about themselves and about their work/deposit to be publicly accessible. All

registration/deposit systems studied charge some kind of fee. Based on the data provided, it appears that the private sector initiative, which offers advanced search functions and some content management features, receives by far the largest number of applications. All systems studied address both individuals and companies. There is little reference material on the number of court cases in which the registration/deposit has been used as evidence.

Overall, three options are presented for a Digital Deposit System at EU level. Two main types of system can be distinguished: a basic system and an advanced system. Within the basic system, two different options are suggested: in option 1, the EUIPO would not store the content submitted, but simply provide reliable electronic proof of the existence of the content at a given moment in time. Option 2 would offer, in addition, a deposit service: it would store the content uploaded by users. In option 1, the EUIPO would simply act as a timestamping/‘certifying’ authority, and in option 2 as a depository. The advanced system, or option 3, would go in the direction into which current electronic systems are being developed, and even slightly beyond so as to be at the forefront of development.

Certain features relating to the basic functioning and technology of the proposed system would apply to all the options proposed. In principle, the EU Digital Deposit System would be entirely electronic and highly confidential; evidence of the exact date of deposit of the content would be provided by the highly secure and accurate technology of timestamping; additional cryptographic methods would provide extra layers of trust; the deposit holder would receive an electronic certificate; the procedures and requirements for opening of a user account would be similar; and the EUIPO would not check the identity of users of the system or the content submitted.

The crucial difference between options 1 and 2 of the basic system lies in the storage of copies of the content certified. Storing a copy of the content at the EUIPO (option 2) would remove the risk that the deposit holder might fail to keep a secure and unaltered copy of the content deposited. It would avoid issues linked to the limited validity of the electronic certificate issued by the EUIPO. Moreover, it would also allow the deposit holder to authorise a court to access the content in the EU Digital Deposit System directly, which would enable easy content verification by courts as an alternative to more technically demanding verification through digital fingerprinting / timestamping.

The advanced system would build on option 2 of the basic system. It would have supplementary features that would bring added value in two respects: first, depositors would be able to manage their content and their accounts; and second, the Digital Deposit System would make certain information about the deposit and, if selected by the deposit holder, even the content itself available to the general public. The advanced system would include a public user interface with content publication and search functions. Internet users could search the EU Digital Deposit System for information submitted by account holders. In options 2 and 3, deposits could be renewed and the corresponding electronic certificate extended/re-signed. A decision on whether the EUIPO would charge a fee for the deposit (and possibly for renewal) will need to be taken. It is crucial that evidence provided by the EU Digital Deposit System be accepted in courts across the European Union. In the context of litigation, a court could thus request access to information

about a deposit or evidence of the date of deposit. In all three options proposed, the deposit holder would need to give consent for the court to receive the relevant evidence: in option 1 the deposit holder would submit the electronic certificate (with timestamp/digital fingerprint) to the court, which would then go through a technical verification process; in options 2 and 3, the deposit holder could also authorise the court to access the content in the EU Digital Deposit System directly (easy content verification).

The legal and technical feasibility of the proposed options were analysed by the different departments of the EUIPO, focusing on legal and technical aspects respectively⁴. Overall, the establishment of an EU Digital Deposit System was found to be feasible from both a legal and a technical perspective. However, some issues would have to be addressed before such a system could be established. Notably, there is currently no explicit legal basis for the EUIPO to set up an EU Digital Deposit System. A system at EU level would either require amendment by inclusion of (a) new provision(s) in existing relevant EU legislation⁵, or the adoption of new EU legislation; either a regulation with direct applicability in the Member States or a directive referring to a regulation. Previously, new powers related to orphan works were delegated to the EUIPO in Directive 2012/28/EU on certain permitted uses of orphan works by referring to Regulation (EU) No 386/2012. The EUIPO's new powers related to an out-of-commerce database are envisaged in a proposal for a Directive on copyright in the Digital Single Market, which also refers to Regulation (EU) No 386/2012.

It was also pointed out that the EU Digital Deposit System could only work on a voluntary basis, and that the EUIPO would only certify the date on which the content was submitted or uploaded. The certification would only apply to a date, and the submitted/deposited content or identity of the depositor would not be verified. The terms of use of the EU Digital Deposit System are crucial. They would notably specify what services will be provided; and include detailed terms of use; a disclaimer and limitations on the EUIPO's and the user's liability; information that the EUIPO does not accept liability for any content provided, as it will not be verified by the EUIPO; data protection issues; and modification, discontinuation or termination clauses. Moreover, the EU Digital Deposit System would have to be in line with standards and internal procedures applied by the EUIPO to ensure that it is secure and highly confidential.

The technical Feasibility Analysis concludes that the establishment and operation of an IT tool meeting the requirements of an EU Digital Deposit System is considered feasible without any restrictions. It is emphasised that in order for the certificates generated by the EU Digital Deposit System to be accepted as a trusted source of evidence, considerable investment in a

⁴ The International Cooperation and Legal Affairs Department (ICLAD) and the Digital Transformation Department (DTD).

⁵ Council Regulation (EC) No 207/2009 on the Community trade mark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trade mark, amended by Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 (EUTMR). Note that these texts were codified by Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark. Since the Feasibility Study was finalised in January 2017, the present text refers to the legal instruments in force at that time.

public key infrastructure (PKI) would be required. The deposit system alone might not justify establishing a ‘certification authority’ within the EUIPO that would operate a ‘fully fledged’ PKI, which would entail significant costs. The storage demand for metadata and certificates (including timestamps), as well as for other purely technical artefacts (such as indices), would not be significant. What would be of greater importance would be the permanent storage demand resulting from the uploaded multimedia content (options 2 and 3). Due to the limited lifecycle of a deposit, the functional complexity of the tool would be moderate. No feature was identified that by full analogy is not already supported in other tools operated and governed by the EUIPO. The technical risk is assessed as being low, provided the tool’s scope could be firmly established up front.

As for the expected impact, it must first be emphasised that setting up an EU Digital Deposit System with EU-wide effect administered by the EUIPO must be founded on a specific legal basis in EU legislation. The legal basis should contain provisions on the establishment, functioning and management of the system. In particular, the legal basis should specify that documentation from the EU Digital Deposit System will be accepted by courts in the EU Member States as sufficient evidence. Mutual recognition of evidence would require agreement from all Member States and obtaining evidence would be based on different national conditions and procedures. An EU Digital Deposit System, however, would provide a fast and easy solution, namely a one-stop system ensuring that evidence would be recognised at EU level with unified conditions and procedures.

Once established, an EU Digital Deposit System could address some of the challenges created by digital technologies. Notably, it could increase legal certainty concerning the ownership of content. The advanced system could also facilitate the exercise of rights in the digital environment. An EU Digital Deposit System could stimulate the legitimate use of content, and help rights holders to protect their rights in cases of infringement claims. For entrepreneurs and small businesses, the EU Digital Deposit System could be a simple and inexpensive way of preventing others from stealing their ideas and innovations. For example, information from the system could serve as a useful piece of evidence for companies wishing to keep their inventions secret, to protect ideas when they are still in the development stage or in the course of negotiations with potential business partners. It could be a significant first step in the innovation process, that is, in the preliminary phase of an application for a design or a patent. In addition, it might support the evidence of IP protection and ownership that platforms can request when they receive take-down notices. The advanced system would contain a public search function, as well as possible rights management features and would allow optional publication of deposited content. The EU Digital Deposit System could constitute an indispensable source of information relating to the identification of content, its author(s) and current rights holder(s).

1. INTRODUCTION

1.1. Background

As part of its Work Programme for 2016, the Observatory has carried out a Feasibility Analysis for establishing a Digital Deposit System⁶ at EU level.

The purpose of this initiative is to analyse the feasibility of developing a digital platform enabling authors, inventors, creators and individuals and businesses in general to keep evidence of the existence of their works or other information at a certain point in time through a central tool that operates in a secure and highly confidential⁷ manner, administered by a public authority.

If such a system were to be established, it would provide information that might help establish a presumption of ownership, depending on the rules and conditions stated in the respective national legislation in this context, and thus simplify proof in legal proceedings; further, depending on the system chosen, it might facilitate management of the content.

1.2. Methodology

The Feasibility Analysis of an EU Digital Deposit System involves a variety of technical and legal aspects. Therefore, a task force was created with representatives from the EUIPO's legal and information technology services participating in order to ensure alignment of the initiative with all relevant aspects.

The first stage of the Feasibility Analysis consisted of gathering information on existing national practices concerning voluntary registration and deposit systems.

As a preliminary step, the Observatory analysed the summary of responses to the World Intellectual Property Organization (WIPO) questionnaires for surveys on copyright registration and deposit systems⁸. For the phase of gathering up-to-date information on existing national

⁶ In the Work Programme 2016 the initiative is referred to as the 'Soleau' envelope digital system. The system of the French envelope Soleau was established by the French National Institute for Industrial property (INPI). It consists in a sealed envelope that serves as proof of the date of an invention, idea or creation of a work. However, a repository system administered by the EUIPO would not necessarily be identical to the envelope Soleau and could be open to the deposit of various types of content, either IP protected or not (e.g. content protected by copyright or constituting a trade secret). In addition, the system envisaged should offer the possibility of digital deposit, and would not entail the collection of physical copies. Therefore the system is called a 'digital deposit system'.

⁷ The system would be highly confidential. The content deposited, following the security classification policy of the EUIPO, would be kept at the 'secret' level ('confidential' would not be sufficient).

⁸ In 2005, the WIPO Secretariat carried out an extensive survey of national legislation on voluntary registration systems for copyright and related rights, based on a questionnaire that was sent to all Member States of WIPO. In 2010, the WIPO Secretariat prepared a second survey, which expanded the earlier survey and examined

deposit systems (including, but not limited to copyright deposit systems) as well as additional information that would be relevant for the feasibility study, a survey was drafted (see below, ANNEX II: QUESTIONNAIRE ON REGISTRATION/DEPOSIT SYSTEM(S))

).

The survey was distributed to selected Observatory stakeholders and focused on EU Member States where, according to the WIPO Surveys, there are examples of voluntary registration and deposit systems⁹ (digital or not)¹⁰. The main focus of the survey was the functioning of voluntary registration and deposit systems managed by public sector institutions. Systems managed by private entities were considered only when they were found to be examples of good practice, for example, widely used.

The respondents were asked to provide institutional and legal information about the registration/deposit system(s) in their Member State, in addition to information on the specific features of the respective system. The legal part focused on information concerning the legal basis for a registration/deposit, the legal effects and liability issues. The questions about the features of the national systems aimed to clarify the main requirements for filing the registration/deposit requests, additional features of the systems (such as a public search facility, restrictions on accessing the content, the possibility of transferring or licensing the content), as well as to gather statistical information about the use of the systems and the main characteristics of their users.

In addition, the EUIPO awarded a contract to the University of Oxford to carry out research on existing registration and deposit systems in selected third countries, namely, the USA and China. The results of the research, which are published separately, provide third-country information that adds to the EU-focused Feasibility Analysis.

registration and deposit systems. See the [WIPO Survey of National Legislation on Voluntary Registration Systems for Copyright and Related Rights](#) and the [WIPO Second Survey on Voluntary Registration and Deposit Systems](#).

⁹ The term 'registration/deposit' is applied throughout the text to cover both situations, whichever is applicable in a particular case.

¹⁰ The questionnaire was distributed to the following Member States: Belgium, Germany, Spain, France, Italy, Luxembourg, Hungary, the Netherlands, Austria, Portugal, Romania and the United Kingdom. Replies were provided by Belgium, Germany, Spain, Italy, Luxembourg (joint reply on behalf of Benelux), Hungary, the Netherlands, Portugal, Romania and the United Kingdom.

In 2018, that is, after the research on existing deposit and/or registration systems had been concluded, the EUIPO was informed that following a reform of the Greek Copyright Act (Law No 4481/2017 amending the second paragraph of Article 69(1) of Law No 2121/1993 on Copyright, Related Rights and Cultural Matters) the Hellenic Copyright Organisation now has a legal basis to, inter alia, provide timestamps. This means that it may provide services of dating works or other subject matter that may be protected by copyright and/or related rights.

2. SUMMARY ANALYSIS OF VOLUNTARY REGISTRATION AND DEPOSIT SYSTEMS IN SELECTED EU MEMBER STATES

On the basis of the information gathered in the survey¹¹, a detailed horizontal assessment of the functioning of the existing voluntary registration and deposit systems was prepared. The survey was carried out between 6 June and 27 July 2016. The detailed horizontal assessment is annexed to this document (ANNEX I: SUMMARY OF REPLIES TO QUESTIONNAIRE FOR SURVEY ON REGISTRATION/DEPOSIT SYSTEM(S))

). This section contains a summary of the information gathered.

Institutional information

In the scope of the survey, the following IP registration/deposit systems, managed by public authorities in EU Member States, were analysed:

- the i-DEPOT tool (Benelux)¹²;
- the *enveloppe Soleau* (France)¹³;
- the Voluntary Register of Works Protected by Copyright (Hungary)¹⁴;
- three public registers established in Italy: the General Public Register for Works Protected by Copyright¹⁵; the Cinematographic Public Register¹⁶; the Special Public Register for Computer Programs¹⁷ (Italy);
- the Register of Literary and Artistic Works (Portugal)¹⁸;
- the Register of Works Protected by Copyright (Romania)¹⁹;
- the General Intellectual Property Register (Spain)²⁰.

¹¹ Please note that the information provided about some Member States was more detailed than others.

¹² The register/deposit is managed by the Benelux Office for Intellectual Property (BOIP).

¹³ The register/deposit is managed by the French Intellectual Property Office (INPI).

¹⁴ The register is managed by the Hungarian Intellectual Property Office (HIPO).

¹⁵ The register is managed by the Italian Ministry of Cultural Heritage, Cultural Activities and Tourism.

¹⁶ The register is managed by the Italian Society of Authors and Publishers (SIAE);

¹⁷ The register is managed by the SIAE;

¹⁸ The register is managed by the Portuguese General Inspection for Cultural Activities (IGAC).

¹⁹ The register is managed by the Romanian Copyright Office (ORDA). ORDA administers six National registers: i) the National registry for phonograms; ii) the National registry for videograms; iii) the National registry for computer programs; iv) the National registry for multipliers of CDs, audio and videocassettes; v) the National registry for private copies; vi) the National registry for works.

A private initiative was examined in this context as an example of good practice, that is, the system was considered to be widely used.

IP registration/deposit systems managed by collective management organisations were outside the scope of the survey, as they serve a different purpose (to enable rights holders to enter their works on the records of collective management organisations).

Legal information

Each publicly administered IP registration/deposit system of the selected Member States has a legal basis in national law, often in national IP acts or copyright acts.

Regarding the content that can be registered/deposited, two categories of systems could be observed: i) the system offers the possibility of registering/depositing any type of content (IP related or not); no information on the content is supplied by the user (i-DEPOT tool, French *enveloppe Soleau*); ii) the system is mainly designed to register/deposit content protected by copyright and related rights; the information on the type of content is supplied by the user (registers in Spain, Italy, Hungary, Portugal, Romania and the private sector initiative).

In some Member States the registration/deposit process is simple and straightforward, that is, the same procedure applies to various types of content and no formality examination is carried out²¹. In other cases, the registration/deposit process is more complex; for example, different procedures can apply depending on the type of content, or if a formality check takes place²².

According to the information gathered, the registration/deposit systems in all analysed Member States establish (or help to establish, in the case of a legal dispute) a rebuttable presumption of authorship/ownership.

One of the essential features of the registration/deposit systems is to provide evidence of the date of registration/deposit (in the paper version it is the date stamped on the envelope or certificate; in the digital version it is the date that appears on the electronic certificate). The private sector initiative provides evidence of the date through timestamping technology.

Other benefits of the registration/deposit system(s) include the following: application in numerous IP-related fields (i-DEPOT), facilitation of access to state funds for culture-related activities (registries in Spain²³ and Italy), use for mortgage purposes (Spain²⁴) or facilitating

²⁰ The register comprises the Central Intellectual Property Register, managed by the Spanish Ministry of Education, Culture and Sport, and the regional Intellectual Property Registers, which are managed by the regional governments of Spain and the autonomous cities of Ceuta and Melilla.

