D5.7

Cross-Border Legal Compliance and Validity of Delegation (2)

Document Identification	
Date	30.08.2019
Status	Final
Version	1.1

Related WP	WP 5	**Related Deliverable(s)**	D2.10, D6.7, D5.2, D5.6
Lead Authors	Hans Graux (TIL), Edwin Jacobs (TIL)	**Dissemination Level**	PU
Lead Participants	TIL, OIX	**Contributors**	TIL
Reviewers	OIX, USTUTT		

This document is issued within the frame and for the purpose of the LIGHT*est* project. LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No 700321.

1. Executive Summary

The central objective of LIGHTest is to create the tools to use a global trusted communications mechanism – the DNS – for the discovery, validation and translation of certain trust information. This trust information in the context of LIGHTest principally relates to trust policies, i.e., a recipe that takes an electronic transaction and potentially multiple trust schemes, trust translation schemes and/or delegation schemes as input and creates a single Boolean value (trusted [y/n]) and optionally an explanation (e.g., why not trusted) as output (source: D2.1 – Inventories). Broken down to the simplest terms, a trust policy contains the rules to decide whether a transaction can be trusted or not.

One of the goals of LIGHTest is also to permit the discovery and validation of delegations, as a part of such transactions. As explained in detail in D5.2 – Conceptual Framework for Delegations (1), this will be done via so-called Delegation Publishers and Delegation Providers. The Delegation Publisher operates an off the shelf DNS server with DNSSEC extensions turned on, with DNS records pointing to delegation information. This substantive delegation information is stored by the Delegation Provider in a standardised format. The Delegation Provider provides a signed list that proves the claim of a proxy to act on behalf of a mandator. The list can be used to publish different delegation types. In practical terms, the Delegation Provider can be thought of as a repository of delegations, and the Delegation Publisher as the discovery component.

Within LIGHTest, several types of delegations can be modelled. In each case, a person – a mandator – has given a certain authority to act on his/her behalf to another person, the proxy. Conceptually, delegations can include person-to-person representations (mainly contractual delegations, i.e. one person granting someone the legal authority to represent them for certain aspects in certain contexts), company representations (discovering who can represent a legal entity), or even statutory mandates (granted by law, such as the power to represent one's children). In practice, LIGHTest is currently expected to only pilot the former two (contractual mandates and company representations), excluding statutory representations.

Each of these types of delegations has specific legal challenges, including the identification of the parties, the definition of the delegation, the determination of the integrity and authenticity of the parties, its limitations in terms of scope and time, and its legal reliability (i.e. the extent to which a third party can reasonably depend upon it).

While some types of delegations have a clear legal background, this is not universally the case, and the legal framework is largely unharmonized at the EU level. By way of examples of this lack of harmonisation and the resulting legal challenges in relation to the two types of delegations within the scope of LIGHTest:

- Legal requirements for the creation of a contractual delegation can differ from country to county: in some cases signatures may be a constitutive requirement without which a mandate cannot exist, whereas in other cases informal mandates need not even be in writing. The question of whether a delegation requires only a signature from the mandator or also an explicit acceptance from the proxy is similarly dealt with differently from country to country. And for some types of contractual mandates, specific formalities such as notarisation or registration will be required.
- Similarly, the powers to represent a company will depend on the type of company, the type of representative, the transaction involved, and of course the country; neither the concepts nor the substantive rules are harmonised at the EU level. Furthermore, articles of association in a company can change the default rules enshrined into law (e.g. by requiring multiple signatures for transactions above a certain threshold).
- And of course, there is an overlap between both of the aforementioned categories: a company may give a contractual mandate to e.g. a third party to manage its taxes, payroll, social security requirements, asset management, etc; this is technically a contractual delegation falling within the first category described above, but its validity will be determined by company representation powers in the second category above.

Rules for transactions can be defined in a very ad-hoc and context specific manner, varying from country to country. A generic legal framework for the discovery and validation of delegations must therefore be created within LIGHTest that allows this variety to be captured.

In a first version of this deliverable (D5.6 – Cross-Border Legal Compliance and Validity of Delegation (1)), which was produced in the first year of the project, we explored the legal challenges in relation to the discovery and validation of delegations via the DNS. This first version explained how within the LIGHTest project, and more broadly in relation to the LIGHTest technology, we can create a legal solution that allows users of the LIGHTest technology to provide acceptable legal certainty in providing trustworthy delegation information. In practical terms, as will be explained below, these will be addressed principally through assurances from the Delegation Provider, which stores the delegation information in a standardised form. The Delegation Provider, as the substantive source of delegations, will be tasked with ensuring that the delegations which it stores and makes accessible are valid and trustworthy, at least for certain purposes and contexts.