²¹ This is the case for the i-DEPOT tool, the French *enveloppe Soleau*, the register in Hungary, and for the private sector initiative.

²² More complex procedures were reported for registers in Italy, Spain, Portugal and Romania.

²³ It is a requirement in Italy and Spain to enter the works protected by copyright (such as cinematographic works in Italy) in the register, to be able to benefit from access to State funds for culture-related activities.

²⁴ The mortgage legislation in Spain requires registering in the General Intellectual Property Register rights in protected works that are intended to be mortgaged.

licensing of content (the private sector initiative).

No particular liability issues linked with the administration of the systems were identified in the survey. Unauthorised disclosure of information to third parties does not seem to be a matter of concern in practice. In relation to disclosure of deposited elements to third parties, some analysed systems are confidential (i-DEPOT), whereas others are open (to a certain extent) to the public for consultation²⁵.

In cases of dispute between a user of the system and a third party (e.g. about the date on the evidence), the authority running the registration/deposit system does not have any specific role. No specific mediation or arbitration procedure is envisaged in any of the public and private systems analysed. The responsibility of the registration/deposit authority is to deliver, upon request of the rights holder, the document that may serve as evidence of the date.

Features of the national systems

There are electronic registration/deposit systems in Benelux (i-DEPOT), Spain, Portugal and Romania. In France, an electronic version of the system was launched on 15 December 2016²⁶. The private sector initiative offers a fully electronic registration/deposit system. Most of these systems use some cryptographic methods; the qualified certificate provided by i-DEPOT and the timestamp issued by the private sector initiative²⁷ are worthy of note. The systems studied vary regarding user identity checks: while some systems merely require the creation of an account and a password (e.g. i-DEPOT and the private sector initiative), others require a digital certificate confirming identity (Spain).

The requirements for filing a request for registration/deposit mainly vary in their degree of specification. Usually, some information about the applicant is required (notably contact details). In addition, the registration/deposit may require, for example, some information about the type of work/content/rights deposited or registered, proof of payment of the fee, or more specific information on the work/content deposited. In some of the systems, the requirements are different for different types of works.

In some registration/deposit systems, there is at least a formal check of the elements submitted. In the case of i-DEPOT (which is confidential) and of the private sector initiative, the applications are not examined, and the filing process is automatic. With the exception of Hungary, all the public registries/deposits studied keep a fixed copy of the content to which the application relates. The timestamp used by the private sector initiative may be applied independently of a **deposit** of a copy of the content (i.e. there is an option to have the content

²⁵ For example, in Spain any person may request disclosure of registered entries without restrictions. However, apart from the IP rights holders, only third parties that are able to demonstrate a legitimate interest are permitted to consult the documents in the archived files. Access to the content of the files, including identifying the copy of the work, is not permitted.

²⁶ http://www.ieepi.org/linpi-lance-lenveloppe-soleau-electronique-e-soleau/?utm_source=lettre-pi.

²⁷ These serve as evidence and allow the existence of the content at a certain point in time to be proven independent of the registry, for example, before a court.

stamped and sent back to the applicant). Five of the systems studied support collections, and four support the registration/deposit of different versions.

A significant point of divergence is the confidentiality of the elements or rights registered/deposited. Some registration/deposit systems are confidential (Benelux, France, Portugal); registration/deposit systems can also have an administrative public information purpose (Italy). In some systems, while the content of the deposit or certain personal data may not be publicly accessible, some bibliographic elements are. In a few systems, there is a publication and public search function; the elements that can be accessed vary. As for the private sector initiative, users may decide if and to what extent they wish information about themselves and about their work/deposit to be publicly accessible.

In several of the systems studied, a registration/deposit may be revoked. Renewal of the registration/deposit is possible in some systems; several replies point out that renewal is not necessary in terms of evidential value. The second compartment of the French *enveloppe Soleau* is kept by the French INPI for a period of 5 years, renewable once. Four registration/deposit systems offer the possibility of recording transfers of rights in a work/in the content deposited. The private sector initiative also has a contract management feature, including the possibility of licensing the content deposited through the system.

All the registration/deposit systems studied charge some kind of fee. The fee is due either for registration/deposit or for producing evidence. Fees vary between EUR 10 and 100.

Use of the national systems

Data on the number of users were provided regarding different time periods. A direct comparison is therefore difficult. Based on the data provided, it appears that the private sector initiative analysed receives by far the largest number of applications.

Statistics on the number of requests for information received per year are not available for all of the systems studied. In the systems that provided data, there are between approximately 877 and 2 000 requests for information during the 1-year period²⁸.

In all of the registration/deposit systems studied (where statistics are available), the users are mainly nationals of the respective Member States. However, notably the i-DEPOT and the private sector initiative also receive applications from international users based within and outside the EU. All systems studied deal with both individuals and companies. There is very little reference material on the number of court cases in which a registration/deposit has been used as evidence.

²⁸ The private sector initiative approximately 575 000 (2007-2016); RO approximately 230 000 (time period unknown); ES approximately 104 000 (2012-2014).

3. STRUCTURE OF THE DIGITAL DEPOSIT SYSTEM FOR THE FEASIBILITY ANALYSIS

The Feasibility Analysis will cover the respective features of two different main systems: a basic system that would be managed automatically (basic system), and a more complex, advanced system with additional features, also largely automatic (advanced system).

Two options are suggested for the basic system: in option 1, the EUIPO would not store the content submitted, but simply provide reliable electronic proof of the existence of the content at a given moment in time. Option 2 would offer, in addition to this, a deposit service, that is, the EUIPO would store the content deposited by users of the basic system. In option 1, the EUIPO would simply act as a timestamping/certifying authority, and in option 2 as a depository.

The advanced system suggested (option 3) would go in the direction into which current electronic systems are being developed (see the BOIP's i-Depot) and even goes slightly beyond so as to be at the forefront of the development. The features of the different options are described below.

While the options are presented as alternatives, the basic system in option 2 could also be considered as a first step, while the advanced system could be implemented later on, also depending on the success of the basic system and user demand²⁹.

The features of the different options were selected after studying the features of the different public sector registration and deposit systems covered by the survey as well as those of a private sector system. Certain features relating to the basic functioning and technology of the system envisioned would apply to all the proposed options. The crucial difference between options 1 and 2 of the basic system lies in the storage of copies of the timestamped/certified content. Option 3 would build on option 2 of the basic system, and have additional features that would notably allow for management/organisation of the content deposited, and public accessibility of certain elements relating to that content or even the content itself.

3.1 Basic system

Two options are proposed for the basic system: in the first alternative, the EUIPO would provide electronic proof of the date of submission of the content, that is, of the existence of the content at a given point in time. However, no copy of the content itself would be stored at the EUIPO.

²⁹ Note that the advanced system would in any event entail deposit of the content submitted. That is, it would be based on option 2 of the basic system.

Option 1 would not amount to a Digital Deposit System, since users would be responsible for storing the documents that they submitted to the EUIPO, which would not be kept by the EUIPO. The EUIPO would store the digital fingerprint generated at the moment of upload of the content. In the second option the EUIPO would, in addition to providing timestamps and certificates, store a copy of the content submitted in its digital deposit. This copy could be retrieved by holders of such digital deposits.

3.1.1 Option 1: no deposit of the content

3.1.1.1 *An electronic timestamping/certification system*

The basic system analysed for feasibility would be entirely electronic. Evidence of the exact moment of submission of the content would be provided by timestamping (of a copy of the content submitted³⁰) and by issuing a certificate of submission of the content. The latter would include all the compulsory information provided by users of option 1 of the basic system (users), would confirm the information and exactly when the content was submitted to the EUIPO; the certificate would be created automatically, and sent to the user by email to the email address the user specified as a contact email when the user account was opened. In order to ensure that the methods used guarantee the highest safety and accuracy possible, they would have to be in compliance with the conditions set by EU law on electronic signature, identification and trust services³¹.

3.1.1.2 *Opening a user account*

In order to have content timestamped and to receive a certificate, users would need to open an account on the EUIPO website: they would have to provide a name, family name, a valid email address, a postal address and a telephone number (and details of the payment method if a fee were to be charged). While there would be captcha control (to ensure that a physical person opens the account), the EUIPO would not check the identity of users, and the process would be entirely automatic. The EUIPO would assign a user ID number to each user once he or she has opened an account (account holders). Account holders could be natural or legal persons. Opening an account would require the creation of a password, sent to the user's email address³².

3.1.1.3 *Submitting content for timestamping and 'certification'*

Account holders, once logged in, could submit content for timestamping and 'certification'.

³⁰ In the course of uploading the content, the evidence would be generated by computing a unique fingerprint for the content uploaded, attaching a timestamp to the fingerprint and sealing the fingerprint together with the timestamp by cryptographic means.

³¹ [Regulation \(EU\) No 910/2014](#) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing [Directive 1999/93/EC](#), OJ L 257, 28.8.2014, pp. 73-114.

³² A temporary code will be sent to the email address provided by the user. This way the system ensures that the email address exists.

Different types of content (IP related or not, such as trade secrets) could be submitted. The content submitted to the EUIPO would not be kept by the EUIPO³³. In the electronic form, the user would be asked to indicate the title of the submission (e.g. the name of the work) (mandatory field), and have the possibility of also providing a description of the content (non-mandatory free text field). The submission form would also contain a mandatory field with a drop-down list (or tick boxes) in which the user would indicate the type of content that is being submitted³⁴. A copy of the content to be timestamped/'certified' would be provided using the download function. The copy would later be returned to the user.

3.1.1.4 The role of the EUIPO in option 1

The information submitted would not be examined by the EUIPO. An information helpdesk would provide technical support for users of the system; however, the staff of the EUIPO would not have access to the content submitted.

The EUIPO would apply a timestamp and a unique digital fingerprint to the copy of the content submitted by the user; the copy would then be encrypted. The certificate, issued automatically, would contain (next to the above-mentioned information about the content) the cryptographic detail necessary to reverse the encryption. The EUIPO would return the timestamped/certified copy of the content to the user, together with the certificate. The entire process would be automatic, and the EUIPO would not store any copy of the submitted content. The EUIPO would, however, in this case store the digital fingerprint generated at the moment of upload of the content.³⁵ The (technical) validity of a certificate would expire after approximately five years. Since no copy of the content itself would be kept, the EUIPO would not be in a position to extend the validity of a certificate. Users would be required to submit the content for 'recertification', which would entail a different (later) date on the timestamp. Extension of the validity of the certificate is only possible in options 2 and 3, in connection with the renewal of the deposit. The EUIPO would also keep an automatic record of the facts of the deposit (dates, etc.), and of the information or metadata provided by the user.

In order to serve as evidence, the original certified document and the certificate would have to be presented to the court. The user would be responsible for keeping the original documents unaltered and for not losing them. Under option 1, the EUIPO could grant a court access to the certificate stored, when the user consents to this.

In addition, an online cryptographic verification tool is envisaged: it would allow the account holder or courts (on the role of the EUIPO vis-à-vis courts see below) or other third parties to check the identity of contents on the basis of the digital fingerprint and the certificate, with the

³³ EUIPO non-liability regarding the content submitted would be defined in the terms of use. The user would need to agree to these terms. The user would be informed that the content is not stored by the EUIPO and it is a responsibility of the user to keep an original copy of the content unaltered and for not losing the content.

³⁴ The list would contain the category 'other', also in case the user does not wish to submit information about the type of content.

³⁵ Note that if the fingerprints were damaged or lost for some reason or expired, it could not be recreated when the content is not stored.

consent of the account holder.

For statistical reasons, the EUIPO collected the following basic information related to submissions made by users: type of content (as indicated by the user), country of user.

3.1.2 Option 2: deposit of the content

The crucial difference between options 1 and 2 of the basic system lies in the storage of copies of the content certified. Storing a copy of the content at the EUIPO (option 2) would remove the risk that the deposit holder might fail to keep a secure and unaltered copy of the exact version of the content originally deposited³⁶. It would consequently provide greater assurance that the ultimate aim of facilitating submission of evidence has been fulfilled. Moreover, the electronic certificate issued in option 1 has limited validity. As computing power and cryptographic methods develop, certificates become insecure (cryptographic code might be broken). Time periods for this can vary, but are generally estimated at five years. If, in line with option 1, no content is stored by the EUIPO, the quality of the certificate to act as evidence once it has become insecure will be compromised. The deposit holder could submit the content again, but would receive a different date/timestamp. However, the EUIPO could extend/re-sign the certificate if the content itself were stored (option 2). Finally, if the EUIPO were to store the content (option 2), this would also allow the deposit holder to authorise a court in a specific case to directly access the content in the EU Digital Deposit System, which provides a means of evidence easily accessible by courts as an alternative to more technically demanding content verification through digital fingerprinting/timestamping.

3.1.2.1 Common characteristics of the two options of the basic system

Option 2 of the basic system would share the basic characteristics of option 1 (described in above, at 3.1.1.1, 3.1.1.2): the system would be entirely electronic and highly confidential (except for authorised court access); evidence of the exact date of deposit of the content would be provided by the same technical process used in option 1; the procedures and requirements for opening of a user account would be the same; and the EUIPO would not check the identity of users of the system or the content submitted. Online cryptographic verification tool would also be available.

Nevertheless, instead of directly sending the timestamped content and the certificate back to the users of the system, the EUIPO would store a copy of the content in option 2. Option 2 would therefore consist in a Digital Deposit System. The advantages of option 2 over option 1 are described above.

3.1.2.2 Making a deposit in the Digital Deposit System

Account holders, once logged in to their account, could file one deposit, several deposits or

³⁶ All digital deposit systems analysed in the survey, except for Hungary, store a copy of the content.

different versions of a deposit using a feature available in the user account (holders of a deposit within an account are referred to as 'deposit holders'). As in option 1, different types of content (IP related or not, such as trade secrets) could be deposited. The content deposited with the EUIPO would remain secret³⁷. The EUIPO would assign a permanent identifier to each deposit and a variation of that identifier to each version of the same deposit. In the electronic deposit form, the deposit holder would be asked to indicate the title of the deposit (e.g. the name of the work) (mandatory field) and would also have the possibility of providing a description of the deposited content (non-mandatory free text field). The deposit form would also contain a mandatory field with a drop-down list (or tick boxes) in which the deposit holder would indicate the type of content being deposited. A copy of the content would be provided using the download function.

3.1.2.3 The role of the EUIPO during the lifespan of a deposit

As in option 1, the information submitted would not be examined by the EUIPO. An information helpdesk would provide technical support for users of the EU Digital Deposit System; however, the staff of the EUIPO would not have access to the content deposited.

The EUIPO would store an original fixed copy of the deposited content, and the deposit holder would have the possibility of retrieving a copy of the content deposited, together with the certificate, for example, when the deposit holder wishes to use it as evidence in court. If the deposit holder wishes to withdraw the content, that is, to remove it from the system, the deposit holder will be able to do so. Although the content would no longer be kept by the EUIPO, it would keep an automatic record of the facts of the deposit (dates, etc.).

The term of validity of the deposit would be limited, for example, to five years³⁸. The main objective of limiting the term of validity is to prevent the system from being overloaded with deposits that are no longer of interest to their owners. In addition, the technical validity of the certificate expires after approximately five years. (Unlimited) renewals for additional periods of five years would be possible, for instance. In the context of renewing the deposit, the (technical) validity of the certificate would also be extended. The procedure for renewal would be as follows: the EUIPO would send an automatic reminder to deposit holders, for example six and again three months before the end of the five-year term. Deposit holders would have to confirm that they wish to keep the deposit by checking the respective box in their account. Reminders would be sent by email only. The EUIPO would implement a 'cleaning policy', with a view to deleting deposits whose holder can be considered no longer to have an interest in maintaining the deposit. The cleaning policy would allow the EUIPO to remove the deposit and the contents of the latter, for example, one year after the term of the deposit has expired (i.e. in the case of non-renewal of the deposit by the holder). The EUIPO would, however, keep an automatic record of the facts of the deposit (dates, etc.), including the date of its expiry. In cases of

³⁷ EUIPO non-liability regarding the content deposited would be defined in the terms of use. The user would need to agree to these terms.

³⁸ National systems such as the French e-Soleau or the Benelux i-Depot offer initial protection terms of five years (the i-Depot also offers an initial term of ten years).

renewals, the (technical) validity of the electronic certificate would have to be ensured by extending or re-signing the certificate.

Deposit holders would thus have the possibility of renewing, retrieving and withdrawing their deposits. To that end, there would be a checkbox in the user account to confirm the renewal of a deposit, and a checkbox to request the withdrawal of the content deposited. The deposit holder would have to confirm that the EUIPO should renew the deposit by checking the box.

For statistical reasons, the EUIPO would collect the following information related to the deposit: type of content (as indicated by the depositor), country of deposit holder, number of deposits opened/renewed/withdrawn/expired.

A decision on whether the EUIPO would charge a fee for the deposit (and possibly for renewal) would need to be taken. All systems studied in the survey charge a fee (either for deposit or for retrieval of the content, see Annex I below). The possibility of charging a fee without an explicit legal basis for the Digital Deposit System is analysed in Chapter 5, section 4.4 of this document.

A deposit system (option 2) would entail higher costs compared with a system that merely 'certifies' copies of content submitted (option 1).

3.1.2.4 Provision of information in the context of court proceedings

The main objective of the Digital Deposit System is to enable authors, inventors, creators and businesses in general to upload their works and other information to a central repository in a secure and highly confidential manner in order to keep evidence of the date of submission of a deposit. The technologies used should therefore provide evidence of the date of deposit of the contents deposited. This evidence would have to be accepted in courts throughout the European Union. In the context of litigation, a court could thus request access to information about a deposit or evidence of the date of deposit (i.e. the certificate of the deposit), and/or to the deposit itself. In all options, the deposit holder could provide the court with the electronic certificate issued by the EUIPO. The court could then go through cryptographic verification either by using a third party or the online tool provided by the EUIPO (cryptographic verification tool). As the content is stored by the EUIPO, the deposit holder could authorise the court in a specific case to have direct access to the content in the EU Digital Deposit System (an easy alternative to the cryptographic content verification). At the request of the deposit holder, the EUIPO would then provide the court with a hyperlink to the deposit, which would be valid temporarily and password protected.

3.2 Advanced Digital Deposit System

3.2.1 The principles of the basic system combined with additional features

The main technical features of the basic system, including the storage/deposit function of

option 2, would also be present in the advanced system³⁹. The advanced system would have two main supplementary features: first, deposit holders would be able to manage their content and accounts; and second, the Digital Deposit System would provide the possibility to make certain information about the deposit and, if selected by the deposit holder, even the content itself available to the general public.

3.2.2 Management of the content deposited (transfer of the deposit)

In relation to content management, account holders would have the possibility of transferring their deposit(s) (i.e. the ownership of a deposit) to another account holder. To this end, both parties would have to have an account in the Digital Deposit System, and account holder B would have to accept the transfer from account holder A. Transfer of the deposit could serve as additional means of proving that rights in the content deposited were transferred from account holder A to account holder B. The transfer of a deposit would not create a valid transfer of the rights in the content, but would serve as additional evidence.

Considering the complexity of IP transfers and the absence of a harmonised legal framework for certain IP rights, IP contracts and general contract law, the EUIPO would need to draw Digital Deposit System users' attention to the fact that a specific contract is necessary for the transfer of rights in the content, and that they should consult a lawyer. For the same reasons, a more complex rights management tool is not considered for the Digital Deposit System for the time being. In cases of transfers, the account holder receiving the deposit should have the possibility of changing the confidentiality settings. After a transfer of deposit ownership, the initial account holder would no longer be able to access, change or delete the deposit. The advanced system would contain additional features for transfers (and acceptance of transfers) of deposits as described above.

3.2.3 Public access to information about deposits (and possibly to their content)

The advanced system would include a public user interface with content publication and search functions. If so chosen by the deposit holder, internet users would be able to search the Digital Deposit System for the information submitted by a deposit holder: title of the deposit, type of content, name of the deposit holder, country of deposit holder or language. If the deposit holder were to submit further information in the form of a description of the content, the description could be searched for by the words contained in it (full text search of descriptions: e.g. introducing the word 'vase' would retrieve information about all deposits with a description containing the word 'vase'). The deposit holder would, in addition, choose to make the content

³⁹ Electronic system, timestamp and electronic certificate, opening of a user account, making deposits, confidentiality secrecy of the deposit(s), storage of a copy of the content deposited, possibility of retrieval, no user identity verification by EUIPO, no examination of information and content submitted, decision on deposit fee pending, renewal of the deposit and extension of the validity of the certificate, withdrawal of the deposit, support of versions, availability of an online cryptographic verification tool.

itself publicly available.

Having public user search functionalities would necessitate a slightly different approach to confidentiality settings. Account holders would have the choice between three options: (1) the deposit and the content deposited is completely secret (including for the EUIPO); (2) certain information about the content deposited is publicly available (see paragraph above); or (3) certain information about the deposit **and the content** of the deposit is publicly available. The third alternative would require further decisions on features that would allow the content deposited to be displayed to the public of (e.g. watching a movie or listening to a song on the Digital Deposit System platform). The advanced system would have a feature that allows the account/deposit holder to select and change the confidentiality settings.

In this context, the initiatives aiming to facilitate automated communications between creators/rights holders and those who wish to use the content legally could be further explored⁴⁰.

3.2.4 Implications for the EUIPO

3.2.4.1 The role of the EUIPO during the lifespan of a deposit

As in options 1 and 2, the information submitted would not be examined by the EUIPO. The advanced system would be fully automatic. An information helpdesk would provide technical support for users of the Digital Deposit System; however, staff of the EUIPO would not have access to the content deposited.

As in option 2, there would be a specific policy established by the EUIPO on content removal (in cases of non-renewal of deposits).

3.2.4.2 Provision of information in the context of court proceedings

The technologies used in both the basic and the advanced systems should provide evidence of the contents deposited. This evidence would have to be accepted in courts throughout the European Union. The content verification possibility for option 2 of the basic system, namely, the court using the cryptographic verification, having received the electronic certificate from the deposit holder, or, as an easy alternative, the deposit holder authorising the court to have direct access to the content in the Digital Deposit System (hyperlink sent to the court by the EUIPO at the request of the deposit holder).

⁴⁰ There are various initiatives in the market that aim to enable greater legitimate use of digital content through better management of data relating to rights across the network.

3.3 Overview of the characteristics of the basic and the advanced options of the Digital Deposit System

The following table provides an overview of the main characteristics of the basic and advanced options of the Digital Deposit System:

	BASIC SYSTEM		ADVANCED DIGITAL DEPOSIT SYSTEM
	OPTION 1 (NO DEPOSIT)	OPTION 2 (DEPOSIT)	OPTION 3
Purpose of the system	<p>To enable authors, inventors, creators and businesses in general to prove the existence of works or other information at a certain point in time through a central tool that operates in a secure and highly confidential manner, administered by a public authority.</p> <p>Simplification of proof in legal proceedings.</p>	<p>To enable authors, inventors, creators and businesses in general to upload their works and other information to a central repository in a secure and highly confidential manner so as to keep evidence of the existence of the work or other information at a certain point in time.</p> <p>Simplification of proof in legal proceedings.</p>	<p>To enable authors, inventors, creators and businesses in general to upload their works and other information to a central repository in a secure and highly confidential manner so as to keep evidence of the existence of the work or other information at a certain point in time.</p> <p>Simplification of proof in legal proceedings.</p> <p>Public information and publicity purposes.</p> <p>Management of content deposited.</p>
Electronic system	Yes	Yes	Yes
Main cryptographic methods used	<p>Timestamping (in the course of uploading the content, a unique fingerprint for the artefact uploaded would be generated, attaching a timestamp to the fingerprint and sealing the fingerprint together with the timestamp by cryptographic means).</p>	<p>Timestamping (in the course of uploading the content, a unique fingerprint for the artefact uploaded would be generated, attaching a timestamp to the fingerprint and sealing the fingerprint together with the timestamp by cryptographic means).</p>	<p>Timestamping (in the course of uploading the content, a unique fingerprint for the artefact uploaded would be generated, attaching a timestamp to the fingerprint and sealing the fingerprint together with the timestamp by cryptographic means).</p>

FEASIBILITY ANALYSIS
FOR AN EU DIGITAL DEPOSIT SYSTEM



	<p>and</p> <p>Delivery of a certificate containing a timestamp, created automatically and sent to the depositor.</p> <p>Methods used to be in compliance with the conditions set by EU law for electronic signature, identification and trust services 41.</p>	<p>and</p> <p>Delivery of a certificate containing a timestamp, created automatically and sent to the depositor.</p> <p>Methods used to be in compliance with the conditions set by EU law for electronic signature, identification and trust services.</p>	<p>and</p> <p>Delivery of a certificate containing a timestamp, created automatically and sent to the depositor.</p> <p>Methods used to be in compliance with the conditions set by EU law for electronic signature, identification and trust services.</p>
Storage of an original fixed copy of the deposited content by the EUIPO	<p>No</p> <p>The digital fingerprint would be stored.</p>	<p>Yes</p>	<p>Yes</p>
Retrieval of content deposited by deposit holders	<p>n/a</p> <p>The content would need to be stored by the deposit holder.</p>	<p>Yes, by deposit holder (together with the certificate).</p>	<p>Yes, by deposit holder (together with the certificate).</p>
User identity verification by the EUIPO	<p>No identity verification</p> <p>Creation of a user account would require certain user data: name, family name, valid email address, postal address and telephone number, possibly details about payment method.</p> <p>Captcha control</p>	<p>No identity verification</p> <p>Creation of a user account would require certain user data: name, family name, valid email address, postal address and telephone number, possibly details about payment method.</p> <p>Captcha control</p>	<p>No identity verification</p> <p>Creation of a user account would require certain user data: name, family name, valid email address, postal address and telephone number, possibly details about payment method.</p> <p>Captcha control</p>

⁴¹ [Regulation \(EU\) No 910/2014/EU](#) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing [Directive 1999/93/EC](#), OJ L 257, 28.8.2014, pp. 73-114.

FEASIBILITY ANALYSIS
FOR AN EU DIGITAL DEPOSIT SYSTEM



	<p>Temporary code to be sent to the email address provided by the user. This way the system would ensure that the email address exists.</p>	<p>Temporary code to be sent to the email address provided by the user. This way the system would ensure that the email address exists.</p>	<p>Temporary code to be sent to the email address provided by the user. This way the system would ensure that the email address exists.</p>
<p>Main information fields and actions required when opening an account and filing deposits</p>	<ul style="list-style-type: none"> Information about account holder (see user identity verification above) to be uploaded automatically by the system User ID number to be assigned to account holders (mandatory) Title of the submission (mandatory) Description field for additional information on content submitted (optional) Information field with drop-down menu (or tick boxes) to indicate the type of content (mandatory) <p>Download function to provide a copy of the content (that would be sent back to the user).</p>	<ul style="list-style-type: none"> Information about account holder (see user identity verification above) to be uploaded automatically by the system User ID number to be assigned to account holders (mandatory) Permanent identifier to be assigned to each deposit by the EUIPO; a variation of that identifier to be assigned to each version of the same deposit (mandatory) Title of the deposit (mandatory) Description field for additional information on deposit (optional) Information field with drop-down menu (or tick boxes) to indicate the type of content deposited (mandatory) <p>Download function to provide a copy of the content.</p>	<ul style="list-style-type: none"> Information about account holder (see user identity verification above) to be uploaded automatically by the system User ID number to be assigned to account holders (mandatory) Permanent identifier to be assigned to each deposit by the EUIPO; a variation of that identifier to be assigned to each version of the same deposit (mandatory) Title of the deposit (mandatory) Description field for additional information on deposit (optional) Information field with drop-down menu (or tick boxes) to indicate the type of content deposited (mandatory) <p>Download function to provide a copy of the content.</p>
<p>Other main features in the user account</p>	<p>Box for agreement to terms of Use (declaring, inter alia, the EUIPO's non-liability for the content submitted) (mandatory, checking of box mandatory).</p>	<ul style="list-style-type: none"> Box for agreement to terms of Use (declaring, inter alia, the EUIPO's non-liability for content deposited) (mandatory, checking of box mandatory) Box to confirm the renewal of a deposit <p>Box to confirm the withdrawal of a deposit.</p>	<ul style="list-style-type: none"> Box for agreement to terms of Use (declaring, inter alia, the EUIPO's non-liability for content deposited) (mandatory, checking of box mandatory) Box to confirm the renewal of a deposit Box to confirm the withdrawal of a deposit. Feature (box or otherwise) that would allow ownership of the deposit to be transferred from one account holder to another account holder, and for the latter to accept the transfer.

FEASIBILITY ANALYSIS
FOR AN EU DIGITAL DEPOSIT SYSTEM



			Feature (box or otherwise) that would allow selection of confidentiality settings related to making information or information and content of a deposit available to the public in the Digital Deposit System.
Examination of information submitted by the EUIPO	No	No	No
EUIPO intervention (entailing human intervention)	Helpdesk for users of the system (without access to content submitted)	Helpdesk for users of the system (without access to content deposited)	Helpdesk for users of the system (without access to content deposited)
Possible deposit holder actions in relation to the content deposited	n/a	<ul style="list-style-type: none"> Retrieval of content (see above) <p>Deposit of different versions of the content (previous versions to be kept by the EUIPO, possibility of retrieval of previous versions).</p>	<ul style="list-style-type: none"> Retrieval of content (see above) Deposit of different versions of the content (previous versions to be kept by the EUIPO, possibility of retrieval of previous versions) Transfers of the ownership of deposit from one account holder to another Publication of information on deposit <p>Publication of information on deposit and content itself.</p>
Content publication and public search function	No	No	<p>Yes (public user interface)</p> <p>Publication depends on choice of deposit holder, who could choose for no information to be published, for information on deposit to be published or for information on deposit and content itself to be published (e.g. title of deposit, type of content, holder of deposit, country, language).</p>

FEASIBILITY ANALYSIS
FOR AN EU DIGITAL DEPOSIT SYSTEM



Access restrictions	Yes	Yes Only the deposit holder would be allowed to access the content deposited. (No third-party inspection of files)	Yes In principle, only the deposit holder would be allowed access to content deposited (unless the deposit holder were to agree to make information and/or content deposited publicly available).
Court access	The deposit holder provides the court with the electronic certificate issued by the EUIPO (containing a digital fingerprint). The court could then go through cryptographic verification either by using a third party or the online tool provided by the EUIPO (cryptographic verification tool).	The deposit holder provides the court with the electronic certificate issued by the EUIPO (containing a digital fingerprint) for the court to use cryptographic verification (see option 1). In addition, the deposit holder could authorise the court in a specific case to have direct access to the content in the Digital Deposit System (an easy alternative to cryptographic content verification). At the request of the deposit holder, the EUIPO would then provide the court with a hyperlink to the deposit, which would be valid temporarily and password protected.	The deposit holder provides the court with the electronic certificate issued by the EUIPO (containing a digital fingerprint) for the court to use cryptographic verification (see option 1). In addition, the deposit holder could authorise the court in a specific case to have direct access to the content in the Digital Deposit System (an easy alternative to cryptographic content verification). At the request of the deposit holder, the EUIPO would then provide the court with a hyperlink to the deposit, which would be valid temporarily and password protected.
Online cryptographic verification tool	Online cryptographic verification tool allowing deposit holders/courts or other third parties (if the deposit holder consents) to compare contents or fingerprints with the help of the certificate (see Chapter 5 on technical feasibility)	Online cryptographic verification tool allowing deposit holders/courts or other third parties (if the deposit holder consents) to compare contents or fingerprints with the help of the certificate (see Chapter 5 on technical feasibility).	Online cryptographic verification tool allowing deposit holders/courts or other third parties (if the deposit holder consents) to compare contents or fingerprints with the help of the certificate (see Chapter 5 on technical feasibility)
Secrecy	Yes, total Information about deposit kept secret (including for the EUIPO).	Yes, total Content deposited completely secret (including for the EUIPO).	Three possibilities for the deposit holder to choose from: 1) content deposited completely secret (including for the EUIPO)