In any use case, a relying party should have sufficient legal guarantees that the delegation information originates from a known and identifiable Delegation Provider. The relying party will not necessarily be able to identify what the legal framework in relation to a specific delegation was (especially for delegations which are subject to foreign law), but it will be able to find the Delegation Provider that originated the delegations. This implies that, if the Delegation Provider is required to

publish the assurances that it provides in relation to the delegations that it makes available via LIGHTest, relying parties have a viable avenue for making trust decisions.

This approach is capable of addressing the main legal challenges that were already identified in deliverable 5.6, and which can be summarised as follows:

- **Integrity and authenticity can be provided by the fact that the Delegation Provider electronically signs the delegations** that it makes available to third parties. This provides integrity (in the sense that relying parties can determine that the information was not corrupted after the signing by the Delegation Provider) and authenticity (in the sense that relying parties can determine that the delegation information originated from the Delegation Provider).
- **The scope of delegations can be standardised and defined precisely by each Delegation Provider.** This is a viable approach, since it is likely that any Delegation Provider will deal with only a relatively narrowly defined context of delegations. The scoping in each context can be standardised and defined on a case by case basis, in a way that is logically understandable, consistent and reasonably complete for the Delegation Providers and the third parties that it wishes to assist.
- **The compliance and legal recognition burden can be more easily shouldered by the Delegation Provider,** since it will know the complexities of its delegations and the applicable rules. The Delegation Provider will need to determine itself whether the delegations that it makes available are legally valid, and communicate its assurances on this point to relying parties.
- **Finally, the trustworthiness of the delegations can be addressed in the same way: the Delegation Provider can and must communicate to third parties which assurances (if any) it provides in relation to the delegation information that it makes available.**

This approach is pragmatic, and essentially has one key legal characteristic: the information that the Delegation Provider offers (the electronic mandate) should not be considered as the delegation as such, but rather as an electronic assertion from the Delegation Provider that a delegation exists that meets the description of the electronic assertion.

The strength of this approach is that it can be applied in any use case, for any delegation in a global context, which is a key objective of LIGHTest. In this approach, legal value and validity is to some extent dependent on the procedures of the Delegation Provider, their willingness to provide assurances on this point, and the ability of third parties to correctly appreciate these assurances. It does not solve more fundamental questions, such as e.g. whether the correct signatures have been applied to the delegation, and whether its validity under applicable law can be determined. This is however not a fundamental problem, nor a weakness: the objective of LIGHTest is not to harmonise laws and practices for the creation of delegations – indeed, that would be a task far beyond the ability of a project such as LIGHTest - but rather to enable the use

of the DNS for the discovery and validation of existing delegations. The delegations as such must validly pre-exist before they can be discovered and validated through the LIGHTest infrastructure.

The present deliverable, which is an updated version of D5.6, provides the tools for establishing this legal solution, in the form of a standardised legal document that can be used by a Delegation Provider when making delegation information available as a service to a LIGHTest user. While this standardised legal document – in effect a template terms and conditions document – must be tailored to each context and to each use case, this deliverable also provides guidance on which choices need to be made, what the principal legal challenges are, and how they can affect the drafting of final terms and conditions in real life use cases.

As with the first version of the deliverable, this document too is a part of a quartet of legal deliverables in LIGHTest that should be read collectively. While the background of each legal deliverable is the same, each deals with a specific aspect of a legal challenge in LIGHTest. Notably:

- D3.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Publication explains the legal challenges behind the **publication of trust schemes**, including data protection assurances and the need for a trust framework (through laws or contracts) that explains the legal assurances and guarantees behind the publication.
- D4.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Translation explains the legal challenges behind the **translation of trust schemes**, including the need to publish terms under which the translation can be done (via a law or treaty, or simply via a contract).
- D5.7 - Cross-Border Legal Compliance and Validity of Delegation explains the legal challenges behind creating and managing **delegations**, including the focus on data quality (creation, validation, keeping it up to date, and liabilities behind it).
- D6.8 - Cross-Border Legal Compliance and Validity of Trust Policy and Trust Decisions explains how this infrastructure is used in practice to support **decision making**.

Since the background of each deliverable in this quartet is the same, the general sections (Chapter 4 and 5 of the deliverables) will be identical, whereas the specific challenges for each topic are commented in Chapter 6. References to relevant sources are reprised in section 7. While this creates significant duplication in the content of the deliverables, it also ensures that the deliverables can be read and understood as stand-alone documents.