FEASIBILITY ANALYSIS
FOR AN EU DIGITAL DEPOSIT SYSTEM



	For statistical reasons, the EUIPO would collect information related to the deposit (see above: type of content, country, number of deposits submitted/renewed/revoked).	For statistical reasons, the EUIPO would collect information related to the deposit (see above: type of content, country, number of deposits submitted/renewed/revoked).	<p>2) certain information about content deposited is publicly available (see above, public search function)</p> <p>3) certain information about deposit and content itself is publicly available (publication function).</p> <p>In cases of transfers: the new deposit holder would have to have the possibility of changing the confidentiality settings.</p> <p>For statistical reasons, the EUIPO would collect information related to the deposit (e.g. type of content, country, number of deposits filed/renewed/revoked, number of confidential/partially accessible/public deposits).</p>
Deposit fee	To be decided	To be decided	To be decided
Term of validity of the certificate	Five years	Five years	Five years
Extension of validity of the certificate	Not possible (content not stored)	Extension/re-signing possible with the renewal of the deposit after five years (see below).	Extension/re-signing possible with the renewal of the deposit after five years (see below).
Renewal of the deposit	n/a	<p>Yes</p> <p>Term of validity of the deposit to be limited (e.g. five years).</p> <p>(Unlimited) renewals for additional terms of five years possible.</p>	<p>Yes</p> <p>Term of validity of the deposit to be limited (e.g. five years).</p> <p>(Unlimited) renewals for additional terms of five years possible.</p>

FEASIBILITY ANALYSIS
FOR AN EU DIGITAL DEPOSIT SYSTEM



		<p>(Technical) validity of electronic certificate to be ensured (extension/re-signing, see above).</p> <p>Reminder to be sent to deposit holders six and three months before expiry of the term (by email).</p> <p>Account/deposit holder to confirm that the EUIPO should keep the deposit (see above, box to be checked in account).</p>	<p>(Technical) validity of electronic certificate to be ensured (extension/re-signing, see above).</p> <p>Reminder to be sent to deposit holders six and three months before expiry of the term (by email).</p> <p>Account/deposit holder to confirm that the EUIPO should keep the deposit (see above, box to be checked in account).</p>
EUIPO 'Cleaning policy'	n/a	<p>The EUIPO would implement a 'cleaning policy' with a view to deleting deposits whose deposit holder could be considered no longer to have an interest in maintaining the deposit.</p> <p>Objective: avoid overload of the system</p> <p>Operation: the cleaning policy would allow the EUIPO to remove the deposit and the content deposited, for example, one year after the term of the deposit has expired, where the deposit holder has not opted for a renewal.</p> <p>In the case of deletion, the EUIPO will keep an automatic record of the facts of the deposit (dates, etc.), including the date of its expiry.</p>	<p>The EUIPO would implement a 'cleaning policy' with a view to deleting deposits whose deposit holder could be considered no longer to have an interest in maintaining the deposit.</p> <p>Objective: avoid overload of the system</p> <p>Operation: the cleaning policy would allow the EUIPO to remove the deposit and the content deposited, for example, one year after the term of the deposit has expired, where the deposit holder has not opted for a renewal.</p> <p>In the case of deletion, the EUIPO will keep an automatic record of the facts of the deposit (dates, etc.), including the date of its expiry.</p>
Withdrawal/ deletion of a deposit by account holder	n/a	<p>Yes (a technical feature would be required in the account).</p> <p>Digital Deposit System to keep a record of the filing details (user ID, deposit ID).</p>	<p>Yes (a technical feature would be required in the account).</p> <p>Digital Deposit System to keep a record of the filing details (user ID, deposit ID).</p> <p>After transfer of ownership, deletion would no longer be possible for the initial deposit owner.</p>

4. LEGAL FEASIBILITY

The legal assessment is based on the information provided in Chapter 3 (STRUCTURE OF THE DIGITAL DEPOSIT SYSTEM FOR THE FEASIBILITY ANALYSIS)

). Given the number of options proposed and pending a definite structure of the system to be set up, the assessment was carried out based on the assumptions how all three proposed options might function.

4.1 Legal basis for setting up an EU-wide Digital Deposit System that would be managed by the EUIPO

According to Chapter 3 of the Feasibility Analysis, an EU Digital Deposit System could be used to:

- **Option 1:** enable authors, inventors, creators and business in general to **prove the existence of their works or other information at a certain point in time**; or
- **Option 2:** enable authors, inventors, creators and business in general to **upload their works and other information to a central repository so as to keep evidence of the date of deposit**; or
- **Option 3:** enable authors, inventors, creators and business in general to **upload their works and other information to central repository so as to keep evidence of the date of deposit with additional functionalities**, such as **management** of certain rights in content deposited or making available to the **public information** about the content or the content itself.

First of all, in order for an EU Digital Deposit System to be functional, the creation, operation and management of such system should be provided for in a relevant piece of EU legislation, and in addition specifically as one of the EUIPO's tasks.

From a legal point of view, all three options of an EU Digital Deposit System analysed below propose a **digital certification system**. The object of the certification is that **digital content had been submitted/deposited at a specific point in time by a certain user of the system**. Option 3 would also offer some extra functionalities. The EUIPO certification **would not confirm** that the content was created by the submitter/depositor at the time of submission/deposition.

Two identical/similar pieces of content may be submitted/deposited by different users of the

system and a timestamp would solely serve as a proof of an earlier date of submission/deposit. The legal or evidential value of the system other than what has been explained above cannot be determined by the EUIPO itself, except possibly with respect to its own proceedings. Regarding documents used or to be referred to in proceedings before the Office, the system of certification could perhaps be based on Article 123b(1)(a) and (b) of Council Regulation (EC) No 207/2009 of 26 February 2009 on the European Union trade mark as amended by Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 (EUTMR)⁴².

With respect to certification of content that could serve another purpose than being used in the proceedings before the Office, there currently appears to be no legal basis either in the EUTMR, or in Regulation (EU) No 386/2012 of the European Parliament and of the Council of 19 April 2012 on entrusting the Office for Harmonization in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights, including the assembling of public and private sector representatives as a European Observatory on Infringements of Intellectual Property Rights (Regulation (EU) No 386/2012)⁴³.

To sum up, the main features of an EU Digital Deposit System that will be assessed in detail below are the following:

- a) the system will not create any new rights for its users;
- b) the content will only be in digital form;
- c) the system should be highly confidential and secure;
- d) in principle, no modification of submitted/deposited content or information that serves to identify the content should be allowed (as specific content with a specific title would be certified at a certain point in time, that of submission/deposit);
- e) any modification to already certified content would require a new date of certification and would be considered as a submission/deposit of new content with the new date of submission/deposit;
- f) the date of submission or deposit of the specific content will be digitally certified/timestamped by the EUIPO;

⁴² Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 amended Council Regulation (EC) No 207/2009 on the Community trade mark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trade mark, and repealed Commission Regulation (EC) No 2869/95 on the fees payable to the Office for Harmonization in the Internal Market (Trade Marks and Designs) (Text with EEA relevance), OJ L 341, 24.12.2015, pp. 21-94. Note that these texts were codified by Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (the corresponding provision is Article 151). The Feasibility Study was finalised in January 2017; the present text therefore refers to the legal instruments in force at that time.

⁴³ Regulation (EU) No 386/2012/EU of the European Parliament and of the Council of 19 April 2012 on entrusting the Office for Harmonization in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights, including the assembling of public and private-sector representatives as a European Observatory on Infringements of Intellectual Property Rights (Text with EEA relevance), OJ L 129, 16.5.2012, pp. 1-6.

- g) the certificate will be valid for a certain period of time and may be extended/re-signed for an unlimited number of times with the renewal of the deposit (only with the user's consent);
- h) the content will not be checked/verified by the EUIPO and will be kept secret, that is, it will only be known to the submitter/depositor of that content (unless the depositor chooses to make it publicly available/option 3 of the Digital Deposit System);
- i) EUIPO staff should not be able to access the content under any circumstances, unless the user gives prior express written permission;
- j) the identity of the submitter/depositor will not be verified by the EUIPO;
- k) there will be no limitations on users regarding their place of residence, business or nationality (worldwide submission/deposit);
- l) the certificate should be accepted by all courts of EU Member States as proof of date of submission/deposit of certain content by a certain user of the system;
- m) users may be charged for using the Digital Deposit System;
- n) the EUIPO will keep a record of information about the date when specific content was certified by the EUIPO.

4.2 Assessment of the legal feasibility of each of the proposed options for the system

4.1.1 Basic system

4.1.1.1 *Option 1 for the basic system*

Under proposed **option 1** for the basic system, the EUIPO **would not store** the submitted content and would only provide **electronic proof of the date of submission and the existence of the content at a certain moment in time**. Therefore, from a legal point of view, in reality the proposed system would not function as a deposit as there will be no physical storage of the provided content (the created copy of the content would not be retained by the EUIPO). However, the EUIPO would still need to ensure that a temporarily created copy would not be accessed by anyone during that time, that is, confidentiality and security during the process should still be guaranteed to users.

4.1.1.2 *Option 2 for the basic system*

Option 2 for the basic system would allow the deposit of digital content. The EUIPO would issue proof that the content has been deposited on a specific date by the specific user. In this case, the EUIPO would not only certify the date of a deposit, but would also provide the possibility of depositing/keeping the certified content in its digital depository system for a certain period of time. However, all other features of option 1 of the system would be applicable.

Moreover, the deposited content would need to remain confidential and secure. In Chapter 3 of the Feasibility Analysis, it is proposed that the EUIPO would not be liable for the content deposited. However, if the system were claimed to be secure and highly confidential, the

EUIPO would be still responsible for ensuring that the content could not be accessed by anyone at any point in time (unless the user gives prior express written consent). For that purpose certain measures would need to be put in place by the EUIPO.

For example, Article 2 of Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed **know-how** and business information (trade secrets) against their unlawful acquisition⁴⁴, use and disclosure states that ‘trade secrets’ means information which meets all of the following requirements, [i.e.] it is secret [...], has commercial value because it is secret [and] has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.’ Therefore, in order to provide such protection, the EUIPO should ensure that such information would remain secret and not be disclosed internally or externally without the trade secret holder’s knowledge. In addition, even if access with the agreement of the depositor should not be problematic (and it would need to be given in advance or on a case-by-case basis), accessing the content without the agreement/authorisation of the depositor might be more complicated legally⁴⁵.

4.1.2 Advanced Digital Deposit System (option 3)

The **advanced Digital Deposit System** would be based on **option 2** for the basic system but would have additional features, such as the possibility of users managing their deposited content and granting public access to certain elements relating to the content.

Depending on the proposed additional features, as explained in option 2, it needs to be ensured that secrecy of the deposited content is not breached, and that personal data are processed in line with data protection laws applicable to the EUIPO.

Currently, the EUIPO states that all personal data collected by the Office is processed in accordance with the provisions of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data⁴⁶. As a general principle, the EUIPO only **processes personal data for performing tasks carried out in the public interest on the basis of the Treaty on the Functioning of the European Union, on the basis of (1) the EUTMR and the Community Design Regulation (CDR)⁴⁷ (2) or in the legitimate exercise of official authority vested in the EUIPO or in a third party to whom the data are disclosed**. Hence, the processing of personal data has to be directly linked with performing tasks of the EUIPO.

⁴⁴ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157, 15.6.2016, p. 1-18.

⁴⁵ Note that all options presented for an EU Digital Deposit System require the express consent of the deposit holder for anyone to access the content of the deposit.

⁴⁶ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, pp. 1-22.

⁴⁷ Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, OJ L 3, 5.1.2002, pp. 1-24.

In addition, transfer of the content should ensure that the digital timestamp would stay intact and that the content would not be modified. Any access to the content deposited would require prior express consent from the deposit holder (provided for by the system). Any EUIPO intervention without prior express written consent from users in the advanced Digital Deposit System to access the content before the content has been published would breach the protection guaranteed to the users of the system, that is, security and high confidentiality.

Aspects of the possible legal regulation of an EU Digital Deposit System are explained below.

4.1.2.1 EU law

Article 123b EUTMR, which specifies the tasks of the EUIPO, including the tasks referred to in Regulation (EU) No 386/2012, does not specifically envisage any possibility of creating and managing an EU-wide Digital Deposit System. Nor is there any such reference in any other EU legislation. Accordingly, although the description of the tasks of the Office in Article 123b EUTMR is not exhaustive (i.e. the existence of a separate legal basis would suffice even if not expressly mentioned in the EUIPO's founding act), the current lack of any legal basis means that it is not possible to go on with creating a Digital Deposit System in any form, without appropriate, targeted changes in the existing regulatory framework.

Therefore, for this particular purpose: (i) either specific EU legislation would need to be adopted allowing for the creation/existence and management of such a system. For example, specific provisions to that effect could be added to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (IPRED)⁴⁸, following the model used in the case of the new powers of the EUIPO related to orphan works (provided for in the specific Directive by referring to Regulation (EU) No 386/2012) or powers related to a possible out-of-commerce database (as envisaged in a proposal for a Directive on copyright in the Digital Single Market⁴⁹), which are contained in both Directives. Alternatively (ii), Article 123b EUTMR would have to be amended by including new provision(s) entrusting the EUIPO with that particular task. In addition, the purpose of the system is to have EU-wide applicability, that is, that the EUIPO certification would be accepted as proof of evidence in legal proceedings by all courts throughout the European Union. It remains to be seen whether this could also be accepted as proof outside the EU, because the system would be based on EU legislation.

However, it would only serve as evidence of the date on which the content was deposited by the person for the courts of Member States, and only as far as the laws of the relevant Member State were to allow it, that is, unless EU legislation directly applicable to Member States clearly stated that the documentation would be accepted and recognised by all EU courts as sufficient evidence.

⁴⁸ Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004), pp. 16-25.

⁴⁹ Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM/2016/0593 final — 2016/0280 (COD), Article 7 et seq.

4.1.2.2 *International law*

Even if a relevant legal basis were to be established, the use of the proposed deposit system could only work on a voluntary basis. Under Article 5(2) of the Berne Convention for the Protection of Literary and Artistic Works⁵⁰, copyright protection cannot be conditional upon compliance with any formality (principle of ‘automatic’ protection). This principle entails that the author of an original work receives, by the mere fact of creating the work, a bundle of national rights throughout the territory of the EU⁵¹. All Member States of the EU are parties to the Berne Convention, a binding international instrument that applies to the protection of works outside of the country of origin and of foreign authors. In addition, Article 9(1) of the TRIPS Agreement⁵², to which all Member States and the EU are parties, obliges its members to comply with most of the substantive provisions of the 1971 Paris Act of the Berne Convention; this includes Article 5(2).

As the responses to the survey (see ANNEX I: SUMMARY OF REPLIES TO QUESTIONNAIRE FOR SURVEY ON REGISTRATION/DEPOSIT SYSTEM(S)

) have shown, depending on the law of the respective country, that **voluntary** registration/deposit systems may have certain legal effects: they may create a rebuttable presumption that the person who registers is the author or derivative rights holder, or that a copyright subsists in the work registered⁵³.

The Digital Deposit System will only certify the date of submission/deposit of content, without explicitly regulating in which cases it could be used as proof for any specific purposes. The use of this system should be on a voluntary basis, that is, without creating a legal obligation that would require this specific certification in certain definite cases.

4.3 Liability of the EUIPO

If the EUIPO does not verify the identity of users and content submitted by them, it will only **be liable for the correctness of certification of the date of submission of the content/its deposit in a depository by the user.**

Therefore, in principle, the EUIPO **should not be liable for the content provided or the identity of the person submitting the content**, for example, if it might have been stolen from

⁵⁰ Berne Convention for the Protection of Literary and Artistic Works (as amended on 28 September 1979).

⁵¹ See, Dreier, T., Hugenholtz, B. (eds.), Concise European Copyright Law, Wolters Kluwer, Alphen aan den Rijn, the Netherlands, 2016, p. 8 et seq.

⁵² The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) is Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.

⁵³ See also in this context, Lewinski, S. von, International Copyright Law and Policy, Oxford University Press, Oxford, 2008, at 5.61, referring to the results of the WIPO surveys.

the real owner.

4.4 Fees

There must be an explicit legal basis for the EUIPO to be able charge a fee; the amount of the fee would need to be specified as well as for what services it would be charged. That should appear in the legal act that will govern provision of these services (e.g. Annex I to the EUTMR includes services with their applicable fees).

4.5 Access to/disclosure of content

The main issue to consider is when and under what conditions the content could be accessed by the EUIPO/requested to be disclosed to third parties:

- a) at the request of any EU national court — only with prior express written consent from the user;
- b) under a request for access to documents — whether the content would qualify for requests for access to documents; whether it could be accessed at all (i.e. public interest versus private interest).

Regulation (EC) No 1049/2001 on public access to documents⁵⁴ establishes that any citizen of the European Union, and any natural or legal persons, residing or having their registered office in a Member State, has a right of access to documents of the institutions, subject to the principles, conditions and limits established by the Regulation.

The above Regulation defines a 'document' as 'any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility'.

In theory, this definition of 'document' could cover the digital content in the Digital Deposit System. Therefore, there might be cases where the EUIPO could receive a request to grant public access to certain content in the Digital Deposit System.

In such cases, according to Article 4 of Regulation (EC) No 1049/2001, it remains to be seen whether this request would fall under exceptions or not. It specifies that:

The institutions **shall refuse access to a document** where disclosure would undermine the protection of:

- (a) the public interest as regards:

⁵⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, pp. 43-48.

- public security,
- defence and military matters,
- international relations,
- the financial, monetary or economic policy of the Community or a Member State;

(b) privacy and the integrity of the individual, in particular in accordance with Community legislation on the protection of personal data.

2. The institutions **shall refuse access to a document** where disclosure would undermine the protection of:

- commercial interests of a natural or legal person, including intellectual property,
 - court proceedings and legal advice,
 - the purpose of inspections, investigations and audits,
- unless there is an overriding public interest in disclosure.**' (emphasis added)

However, note that paragraph 2 above specifies that access could be granted if 'there is an overriding public interest in disclosure'.

Moreover, as the content will not be the EUIPO's, but would belong to third parties, according to the wording of the same Article 4, 'As regards third-party documents, the institution shall consult the third party with a view to assessing whether an exception in paragraph 1 or 2 is applicable, unless it is clear that the document shall or shall not be disclosed.' Therefore, the disclosure to third parties of the digital content under an access to documents request is highly unlikely.

4.6 Terms of use

The terms of use would probably be governed and construed under Spanish law and any disputes, controversy or claims arising out of or about these terms of use, or the breach or validity would have to be settled by the court of Alicante, Spain.

The terms of use would need to be accepted by a person before using the system, that is, by submitting the content and/or depositing it.

The terms of use will need to provide information on the following issues:

- a) what services will be provided and to what extent the user grants the EUIPO a right to use the deposited content, if any;
- b) detailed conditions of use;
- c) disclaimer about the liability and limitations of the EUIPO and users;
- d) what content can be accepted (unless the EUIPO claims non-liability for any content provided as it will not be verified by the EUIPO);

- e) cases when the content could be accessed by the EUIPO or disclosed. However, this may require prior express written consent from the user (for each case) and/or duly justified reasons to be provided by the EUIPO as well;
- f) data protection issues;
- g) modification, discontinuation or termination clauses;
- h) other miscellaneous provisions etc.

The above list is non-exhaustive and only serves as an example.

4.7 Additional questions related to security and data protection

4.7.1 The EUIPO's relation to the EU Regulation on digital trust

The new Regulation on digital trust (eIDAS)⁵⁵ is only applicable to Member States and does not apply directly to the EU institutions. Therefore, it should not be applicable to other EU bodies by default either.

The EUIPO will apply its own procedures for providing digital services, that is, the internal procedures that have to be followed in this case. This issue should be reflected in the feasibility assessment by the information and communications technology services.

4.7.2 The EUIPO's relation to other international timestamping standards such as RFC 3161, X9.95 or ISO 18014

Currently, the EUIPO recognises international management standards in quality (ISO 9001), environment (EMAS Regulation)⁵⁶, occupational health and safety (OHSAS 18001), **information security (ISO 27001)**, as well as universal accessibility (UNE 170001). The guiding principles of the security policy of the Office are defined in accordance with the **ISO/IEC 27001 standard**, which establishes a reference security framework supported and recognised internationally.

⁵⁵ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73-114.

⁵⁶ Regulation (EC) No 1221/2009 of the European Parliament and of the Council of 25 November 2009 on the voluntary participation by organisations in a Community eco-management and audit scheme (EMAS), repealing Regulation (EC) No 761/2001 and Commission Decisions 2001/681/EC and 2006/193/EC, OJ L 342, 22.12.2009, pp. 1-45.

4.7.3 Requirements resulting from ISO 27001 for the management of customer data

Customer data should be managed in line with the security policy of the EUIPO, which has been defined in accordance with the requirements of the ISO 27001 standard.

4.7.4 The EUIPO's relation to EU legislation on data protection

All personal data collected by the EUIPO is processed in accordance with the provisions of **Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data**⁵⁷. Therefore, any personal data will have to be processed under the requirements of this Regulation.

4.8 Legal conclusions

The conclusions intend to briefly address legal aspects that would be applicable to all three options proposed. However, the detailed separate assessment of each option is carried out in section b of this legal assessment.

Currently, there is no explicit legal basis for the EUIPO to set up the Digital Deposit System. Such a system at an EU-wide level would require either the amendment of Article 123b EUTMR or the inclusion of provisions on new EUIPO powers in the already existing specific EU legislation, or the adoption of a new regulation directly applicable in the Member States.

Under the current proposal, the EUIPO would only certify the date when the content was submitted or uploaded. Such certification would only apply to a date and no verification would be carried out on the submitted/deposited content or an identity of the owner of the content. Moreover, the certification would not result in granting IP or any other rights.

Even if a legal basis were established, the use of the proposed deposit system could only work on a voluntary basis; under the Berne Convention for the Protection of Literary and Artistic Works, protection must not be conditional upon compliance with any formality (principle of 'automatic' protection).

Terms of use of the Digital Deposit System would need to be established containing all

⁵⁷ Regulation (EC) No 45/2001 should be adapted to the principles and rules established in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), and applied in the light of the GDPR (see recital 17 and Article 2(3) GDPR).. See, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM/2017/08 final.

provisions related to the use of services, content deposited, choice of law and court with regard to disputes in relation to these terms of use. The submitter/depositor submitting/depositing the content would need to agree to the terms before using the Digital Deposit System.

The Digital Deposit System must be in line with standards and internal procedures applied by the EUIPO to ensure that the system is secure and highly confidential.

5. TECHNICAL FEASIBILITY

The evaluation of the technical feasibility of the Digital Deposit System is based on the summary analysis laid out in Chapter 2 and the options given in Chapter 3. Focus is on creating and operating an IT tool under the following aspects:

- a) security requirements
- b) principle of operation of the system
- c) trusted timestamping
- d) technical features of the content or information deposited
- e) functional features.

The technical feasibility is concluded in section (f). Information concerning initial and running costs for each option has been provided in Chapter 7.

5.1 Security requirements

A prominent characteristic of the system is keeping the deposited content secret. The architecture of the system should correspond to this requirement.

In a preliminary assessment, the system is evaluated in relation to confidentiality, integrity (correctness) of data processed and stored, as well as the availability of the tool. These requirements lead to an overall security classification. **With respect to confidentiality, it is assumed that the content managed on behalf of the user must be kept at the ‘secret’ level (‘confidential’ is not sufficient).** With respect to integrity and availability, the tool will be considered ‘critical’ for the operations of the EUIPO.

In order to keep data secret, data access restrictions that are compliant with the rules laid out in the SOC2 standard are considered necessary. This results in **encrypted data storage** with controlled access policies and a reproducible audit trail of any access to content (including reading of data/content).

5.2 Principle of operation of the system

In a straightforward approach, a registered user uploads digital content in an electronic file attached to a web form and supplies certain metadata. After submission of the form and on completion of reception, the tool records the point in time and securely stores the timestamp, the data supplied, as well as either the content itself (option 2 and 3) or merely a unique fingerprint of the uploaded file (option 1) as a new deposit.

All deposits belonging to a user are accessible through the user’s account. For example, a user may change a deposit’s title or other metadata, delete a deposit and group multiple deposits in a folder.

For example, the tool will assign a unique identifier to each deposit and provide the user with a permanent hyperlink to the page describing the deposit. By default, access to the page would be granted only to the user depositing the content. Users might — depending on the option — be able to grant third-party access to certain attributes of their deposits (e.g. under option 3, the user could grant public access to the information and/or the content deposited).

5.3 Trusted timestamping

The aim of the tool is to provide unequivocal evidence about the existence of content or other information at a certain point in time.

A basic level of certainty has already been achieved through the integrity of the **EUIPO's domain name** 'euipo.europa.eu', as well as the trust placed in the EUIPO associated with its domain name. The point in time of reception of the content or other information is recorded by a tool, thus producing irrefutable evidence.

In addition, the trustworthiness sought — regardless of the option chosen — will be increased by **cryptographic means, namely, 'trusted timestamping'**. This means establishing electronic trust independently of any domain name and the associated web site, thus increasing the level of certainty regarding the source of the record. Under this approach each deposit will be complemented by a **certificate containing a timestamp**. The certificate will be produced on reception of the content and the information provided in relation to the content, and it will be available for downloading.

The technical complexity of generating the certificate must be emphasised. Despite the EU Directive on electronic signature⁵⁸ having been in place for over a decade and having recently been repealed by the eIDAS Regulation⁵⁹, market penetration and legal acceptance of cryptographic means remains low (the latter is likely to change in the upcoming years as a consequence of the adoption of the Regulation).

Therefore, to simplify the proof that given content does correspond with the content that has been certified or deposited, an **online utility (cryptographic content verification tool)** is envisaged. A third party (e.g. a court) would be provided with the possibility of uploading a copy of the disputed content and the certificate for the content to the tool run by the EUIPO. No user account would be required for this purpose. The tool would, at the third party's request, verify whether the copy of the content and the certified content are identical. The proposed approach combines ease of use with an additional layer of trust. When in doubt, the verification may still be carried out by a third party or an expert, independently of the EUIPO and with greater technical effort.

⁵⁸ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, pp. 12-20.

⁵⁹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73-114.

In order to provide a certificate that generates a high level of trust (among the users of the system and in general), it must be possible to verify that the certificate really has been produced by a trustworthy organisation. This challenge is traditionally addressed using a **centralistic approach** under which trust is delegated from a global root to the party actually applying the key necessary to prove PKI identity. Lately, the centralistic approach has been challenged by decentralised methods, for instance, blockchain. However, for this feasibility study, the decentralised approach to trust provision has not been considered, as it has not yet proved to be an established, comprehensive and secure method. Nevertheless, it must be considered that decentralised methods could offer advantages, in particular, when emphasis is placed on transfers of digital content and associated IP rights.

5.4 Technical features of the content or information deposited

An uploaded file would be considered by the tool as an immutable sequence of bytes of a certain length. **Two files would be considered as equal if the sequence of the bytes were identical.** There would be no assessment of similarity either. From a technical point of view, the Digital Deposit System merely provides evidence that a certain, unique, digital sequence has been submitted at a certain point in time.

The Digital Deposit System will be used for uploading different types of content and other information (e.g. ranging from a literary work to audiovisual content). Respectively, numerous digital media content standards (formats) under which uploaded content may be encoded should be considered.

In general, the system may well remain agnostic regarding formats, as **evidence is granted for the underlying digitally encoded sequence.** Nevertheless, in order to support content-based searching (option 3), the tool will need to do both: permanently store the upload (option 2) and interpret the format in order to extract relevant information (e.g. words contained in a PDF document).

Due to the varied nature of the content and other information, the size of the individual upload will range from a few bytes up to several gigabytes. Technically the upload of a two-hour film in high definition quality (~10 GB) would be feasible, provided the tool's processing and (transitional) storage capacities are dimensioned accordingly. The size of an uploaded item is limited mainly by the available bandwidth on the client side and less by storage capacity.

Uploaded items must be considered as client data. The requirements for data protection and data availability could be comparable with other operational data at the EUIPO (e.g. deferred designs). Therefore, similar data governance rules determining operational procedures, such as backup and data restore, archiving and disaster recovery, are likely to be applied. Further, in order to accomplish a higher level of data confidentiality, encrypted storage could be included.

Features that allow grouping the users' deposits, for example, through versions, folders, labelled collections, may be offered. However, it is assumed that the evidence will be provided

for each individual deposit, not for the whole group.

5.5 Functional features

The functionality to be offered is grouped by three different broad categories of users:

- i) registered users of the system (i.e. depositing items);
- ii) general public users (e.g. general public opening an account in the Digital Deposit System, searching the Digital Deposit System (option 3 only) or third parties providing cryptographic content verification (all options));
- iii) administrative users (i.e. managing the tool).

Depositing users register by providing, inter alia, their contact details and a valid email address. No proof of identity would be required for the act of depositing. However, for possible payment of fees, further measures would need to be considered. Users from the general public could remain anonymous. Administrative user management will be operating centrally at the EUIPO in full analogy with other comparable front office EUIPO tools.

For **option 1** the following functional features have been identified.

ROLE	FUNCTIONALITY (LEVEL 1)	FUNCTIONALITY (LEVEL 2)
Public	Opening a user account	User registration
		Email verification
		Account activation
Public	Log in	Log in
Private	Certificate management	Search & display
		Download
Private	Log out	Log out
All	Other	Statistics
		Audit logs
EUIPO	Maintenance console	Statistics
		Audit logs
		Fees
		Communication
Private	Submitting content for timestamping and certification	Accounts
		Submit content
Public	Verify content certificate	Timestamping and certification
		Verify certificate

For **option 2**, the following functional features are included, in addition to option 1:

ROLE	FUNCTIONALITY (LEVEL 1)	FUNCTIONALITY (LEVEL 2)
Private	Making a deposit in the Digital Deposit System	Submit new content
		Submit new version
		Timestamping and certification
Private	Management of the content deposited	Download content
		Withdrawal
		Expiry
		Renewal

For **option 3** the following functional features are included, in addition to option 2:

ROLE	FUNCTIONALITY (LEVEL 1)	FUNCTIONALITY (LEVEL 2)
Private	Management of the content deposited	Download content
		Withdrawal
		Expiry
		Renewal
		Transfer deposit ownership
		Content publication/confidentiality
Public	Public access to information about deposits	Search
		Display
		Denounce content
EUIPO	Sporadic control of deposited content	Automatic content revision
		Manual content revision
Public	Court proceedings	Provide information to the court

6. IMPACT

A voluntary Digital Deposit System at EU level may help address some of the challenges created by digital technologies; for instance, it could increase legal certainty concerning the ownership of content, or facilitate exercising rights in the digital environment. Such a system could stimulate the legitimate use of content, and help rights holders enforce their rights in cases of infringement claims.

In any event, the establishment of an EU Digital Deposit System with EU-wide effect and administered by the EUIPO must be founded on a specific legal basis (6.1). Once established, the system is expected to have a positive impact on both individual and corporate users (6.2).

6.1 The need for a legal basis

An EU voluntary Digital Deposit System must have an explicit legal basis in EU legislation. The legal basis should contain provisions on the establishment and functioning of the system; it should, inter alia, specify the possible fees due for depositing content, and for renewal of the deposit.

In particular, the legal basis should specify that the deposit documentation, issued by the EUIPO, is accepted by courts in the EU Member States as sufficient evidence of the date of deposit. Especially in the context of cross-border exploitation of content, a system providing evidence that is valid throughout the EU would present clear advantages compared with a national system.

There is insufficient information as to whether documents proving the date of deposit issued by a national registration/deposit body are recognised by the courts in other EU Member States. Recognition of evidence in relation to the date of deposit could be addressed either by a mutual recognition procedure of national deposit systems of EU Member States (where in existence), or by establishing a deposit system at EU level that is recognised as evidence in all Member States. While mutual recognition would require agreement from all Member States and obtaining evidence would be based on different national conditions and procedures, an EU Digital Deposit System would provide a fast and easy solution, namely a one-stop system for ensuring evidence be recognised at EU level with unified conditions and procedures. Finally, it should be emphasised that a Digital Deposit System at EU level would not be competing with national systems, but complementing them.

6.2 Expected reception and use of the Digital Deposit System

It is expected that any type of content could be deposited. That is, the system will be open primarily to content that is protected by IPR. As the system will be operated on a highly confidential and secure basis, it is possible that any information (not necessarily protected by IP) could be deposited. The content deposited may include, for example, content protected by copyright or constituting a trade secret, unregistered designs or information relating to future designs⁶⁰ or patent applications.

As to possible user groups of the system, deposits both from individual creators or inventors, companies and notably from small and medium-sized enterprises (SMEs) are expected.

The system would be beneficial for individual authors, inventors and other creators because it would fulfil significant evidentiary functions. The entry in the depository would be particularly useful in conflicts where the anteriority of ownership or the priority to the claim must be resolved. The date of deposit would be securely assigned by highly reliable technological tools, including electronic certificates and timestamping technology. Especially regarding enforcement in the online environment, a deposit could help rights holders deliver evidence when they submit a take-down notice to an online platform. Evidence generated by the EU Digital Deposit System could also facilitate the work of online platforms, and help them to take down illegal content more quickly.

For entrepreneurs and small businesses, the system could be a simple and inexpensive way to prevent others from stealing their ideas and innovations. For example, the system could serve as useful evidence for companies wishing to keep their inventions secret, to protect ideas when they are still in the development stage or in the course of negotiations with potential business partners. The Digital Deposit System could be a significant first step in the innovation process, that is, in the preliminary phase of an application for a design or a patent.

In the case of the advanced option, containing a public search function and optional publication of deposited content, as well as a possible rights management feature, the system could constitute an indispensable source of information for identifying content, its author(s) and current rights holder(s).

The number of deposits identified in the survey backs up these expectations. Indeed, the timestamping and deposit services offered by the private sector initiative studied appear to have by far the highest number of users. Over a period of 10 years (2006-2016), over 500 000 deposits were filed⁶¹. The private sector initiative focuses on content protected by copyright,

60 Regarding designs, the EUIPO regime for registered Community designs with deferred publication might in some cases be more attractive for creators or entrepreneurs who wish to further develop their marketing strategy or to finalise the preparations for production while not revealing the design to competitors. The proposed digital deposit system (notably the advanced version) does not compete with existing systems of protection. It offers creators and entrepreneurs a simple tool to facilitate the enforcement and possibly the management of their rights.

61 We understand that over 500 000 publicly accessible pieces of content have been deposited/registered.

and offers additional features including publication and public search functions. It also includes some features for content management.

However, in reality the exact number may be higher.

7. COSTS

The cost estimate is based on the following assumptions.

- The tool will be a proprietary development of the EUIPO. It will be created as an EUIPO project and will follow the EUIPO's project methodology.
- The tool's lifecycle management (e.g. change requests) will be under full control of the EUIPO.
- The tool will be deployed and operated by the EUIPO.
- While, for the sake of availability, the tool is operated on a redundant cluster, a single instance of the cluster will productively be active. In other words, multi-tenancy is not supported (multiple separate organisations/units sharing one technical installation).
- The tool is purely web-based for the user. All human interaction with the tool is by interacting with a web browser. The tool remains 'stand-alone'.
- No integrations with other tools except for producing certificates, automated email communication relays and electronic payment gateways are taken into consideration.

Furthermore, it is assumed that the tool will be built and become operational **in one year**.

The main cost is associated with human resources. The development effort of functional features falls under this type (e.g. determining the effort going into quality control). The second largest cost type is the content storage/content management. The third largest cost type goes to producing certificates needed to establish the trust beyond the EUIPO's site (PKI).

The dimensioning of content storage required an estimate of the number of users and the average volume of content uploaded per user. The estimations have been produced under the assumption of having attracted 100 000 users to hold 1 GB of content storage each. The resulting volume of 100 TB could well be accommodated at the EUIPO's data centre. However, the resulting data volume exceeds the volume managed currently by an order of magnitude. As a consequence, technical procedures for operational data management will probably have to be adapted.

The dimensioning of the PKI required an estimate for the number of certificates to be produced annually. It has been assumed that 1 000 000 certificates will be issued annually. In this context, the EUIPO would act as a timestamping authority directly, managing its own PKI, which would have to be created initially at considerable cost and effort (EUR ~100 000). Alternatively, certificates could be produced under a 'managed PKI' solution whereby the security critical infrastructure would be operated by a remote third party, a globally recognised trust provider, which would be dedicated only to the EUIPO. A comparative assessment of vendors, following the rules of public procurement, would be necessary.

ANNEX I: SUMMARY OF REPLIES TO QUESTIONNAIRE FOR SURVEY ON REGISTRATION/DEPOSIT SYSTEM(S)

TABLE OF CONTENTS

1. Institutional Information	52
2. Legal Information	53
a. Legal basis for a registration/deposit system	53
b. Content that can be registered/deposited	54
i. No information supplied on content	54
ii. Information on content supplied by users of the system	55
c. Registration/deposit process.....	55
d. Legal effects of registration/deposit	56
i. Establishing a presumption of authorship/ownership	56
ii. Providing evidence of the date of registration/deposit	57
iii. Recognition by courts in relation to dating evidence	57
iv. Other legal effects or benefits.....	58
e. Liability issues.....	59
i. Disclosure of information to third parties	59
ii. Dispute between a user of the system and a third party	60
3. Features of the National Systems	60
a. Characteristics of electronic registration/deposit systems	60
i. Existence of an electronic registration/deposit system	60
ii. Use of cryptographic methods.....	60

iii.	Authentication of users	61
b.	Requirements for filing requests for registration/deposit.....	61
i.	Main mandatory information fields for filing the registration/deposit request 61	
ii.	(Formal) examination of the information provided upon filing	62
iii.	Obligation of the registry/deposit to keep a fixed copy (in hard or digital form) 63	
iv.	Support for collections of works or versions of works	64
c.	Additional features of the system	64
i.	Confidentiality of the content, restrictions on access and existence of a public search facility.....	64
ii.	Possibility of revocation or renewal of registration/deposit	65
iii.	Possibility of recording a transfer (of rights in the work/content registered/deposited)	66
iv.	Possibility of licensing the content.....	66
d.	Existence and amount of registration/deposit fees	66
e.	Statistical information.....	67
i.	Number of registrations/deposits filed	67
ii.	Number of requests for information filed	68
iii.	Main characteristics of the users	68
iv.	Statistics or anecdotal evidence about the number of court cases in which the evidence submitted to the system has been used	69

1. Institutional Information

The survey was carried out between 6 June and 27 July 2016 on a number of Member States in which there are voluntary deposit/registration systems. The selected Member States were invited to provide information about existing IP registration/deposit system(s) in their countries managed by a public institution. The present analysis is based on the information the EUIPO received in the course of the survey.

The following Member States indicated that there are IP registration/deposit systems managed by **public institutions**⁶².

- **Benelux:** i-DEPOT tool, which allows users to record the existence of an idea, artwork, invention, prototype or other (possibly IP related) matters. The i-DEPOT tool has been available electronically since 2007. The tool is managed by the BOIP⁶³.
- **France:** *enveloppe Soleau*, a sealed envelope with two compartments serving as proof of priority for any content, managed by the INPI⁶⁴. An electronic version of the system was launched on 15 December 2016⁶⁵, that is, after the evaluation of the survey responses was finalised. The e-Soleau was therefore not examined in detail.
- **Hungary:** voluntary register of works protected by copyright, managed by the Hungarian Intellectual Property Office (HIPO).
- **Italy:** the General Public Register for works protected by copyright, managed by the Ministry of Cultural Heritage, Cultural Activities and Tourism. The Cinematographic Public Register and the Special Public Register for Computer Programs, managed by the Italian Society of Authors and Publishers (SIAE).
- **Portugal:** the Register of literary and artistic works, managed by the General Inspection for Cultural Activities (IGAC)⁶⁶.
- **Romania:** the Register of works protected by copyright, managed by the Romanian Copyright Office (ORDA). ORDA administers six National registers: i) the National registry for phonograms; ii) the National registry for videograms; iii) the National registry for computer programs; iv) the National registry for multipliers of CDs, audio and videocassettes; v) the National registry for private copies; vi) the National registry for works.
- **Spain:** the General Intellectual Property Register, comprising the Central Intellectual Property Register, which is part of central government and comes under the remit of the

⁶² In 2018, that is, after the research on existing deposit and/or registration systems had been concluded, the EUIPO was informed that following a reform of the Greek Copyright Act (Law No 4481/2017 amending the second paragraph of Article 69(1) of Law No 2121/1993 on Copyright, Related Rights and Cultural Matters) the Hellenic Copyright Organisation now has a legal basis to, inter alia, provide timestamps. This means that the Copyright Organisation may provide services of dating works or other subject matter that may be protected by copyright and/or related rights.

⁶³ Notaries (judicial officers) and some official bodies (often under the auspices of national tax authorities) offer deposit or registration systems that are, to some extent, similar or comparable with the i-DEPOT. Some of these systems do not exist in each of the Benelux countries and these are not available in a digital version.

⁶⁴ <https://www.inpi.fr/fr/protoger-vos-creations/enveloppe-soleau/enveloppe-soleau> (last accessed 5 September 2016).

⁶⁵ See the website of INPI about the e-Soleau: <https://www.inpi.fr/fr/services-et-prestations/e-soleau> (last accessed 31 January 2017).

⁶⁶ <https://www.igac.pt/apresentacao> (last accessed 12 August 2016).

Ministry of Education, Culture and Sport, and the regional Intellectual Property Registers, which are set up and run by the various regional governments of Spain and the autonomous cities of Ceuta and Melilla.

In addition, Member States were asked to give information about **private entities** that provide an IP registration/deposit service.

Benelux noted that many private (commercial) parties offer similar or comparable services in Benelux and in Europe and that for private (commercial) entities there is no regulation on this matter.

In France, several private entities provide a digital IP registration/deposit service.

Hungary indicated that, on the basis of the Copyright Act, a collective management organisation (CMO) can also provide an IP registration service. The CMO 'Artisjus' maintains such a registration system in Hungary.

In Portugal, the Portuguese Society of Authors (SPA) provides similar services. However, it is not a registration, but a declaration that enables rights holders to enrol their works in the CMO records.

Italy and the United Kingdom provided examples of private entities that offer IP registration/deposit services.

The private sector initiative that was studied in most detail was a Spanish company founded in 2007, which offers a tool that produces timestamps. The currently available online version was established in 2013.

2. Legal Information

a. Legal basis for a registration/deposit system

In relation to the question as to whether there is a legal basis for a registration/deposit system in their country, all selected Member States where there are publicly administered IP registration/deposit systems replied positively.

For the i-DEPOT tool, the legal basis is the Benelux Convention on Intellectual Property which is applicable in all of Benelux and has direct effect. As a means of evidence, the i-DEPOT is not limited to Benelux territory.

In France, Article R.511-6 of the French IP Code is the legal basis for the public registration/deposit system administered by the INPI. A Decree of 9 May 1986⁶⁷ sets out the working principles of the *enveloppe Soleau*.

⁶⁷ [Arrêté du 9 mai 1986](#) fixant les modalités pratiques de recours aux moyens de preuve de la date de certaines créations.

In Hungary, the legal basis for the registration/deposit system is Article 112(5) of the Copyright Act and a Decree⁶⁸ of the Ministry of Justice.

In Italy, the three public registers are provided for under Article 103 of the Law on Copyright. The procedures for deposit and registration in the General Public Register are laid down in the Regulations implementing the Law on Copyright⁶⁹. The Cinematographic Public Register was established under Royal Decree-Law⁷⁰ and the Special Public Register for Computer Programs was established under a legislative Decree⁷¹ and a Prime Ministerial Decree⁷².

In Portugal the system is based on the Copyright and Related Rights Code (Article 213 et seq.) and a Decree-Law⁷³ for the registration of literary and artistic works.

In Romania, the relevant legal basis is the Law on Copyright and Related Rights⁷⁴ and a Government Order⁷⁵ with subsequent supplements and modifications.

In Spain, it is the consolidated text of the Law on Intellectual Property, approved by Royal Legislative Decree⁷⁶, which deals with the Intellectual Property Register in Title II of Book III. The regulations governing the General Intellectual Property Register are approved by Royal Decree⁷⁷.

b. Content that can be registered/deposited

Some systems offer deposit of the content (e.g. i-DEPOT), whereas others register rights in works or other subject matter (e.g. in Spain). The systems can be divided into the following categories, depending on whether the user is required to declare what content he or she has submitted.

i. No information supplied on content

The i-DEPOT system offers the possibility of depositing any content, IP related or not. The BOIP has no insights about the content, which is kept confidential (no information on the content is supplied by the user and the BOIP has no information on whether the content is IP related).

In France, any kind of content may be registered/deposited by means of an *enveloppe Soleau* (e.g. inventions, designs, texts, drawings, business concepts).

⁶⁸ No 26/2010 (XII.28).

⁶⁹ Royal-Decree No 1369 of 18 May 1942.

⁷⁰ No 1061 of 16 June 1938, which became Law No 458 of 18 January 1939.

⁷¹ No 518 of 29 December 1992.

⁷² No 244 of 3 January 1994.

⁷³ No 143/2014.

⁷⁴ No 8/1996.

⁷⁵ No 25/2006.

⁷⁶ No 1/1996 of 12 April.

⁷⁷ No 281/2003 of 7 March.

ii. Information on content supplied by users of the system

In other Member States analysed, registration is mainly focused on content protected by copyright and related rights. In these situations the information on the type of content is supplied by the user upon filing the registration/deposit request.

In Hungary, for example, all types of works and subject matter of related rights established by the Copyright Act can be included in the voluntary register. The same is true for Romania and Portugal. In Spain, registration can be made in respect of rights in works, performances and productions protected by the Law on Intellectual Property. In Italy, different types of works or transactions concerning works can be registered in different registers. The General Public Register includes all types of works protected by copyright⁷⁸, designs for engineering or other similar works, as well as different transactions concerning these works⁷⁹. The Cinematographic Public Register allows transactions relating to films to be recorded (such as the sale of a film or the transfer or pledge of proceeds from a film). In the Special Public Registry for Computer Programs, entries can be made concerning transactions of computer software⁸⁰.

The private sector initiative studied supports registration of various types of content (e.g. literary, audiovisual, design works). The user has the possibility of indicating the type of content when filing the application for registration.

c. Registration/deposit process

The registration/deposit process varies depending on the type of content registered/deposited and whether the formality check is actually carried out by the public authority concerned itself.

In some of the Member States, the registration/deposit process is the same for various types of content, and the information submitted is not checked. For example, in the i-DEPOT system and regarding the French *enveloppe Soleau*, where the content is confidential, there is no difference in the registration process according to the type of content. The information submitted is not examined by the BOIP/INPI. In Hungary, the registration process is also the same for various types of content. The request for deposit has to contain certain required information⁸¹ and there is no further examination of the work.

⁷⁸ More specifically, printed works, magazines and newspapers; musical works and works intended for public performance; works of sculpture, painting, design, engravings and works of visual and similar arts, architectural designs; industrial designs; cinematographic works.

⁷⁹ Transactions inter vivos transferring in whole or in part the rights recognised by law or constituting rights of security interests, transactions of apportionment of company instruments, and measures to expropriate copyright and to withdraw a work from the market.

⁸⁰ Acts that transfer in whole or in part rights to economic exploitation of a piece of software, acts of apportionment (where co-authors decide to divide rights), company acts (where two or more persons give a company ownership rights over a piece of software).

⁸¹ The request for deposit has to contain the original or a copy of the work. The copy must be of a size that allows placement in an envelope of standard A4 size. If the copy is of a larger size, a carrier of not more than A4 size (a photograph, electronic data carrier, magnetic tape), durably fixing the work and suitable for

The Spanish IP Register's responsibility is the registration of **rights** in protectable subject matter, not of the subject matter itself. Each application and fulfilment of the necessary requirements for registration are checked carefully.

In other Member States the registration/deposit process depends on the type of the content (e.g. different forms may have to be used for filing requests for registration). In more complex procedures the examination of content is carried out by the public authority concerned (this is the case for Romania, Portugal and Italy⁸²).

The private sector initiative provides one registration process for all types of content. The information is not examined upon filing.

For more detailed technical information about the (formal) examination of the content submitted, please see below (*Formal*) examination of the information provided upon filing.

d. Legal effects of registration/deposit

i. Establishing a presumption of authorship/ownership

According to the information received, the registration/deposit establishes (or helps to establish in the case of a legal dispute) a rebuttable presumption of authorship/ownership.

In Hungary, the rebuttable presumption of authorship is clearly established in the Copyright Act⁸³. Similarly, the Italian Copyright Law⁸⁴ recognises the presumption of authorship in relation to works entered in the register. Italian law also emphasises that deposit or registration does not constitute the 'granting of a right', since the original title to copyright derives from the creation of the work and not from any form of registration⁸⁵.

Legislation in Spain and Portugal also establishes a rebuttable presumption of the existence of the registered rights and ownership of the latter by their proprietors. Registration/deposit by means of a French *enveloppe Soleau* establishes a simple presumption of authorship/ownership: the presumption can be overturned by any form of relevant and credible proof (e.g. a third party can prove that he or she created the content at issue before the deposit

identifying it, must be enclosed as a copy.

⁸² In the Italian General Public Register, works are deposited by submitting a copy of the work (e.g. for printed works, magazines and newspapers or musical works) or a photograph (e.g. for works of sculpture, painting or design) accompanied by two original declarations certified with revenue stamps. There are also specific procedures for the deposit of designs for engineering works, transactions inter vivos transferring in whole or in part the rights recognised by law, as well as for entering the records into the Cinematographic Public Register and the Special Public Registry for Computer Programs.

⁸³ Article 94(B) of the Copyright Act, which states that '... pending proof to the contrary, the person under whose name the work is registered by the HIPO in the voluntary register of works shall be regarded as the author, if able to substantiate it with a public document (...)'.

⁸⁴ Article 103(5) of Law No 633/41 states that 'registration is evidence that the work exists and has been published, therefore, unless and until there is evidence to the contrary, the authors or producers named in the Register are deemed to be the authors or producers of the works attributed to them'.

⁸⁵ Article 6 of Law No 633/41.

of the *enveloppe Soleau*).

The legal value of an i-DEPOT could be comparable to a notary act. As indicated by the BOIP, 'whereas the i-DEPOT does not create or grant any right, it might be interpreted by courts as a presumption of authorship/ownership'.

ii. Providing evidence of the date of registration/deposit

One of the essential features of the registration/deposit system is to provide evidence of the date of registration/deposit.

The date that is usually invoked is the date of registration/deposit (not the date of creation). For example, the date for registration purposes in Spain is the date of application (the date of the creation of the work does not appear on the application). In the case of i-DEPOT, the system provides evidence of the date of deposit/registration (this date will be invoked as the date of creation or invention⁸⁶).

The private sector initiative provides proof of the date indicated through timestamping. It acts as a timestamping authority (TSA)⁸⁷.

iii. Recognition by courts in relation to dating evidence

From the answers received, it appears that courts recognise (or should recognise) a registration/deposit in relation to dating evidence.

As noted by the BOIP, the digital version of the i-DEPOT is in conformity with the EU Directive on electronic signatures⁸⁸, which implies that the i-DEPOT certificate must be accepted by all courts of the EU. As a means of evidence, the legal value of the i-DEPOT is not territorially limited⁸⁹.

In Hungary, the courts recognise registration as a means of evidence: it can prove that the work that was entered into the voluntary register as the applicant's own creation existed on the date of issue of the certificate, with the same contents as those of the copy of the work attached to the certificate.

The same is true in France, Italy, Portugal and Spain, where registration/deposit can be used as

⁸⁶ In the paper version, it is the date stamped on the envelope. In the digital version, it is the date of the i-DEPOT certificate, which is a certified PDF document.

⁸⁷ A permanent hyperlink to the timestamped registration certificate is sent to the applicant (the information submitted and the upload time can then be viewed on the company's website). The registration certificate including a timestamp can also be downloaded and stored.

⁸⁸ [Directive 1999/93/EC](#) of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures OJ L 13, 19.1.2000, pp. 12-20. That directive was repealed by [Regulation \(EU\) No 910/2014](#) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

⁸⁹ Information gathered by the BOIP from the United States Patent and Trademark Office (USPTO) confirms that the value of i-DEPOT should also be recognised by the US courts.

evidence in legal proceedings. Regarding the General Public Register in Italy, the **compulsory** deposit of printed works, magazines and newspapers, works suitable for public showing or musical works (unless they have already been published in printed form), works of sculpture, painting, drawing, engraving and similar figurative arts, and architectural plans and works, industrial designs and models have evidentiary value. The **voluntary** deposit of instruments executed *inter vivos*, transferring in whole or in part rights afforded by law or constituting rights of possession or security therein, and instruments of partition or of association with respect to such rights, also has evidentiary value.

Spanish law⁹⁰ provides that in legal proceedings certified copies of registered entries, which are considered as public documents, serve fully as proof of evidence. They may also be used as evidence in foreign courts, which will give them the weight they consider appropriate, in accordance with the relevant provisions of the law applicable in each country.

The private sector initiative confirmed that their certificates have been used as evidence in a court case and were recognised by the court, although not cited in the ruling⁹¹.

iv. Other legal effects or benefits

In relation to other legal effects or benefits, the BOIP noted that one of the benefits of i-DEPOT is the possibility of applying the tool in numerous IP-related fields, such as copyright, unregistered designs, prior rights and claims in the field of patents, trade secrets, fair competition, etc. Benefits also include an archive function (the tool is used as a repository for information). The BOIP has more recently launched the public version of i-DEPOT, which allows publishing (partially or completely) the content deposited with the BOIP in a publicly available i-D Space (a database that contains all published i-DEPOTs)⁹².

Italy noted that there are additional benefits associated with the registration of cinematographic works. The entry of cinematographic works in the register provides access to State funds that are intended to encourage film production and distribution. The voluntary deposit of engineering projects and similar works allows the author to receive fair compensation from any person who, with gainful intent and without the consent of the author, carries out the technical project concerned. Similarly, in Spain, the registration of works in the General Intellectual Property Register is a common requirement in the case of applications for state aid or grants for culture-related activities. Mortgage legislation in Spain requires that anyone who wishes to mortgage the rights of protected works register such rights in their favour in the General Intellectual Property Register.

In addition, some systems offer users certain possibilities that facilitate the licensing of the content (see below, section iv).

⁹⁰ Article 319(1) of Law No 1/2000.

⁹¹ Trade Court of Logroño. Case 1240/2010, No 10/2011 (3 February 2011).

⁹² A public version of the system was launched at the end of 2016, that is, after the evaluation of the survey responses was finalised. The public version of i-DEPOT was therefore not examined in detail.

e. Liability issues

i. *Disclosure of information to third parties*

The Member States that participated in the survey did not identify any particular liability issues that could be linked to administration of the system.

To give an example, a possible liability issue could be the unauthorised disclosure of the deposited/registered information to third parties. This could potentially happen in a situation where the information is disclosed ('leaked') to a third party through a fault or hack into the system (IT failure) or via human intervention. None of these possibilities were identified as potential liability issues.

Regarding the disclosure of deposited elements to third parties, some systems are confidential, whereas others are open (to a certain extent) to the public.

For example, the i-DEPOT has recently launched the publication option, which allows publishing (partially or completely) the content deposited with the BOIP in a publicly available i-D Space (a database that contains all published i-DEPOTs)⁹³.

As to the French *enveloppe Soleau*, disclosure by the INPI to third parties is expressly excluded by the law: the *enveloppe Soleau* can be disclosed only by the applicants themselves or by a court of justice in the event of a legal dispute.

In Spain, any person may request disclosure of registered entries without restrictions. However, apart from the intellectual property rights holder, only third parties that can demonstrate a legitimate interest are permitted to consult the documents in the files archived in the Registers (with the exception of the content of the work or creation⁹⁴). In the case of works disclosed under a pseudonym, sign or anonymously, a search of the files is restricted to persons who are able to demonstrate a direct interest. In files relating to computer software, the only elements that may be searched are those contained in the corresponding register entry.

In Italy, anyone can consult the registry and receive a certificate or extract notifying them of registrations or statements in the register and a copy of the documents, submissions and associated paperwork. Upon request, the Italian office may also search the registry in order to provide the information⁹⁵.

⁹³ A public version of the system was launched at the end of 2016, that is, after the evaluation of the survey responses was finalised. The public version of i-DEPOT was therefore not examined in detail.

⁹⁴ It means that there are limitations with regard to the disclosure of the content registered. The Intellectual Property Register may disclose the content of registered entries without restrictions; however, there are restrictions with regard to the ability to access the content of files, including identifying the copy of the work, performance or production, to which access is not permitted.

⁹⁵ The applicant must clearly state in the request the nature of the work, its title and author, and the probable date of deposit; in the case of transfers or contracts to exploit the work, the names of the contracting parties must also be stated.

In Portugal, only a legal representative of the rights holder or the rights holder can ask for the disclosure of any deposited elements.

ii. Dispute between a user of the system and a third party

In the event of a dispute between a user of the system and a third party, for example, about the date on the evidence, the authority running the registration/deposit/timestamping system does not have any specific role.

Upon request of the holder or a court, the BOIP will deliver the envelope recorded⁹⁶. The BOIP does not intervene in disputes between users about the date of evidence.

No specific mediation or arbitration procedure is envisaged by any of the public and private mechanisms in the Member States studied. In the public i-DEPOT, the BOIP has set up a notice and take down procedure, aiming to protect the legitimate interests of third parties.

3. Features of the National Systems

a. Characteristics of electronic registration/deposit systems

i. Existence of an electronic registration/deposit system

The public registration/deposit systems available in Portugal, Romania and Spain and the Benelux i-DEPOT offer the possibility of electronic registration. No such possibility exists in the Italian and in the Hungarian systems. The Hungarian HIPO is considering the possibility of introducing an electronic deposit system in the future. On 15 December 2016, INPI launched the digital version of *e-Soleau*.⁹⁷

The private sector initiative operates online.

ii. Use of cryptographic methods

Cryptographic methods (such as electronic timestamps, postmarks, signatures and seals) are used by the Benelux i-DEPOT and by the publicly administered systems in place in France, Romania and in Spain. The details of these methods are not further specified in the answers to the survey.

I-DEPOT and the private sector initiative state that they comply with the conditions set by EU law regarding electronic signature, identification and trust services⁹⁸. As to the i-DEPOT, the

⁹⁶ In digital version, the certificate can be downloaded on the BOIP's portal, via the holder's account, or can be accessed in i-D Space if the depositor agrees to make the deposit completely publicly available.

⁹⁷ See the website of INPI about the e-Soleau: <https://www.inpi.fr/fr/services-et-prestations/e-soleau> (last accessed 31 January 2017).

⁹⁸ [Regulation \(EU\) No 910/2014/EU](#) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73-114, and Directive 1999/93/EC.

qualified certificate is delivered by a certification-service-provider. Any modification to the i-DEPOT certificate after the date of registration will automatically invalidate the certificate.

iii. Authentication of users

A form of ‘authentication’ of users takes place in several systems. This is mentioned in the survey replies from Romania, Portugal and Spain. The answers for Portugal mention that users are assigned a password. The exact details of the procedure are unclear. According to the website of the General IP Register in Spain, a digital certificate is required for an electronic deposit⁹⁹.

As to the Benelux i-DEPOT, no identity control is carried out as regards the users of the system. The digital version only requires the opening of an account on the BOIP online portal. The identity of the users of the French *enveloppe Soleau* is not checked, either.

On the private company’s website, internet users may search for works anonymously. For uploading content, users have to create an online account; during this process, only the email address is verified.

b. Requirements for filing requests for registration/deposit

i. Main mandatory information fields for filing the registration/deposit request

All systems studied require some information about the applicant. This is mentioned in the survey responses from France (name and address of the applicant); Hungary (name and address, and representative of the applicant); Italy, Portugal and Spain (personal details of the author/creator, of the rights holder and of the applicant if different); on the website of the Romanian Copyright Office (name and address, phone number and email address) and in the answers relating to the private sector initiative (author’s name).

Information about the type/genre of the work is required in Hungary, Portugal, Spain and by the private sector initiative. The survey responses in relation to Italy, Spain and the private sector initiative mention that the title of the work must be indicated.

The i-DEPOT tool only contains two mandatory fields: the title of the deposit, and the use of either the text field or an attachment or both; i-DEPOT does not control what is mentioned in the text field or what file is attached. The contents of the registration are left to the users’ discretion. The survey response highlights that it is in the users’ interest to make sure that they submit sufficient data in order to be able to use i-DEPOT as a functional and relevant means of evidence.

⁹⁹ See <https://sede.mcu.gob.es/rpi4/webpages/publico/certificado.seam> (last accessed 30 August 2016).

As to paper deposits/registration, several forms are available on the [website of the General IP Register](#). A photocopy of the identity card/passport is required for natural persons (note that not all available forms were checked).

In Italy, regarding the General Public Register, the relevant legal provision¹⁰⁰ sets out the mandatory elements that users must provide in the declarations and printed on the work. In addition to elements already stated, these include the publisher and the year of publication, but vary depending on the type of work.

In Portugal, further requirements depend on the type of work, and are mentioned in the relevant legal provisions¹⁰¹.

In Romania, various elements are required; the survey refers to the website of the Romanian IP office¹⁰². According to the website, applicants need to fill in 'Form No 24' (two copies), and provide a copy of the order of payment, in addition to one sample of the artistic creation to be registered (either electronically or on paper). The form does not appear to distinguish between trade marks and other types of IP rights. It consists in a declaration by the artist (or the artist's representative) in which they request registration of the work, provide a description of the latter, and declare that it is an original artistic creation.

In Hungary, further information enabling the unique identification of the work to be registered is required. Annexes may be attached if the author agrees to publication of the data contained in the form.

In Spain, other elements to be included are the type of intellectual property (the Spanish system registers the IP **rights**) and the date of disclosure, where applicable.

Registration/deposit with the portal of the private sector initiative requires information about both the user (name, family name, country, email and password) and the work (a file containing the work or an unequivocal description of it, with the possibility of adding a hash of the file containing the work; the type of work (e.g. music, photo, book, software); the title of the work; the user's relation to the work, (i.e. author, specific rights holder, etc.); and a declaration on the permitted use of the work (e.g. all rights reserved, Creative Commons). The information required is the same for all kinds of works; it mostly serves to classify and locate works. Additional information can be added.

ii. (Formal) examination of the information provided upon filing

Once filed, the information submitted by users is checked in the systems in place in Italy (regarding the General Public Register), Portugal and Romania. While the examination process is not further clarified in the survey responses, it seems that in most cases, it entails a formality check.

At the Italian General Public Register, an officer examines the applications upon receipt. The formal requirements of the law are checked; these vary according to the type of work and the

¹⁰⁰ Royal Decree No 1369 of 18 May 1942.

¹⁰¹ Article 24 of Decree Law No 143/2014.

¹⁰² <http://www.orda.ro/default.aspx?pagina=326> (last accessed 30 August 2016). The information is unavailable in English.

type of registration (e.g. original application for the registration of a work, registration of a transfer of rights, engineering projects or similar).

In Spain, applications are legally assessed by the IP Registry; that is, the registry checks carefully whether the application fulfils all the requirements set out in the relevant provisions of Spanish IP law. The IP Registrar's authority to assess applications is laid down in Spanish IP law¹⁰³. The IP Registrar checks whether the work, performance or production meets the necessary characteristics to be considered the object of IP protection, in addition to checking the legality of, for example, contracts submitted with the application for registration; moreover, the IP Registrar checks other legal elements such as the legal capacity of natural persons, legal representation, or the existence or not of legal entity.

In Hungary, the identity of authors or the entitlement of their representative is examined during submission of the request. There is no further examination of the work.

It can be assumed that personnel of the public authorities in charge of the respective registration/deposit systems handle the information submitted. However, this is not specified in the answers to the surveys. The Hungarian response notes that the Customer Services of the HIPO receive requests filed personally.

As regards the Benelux i-DEPOT and the French *enveloppe Soleau*, the information submitted is not examined. The BOIP notes that identification data for the portal account are not checked.

As to the private sector initiative, the filing process is fully automatic; no examination or assessment of the contents of individual applications takes place.

iii. Obligation of the registry/deposit to keep a fixed copy (in hard or digital form)

A fixed copy of the work (in hard or digital form) is kept by the Benelux i-DEPOT and by the registries/depositories in France, Italy (hard copies), Portugal, Romania and Spain (in the format in which it was supplied by the applicant, i.e. usually on paper and less often in digital format).

In the i-DEPOT, one of the two envelopes is kept at the Office for a period of 5 or 10 years in cases of registration of a paper version. A digital copy (file with qualified certificate) is kept at the Office for a period of 5 or 10 years in cases of electronic registration. Indefinite renewals/extensions for periods of 5 years are possible. In any event, i-DEPOT will remain valid as a means of evidence (even without renewal).

The Hungarian IP Office returns the certificate and the copy of the work (attached together) to the author or the author's authorised representative, and does not store them.

¹⁰³ See Article 145(2) of the Spanish IP code (TRLPI): El Registrador calificará las solicitudes presentadas y la legalidad de los actos y contratos relativos a los derechos inscribibles, pudiendo denegar o suspender la práctica de los asientos correspondientes. Contra el acuerdo del Registrador, podrán ejercitarse directamente ante la jurisdicción civil las acciones correspondientes.

In the private sector initiative, it appears that the artefact uploaded is always kept when a deposit is made. The situation is different when only the timestamper is used. The company pointed out that in certain cases, it is not necessary to deposit a hard/fixed copy of the entire work. For instance, in the case of films, users may also provide unique non-replicable information with, if possible, standardised numbers, or hashes of the files (as long as the user keeps a copy of the hashed file).

iv. Support for collections of works or versions of works

The systems in place in Hungary, Portugal, Romania and Spain, as well as the Benelux i-DEPOT and the private sector initiative offer users the possibility of organising their content.

Collections are supported by the Hungarian, Portuguese and Romanian systems, by the Spanish system (if they are filed in a single application and under the same title), and by the private sector initiative (in flat folders).

The deposit/registration of different versions is supported by the systems available in Portugal, Romania, Spain and by the private sector initiative. On the platform of the latter, different versions of a work or other subject matter may be deposited, whereby each version retains its own timestamp and attributes.

The survey on i-DEPOT simply states that ‘users can identify their i-DEPOTS with several references, allowing them to organise their works or relate i-DEPOTS with each other.’ Changes are envisaged for the public version of i-DEPOT¹⁰⁴.

c. Additional features of the system

i. Confidentiality of the content, restrictions on access and existence of a public search facility

The Benelux i-DEPOT, the French *enveloppe Soleau* and the Portuguese system are confidential. In these registration/deposit systems, only the rights holder(s) of the deposit can access the content deposited. The French survey replies mention that where necessary, a court may access the content of an *enveloppe Soleau*. As for i-DEPOT, with the launch of the public version, optional and possibly partial publication of information is now possible.

In Hungary, the certificate and the copy in the closed envelope can only be used for the purposes of proof; the seal and the envelope must be intact. Therefore, access to the work would entail loss of the legal effect attached to the certificate.

In Spain, with the exception of the content of the work or other subject matter, persons able to demonstrate a legitimate interest may be granted access to documents or receive certified copies of the records. In the case of works disclosed under a pseudonym, sign or anonymously,

¹⁰⁴ A public version of the system was launched at the end of 2016, that is, after the evaluation of the survey responses was finalised. The public version of i-DEPOT was therefore not examined in detail.

a direct interest must be demonstrated. As to computer programs, the only elements that can be consulted are those contained in the corresponding registration entry.

Register publicity of the Spanish IP Register is carried out upon a signed express request from an applicant. The applicant has to pay a fee, the amount of which is fixed by law. There is no general public search function.

The Italian registration/deposit system has public information purposes (General Public Register and Cinematographic Public Register). The General Public Register is public. Anyone can consult it and obtain a copy of the attached documents. The information on the recorded works is published on the administration's website (data from 1973 to 2015 are available). Citizens can search and print the results. Some personal data are not displayed in the public bulletin of deposited works.

In the private sector initiative, deposit holders decide on the confidentiality of the deposited elements. The whole registration/deposit may be kept confidential if the author so decides so; including attached files with contracts or other private information.

The survey responses about some of the registration/deposit systems studied indicate that certain bibliographical elements are publicly accessible (Hungary, if the author agrees; Romania; the private sector initiative).

In this context, note that a public search function is available in the systems in place in Hungary¹⁰⁵, Romania¹⁰⁶, and on the private company's website. The survey responses do not explain the details of the search function of the respective systems¹⁰⁷.

A public search function has been available for the public i-DEPOT since the end of 2016.

ii. Possibility of revocation or renewal of registration/deposit

Revocation of the registration/deposit is possible in the registration/deposit systems in place in Hungary, Portugal, Romania, Spain (by a declaration of invalidity of the act or contract recording the registered right and by confirmed court order) and in the private sector initiative (by deletion). According to the Benelux response to the survey, revocation should be possible in i-DEPOT as of August 2016.

Regarding renewal, it appears to be possible in France, Portugal, Romania and in the Benelux i-DEPOT. An i-DEPOT is registered (i.e. stored at the BOIP) for a period of 5 or 10 years. Non-extension of an i-DEPOT will not affect the validity of the latter as a means of evidence. One compartment of the French *enveloppe Soleau* (in physical form) is kept at the French INPI for a

¹⁰⁵ See the following website: <http://epub.hpo.hu/e-kutatas/?panel=Y> (last accessed 1 September 2016)

¹⁰⁶ A search window is available on the [website of the Romanian Copyright Office \(ORDA\)](http://www.ord.ro/)

¹⁰⁷ In Italy, information on works registered on two of the Italian registers can be found on the website of the online Bollettino [Bulletin] (<http://www.librari.beniculturali.it/it/diritto-dautore/bollettini/index.html> last accessed 11 August 2016). Nevertheless, a 'public search function', that is, the possibility of finding references to works/contents by typing some keywords, does not appear to be available.

period of 5 years, renewable once.

The surveys from Hungary, Italy and the private sector initiative report that registration/deposit only needs to be made once. The survey from Italy emphasises that ‘it is advisable to repeat the deposit process when substantive changes are made to works that have previously been deposited. Newspapers and magazines are outside the scope of this rule — they are required to deposit at least one copy a year.’

iii. Possibility of recording a transfer (of rights in the work/content registered/deposited)

Transfers of the rights in the content registered/deposited are not recorded by the systems in place in the Benelux countries (i-DEPOT), in France, in Hungary, and in Spain¹⁰⁸. The possibility of recording transfers is mentioned in the survey responses from Portugal, Romania, Italy (regarding the General Public Register, the Cinematographic Register and the Special Public Registry for computer programs)¹⁰⁹ and the private sector initiative.

The Benelux answer to the survey notes that the parties to a transaction could, for example, record the transfer of rights in a specific work in a separate i-DEPOT.

iv. Possibility of licensing the content

Of the systems analysed, the possibility of licensing content registered/deposited through use of the registration/deposit system is only mentioned by the private sector initiative and in the survey response from Romania. The private sector initiative offers a contract management feature that includes contract templates. Users can choose from over 200 licence types, available in different EU languages. Through the licences, which mostly appear to be similar to Creative Commons licences, registrants (rights holder(s)) can allow third parties to make certain uses of the work.

The Benelux answer to the survey notes that parties could record their transactions in a separate i-DEPOT.

d. Existence and amount of registration/deposit fees

Some type of fee is charged in all the registration/deposit systems studied.

The registration/deposit fee amounts to EUR 15 in France (for 5 years), to HUF 5 000 (around EUR 16.10)¹¹⁰ in Hungary, to EUR 29.80 in Portugal and to between EUR 10 and 100 in Romania. As to the Benelux i-DEPOT, a paper deposit costs EUR 45 (for 5 years) or EUR 65

¹⁰⁸ It should be noted that on the [website of the General IP Register](#), several forms (for paper deposits) are available. Some relate specifically to transfers of rights (e.g. transmisión de derechos inter vivos). There are also different forms for initial and successive registrations.

¹⁰⁹ See above, section 2.b.ii.

¹¹⁰ According to <https://www.oanda.com/currency/converter/> on 12 August 2016

(for 10 years). A digital i-DEPOT costs EUR 35 (for 5 years) or EUR 50 (for 10 years). It is possible to buy a credit account, which can reduce the fee to EUR 10 per i-DEPOT for 5 years. In Italy, revenue stamps and administrative charges are due for deposits in the General Public Register; there are fixed charges for the other two registers¹¹¹. In Spain, the amount of the fee depends on the Registry that deals with the request, and on the value of the service.

As to the private sector initiative, there is no registration/deposit fee; but a fee will be charged for producing evidence. It amounts to EUR 60 for up to 15 GB of stored content.

e. Statistical information

Participants in the survey were invited to provide data for at least the three previous years.

i. Number of registrations/deposits filed

	i-DEPOT (Benelux)	FR	HU	IT	PT	RO	ES	Private sector initiative
2006								
2007								
2008								
2009	4 093 i-DEPOTS (82 % electronic)							
2010								
2011	5 419 i-DEPOTS (89 % electronic)		5 041 works registered			231 387 (total No; exact time period unknown)		
2012			(16/04/2006-30/06/2016)				35 018	over 500 000 ¹¹²
2013	6 626 i-DEPOTS (94 % electronic)			around 19 200 registrations	2 770 registrations		35 489	
2014					2 767 registrations		33 492	
2015	5 945 i-DEPOTS (94% electronic)	28 043 (perforated envelopes)			2 381 registrations		Consolidated data not available	
2016								

Since 2007, the Benelux i-DEPOT service has received 1 297 requests for renewal (5-year extensions of storage period). The French INPI received 1 496 requests for renewal of an *enveloppe Soleau* in 2015.

¹¹¹ Information on fees is available on the website of the Italian CMO SIAE, <https://www.siae.it/en/about-us/siae/siae-and-its-history> (last accessed 12 August 2016).

¹¹² We understand that over 500 000 publicly accessible pieces of content have been deposited/registered. However, in reality the exact number may be higher.

ii. Number of requests for information filed

i-DEPOT (Benelux)	FR	HU	IT	PT	RO	ES	Safe Creative
No statistics	No statistics	Around 877 in 2015*	Around 1 200 per year (General Public register)	No statistics	Around 1.500 per year	> 2 000 per year**	No statistics

* The Hungarian answer to the survey specifies that the Customer Service and the Copyright Department of the HIPO provided information about the voluntary register of works in 877 cases in 2015.

** The Spanish answer to the survey notes that there are around 400 applications for disclosure per year.

iii. Main characteristics of the users

1) Geographical characteristics

The answers to the survey from Hungary, Italy,¹¹³ Portugal, Romania and Spain report that all or the great majority of users of the respective public registration/deposit systems are nationals of the respective Member State. Altogether, 98 % of i-DEPOTs belong to Benelux users. Nevertheless, the report stresses that i-DEPOT has users from more than 65 countries around the world (within and outside the EU, e.g. Canada, Hong Kong, Singapore). Since registration/deposit of content via an *enveloppe Soleau* is confidential, the French INPI cannot provide any information about users of the system.

According to the data provided by the private sector initiative, a very large number of users are from Spain; however, the Spanish-based company also has users in the other 27 EU Member States as well as, for example, in the US, Australia, Canada, Russia or in various other countries in Latin America, (North) Africa, Asia, and non-EU states in Europe. It was noted that the percentage of non-Spanish users is increasing.

2) User groups

Although information on the characteristics of users is not available in some systems, it appears that the systems studied are used by individuals as well as by companies.

According to the survey responses, the Italian General Public Register is used by authors, publishers, producers (SMEs and large companies). The vast majority of users of the Spanish

¹¹³ The Italian system appears to address Italian authors or authors of works first published in Italy.

public register are individuals; around 5 % of the users are legal persons.

It appears that mainly individuals and SMEs use the private sector initiative.

iv. Statistics or anecdotal evidence about the number of court cases in which the evidence submitted to the system has been used

The answers to the survey on the public registration/deposit systems in Benelux (i-DEPOT), France, Hungary, Italy, Portugal and Spain state that there are no statistics on this question.

The Romanian answer to the survey reports that there were 170 court cases in which the evidence submitted to the system has been used. According to i-DEPOT, lawyers and other users have reported such cases. According to the answer to the survey on the Portuguese public registration/deposit system, courts often turn to the General Inspection for Cultural Activities (IGAC) for information on registration. The private sector initiative reported one court case for which their current system provided evidence¹¹⁴.

¹¹⁴ Trade Court of Logroño. Case 1240/2010, No 10/2011 (3 February 2011).

ANNEX II: QUESTIONNAIRE ON REGISTRATION/DEPOSIT SYSTEM(S)

Questionnaire on Registration/Deposit System(s) in your Country

Institutional questions

QUESTIONS	ANSWERS
Information about existing IP registration/deposit system(s) managed by a public institution	
Do you have information about an existing IP registration/deposit system in your country managed by a public institution?	
If yes, what is the name and legal status of the registration/deposit body? Please provide details of a contact person for additional information.	
Information about existing IP registration/deposit system(s) managed by a private entity	
Do you have information about private entities that provide an IP registration/deposit service?	
If yes, what is the name and legal status of the registration/deposit body? Please provide details of a contact person for additional information.	

Legal questions

QUESTIONS	ANSWERS
Legal basis for a registration/deposit system	
Is there a legal basis for a registration/deposit system in your country?	
If yes, please provide relevant legal act(s) and norm(s) in that respect.	
IP-related content that can be registered/deposited	
What kind of IP-related content can be registered/deposited in your country?	
Is the registration/deposit process different for various types of content?	
If yes, please describe the differences.	
Legal effect of registration/deposit	
Does the registration/deposit establish a presumption of authorship/ownership?	
Does the registration/deposit system provide evidence of the date of creation or invention?	
Do the courts recognise the registration/deposit in relation to dating evidence?	
Any other legal effect or benefit of the registration/deposit system?	

Liability issues	
How are liability issues dealt with in case of a dispute between a user of the system and a third party, e.g. for the date on the evidence?	
Is there, for example, a mediation procedure?	
Are there potential liability issues linked with the administration of the system?	
Can a third person ask for the disclosure of any deposited elements or is such an eventuality expressly excluded by the law?	

Technical questions

QUESTIONS	ANSWERS
Electronic registration/deposit system	
Is there any electronic registration/deposit system in place or in the course of being established?	
If yes, is the system designed using cryptographic methods, such as electronic timestamps, signatures and seals?	
Are the users of the system being authenticated? If yes, by what means?	
Requirements for filing the registration/deposit requests	
What are the main mandatory information fields required to file the registration/deposit request?	
Is the information examined upon filing?	
Must a fixed copy (in hard or digital form) be kept at the registry/deposit?	
Is there support for collections of works or versions of works?	
Additional features of the system	
Is there a public search facility?	
Are there any restrictions for accessing the content?	

Are the deposited elements kept confidential? Are some bibliographical elements concerning the deposit published?	
Is there a possibility for a revocation or a renewal of registration/deposit?	
Is there a possibility to record a transfer of the content?	
Is there a possibility to license the content?	
Registration/deposit fee	
Is there a registration/deposit fee?	
If yes, how much is the fee?	
12. Statistical information (please provide data for at least the last 3 years)	
12.1. What is the number of registrations/deposits filed?	
12.2. What is the number of requests for information filed?	
12.3. What are the main characteristics of the users (national, European, international)?	
12.4. Is the system used by individuals (authors, inventors, creators), representatives or businesses (SMEs or large companies)?	
12.5 Are there statistics regarding the number of court cases in which the evidence submitted to the system has been used? Where there are no statistics as such, is there anecdotal evidence about such use?	

ISBN 978-92-9156-250-3 doi:10.2814/666851 TB-04-18-147-EN-N

© European Union Intellectual Property Office, 2018

Reproduction is authorised provided the source is acknowledged

Avenida de Europa 4

E-03008 – Alicante

Spain



FEASIBILITY ANALYSIS FOR AN EU DIGITAL DEPOSIT SYSTEM