2. Document Information

2.1 Contributors

Name	Partner
Hans Graux	TIL
Edwin Jacobs	TIL
Michelle Parks	OIX
Sven Wagner	USTUTT

2.2 History

Version	Date	Author	Changes
1.0	26.07.2019	TIL	Draft for review
1.1	28.08.2019	TIL	Final version after internal review

3. Table of Contents

3.1 Table of Figures

3.2 Table of Tables

4. Legal compliance and validity within LIGHTest in general

4.1 Understanding LIGHTest

The central objective of LIGHTest is to create the tools to use a global trusted communications mechanism – the DNS – for the discovery, validation and translation of certain trust information. This trust information in the context of LIGHTest principally relates to trust policies, i.e., a recipe that takes an electronic transaction and potentially multiple trust schemes, trust translation schemes and delegation schemes as input and creates a single Boolean value (trusted [y/n]) and optionally an explanation (e.g., why not trusted) as output (source: D2.1 – Inventories). Broken down to the simplest terms, a trust policy contains the rules to make a decision on whether a transaction can be trusted or not.

Trust schemes and trust decisions can take many forms and cover many topics, and the legal framework that applies to these – including the liberty that parties have for making a trust decision – can vary from case to case. To give a few examples:

- A relatively simple trust decision that LIGHTest will support is validating whether a trust service provider (i.e. the provider of services in relation to electronic signatures, electronic seals, time stamps, electronic registered delivery services, or website authentication) complies with the legal rules of the eIDAS Regulation, and more specifically whether the service providers are qualified or not. The rules (and indeed the entire trust scheme) in relation to this decision are captured in law, notably in the eIDAS Regulation (EU) No 910/2014[1]. The trust policy is therefore simple, and consists of the rules of the eIDAS Regulation which act as the trust scheme. The trust decision is correspondingly simple, and consists of an assessment whether the provider complies with the requirements of the eIDAS Regulation (which are explained in D2.10 in greater detail). The law (namely the eIDAS Regulation) is relatively comprehensive on this point, and the decision is a relatively straightforward yes/no decision: a provider complies or it does not. No notable margin of appreciation exists.
- In realistic cases, business decisions can be much more complex. If a company receives an electronically signed document – e.g., an order for a product or service – it can create its own rules (its own trust scheme) on how it will assess the validity of these orders. These

[1] 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, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

rules constitute the trust scheme, and the resulting decision – do I accept the order or not? – is the trust decision. The presence of an electronic signature and whether it complies with the eIDAS Regulation can be a factor. Other elements may be whether the customer is known, the size of the order, its place of establishment, etc. Laws do not answer all of these questions: while there are rules on what constitutes a lawful order, individual preferences and choices can play a role. Indeed, a company may simply have a rule that it doesn't accept electronic orders at all, for whatever reason, or that it only accepts electronic orders which are signed using signatures from a local trust service provider. Such policies (and the resulting trust decisions) may be objectively irrational or illogical, but none the less they can exist.

- Finally, there are cases where trust policies and trust decisions are entirely determined by the participants in a transaction or business relationship, without any significant impact from legislation. By way of example, a European trade association may have its own internal rules on which companies are permitted to join. These are likely to include rules on business activities, place of establishment or business, membership fees, and adherence to codes of conduct. The trade association may decide to publish membership, so that its members can make trust decisions on that basis (do I know that this company is indeed a member of this trade association)? The rules of membership are then the relevant trust policy, and the members can take their own trust decisions on the basis of the information made available by the trade association – which may or may not be covered by any legal assurances from the trade association, depending on its own trust policies.

The examples above serve to make a central challenge clear: LIGHTest is a technology that can be applied to a nearly unlimited range of use cases, with vastly diverging legal and policy challenges. In these situations, there is no 'one-size-fits-all' approach that ensures that the technology is automatically compliant with legal requirements and with the trust policies that parties may have defined on a case-by-case basis.

The same observation applies also to the topic of delegation, which can exist in many shapes and forms, each of which are subject to different legal requirements. One need only consider a contractual delegation to go shopping for groceries on behalf of a person, to buy a house on behalf of that person, or to vote in national elections on behalf of that person. Depending on the context and country, the delegation may be simple and straightforward – an oral agreement suffices – or highly complicated, requiring signatures from both parties which are certified and registered by a trusted third party such as a notary. In other contexts, it may not even be possible to issue a legally valid delegation at all (e.g. giving a mandate to vote to a person who is not qualified).

LIGHTest aims to use the same infrastructural model for the discovery and validation of all such delegations. Given that legal requirements vary from use case to use case, it is clear that LIGHTest

cannot ensure that trust decisions made using LIGHTest technology are automatically legally valid without any further customisation or tailoring, or without validating whether the use case is legally viable to begin with. The technology itself cannot ensure legal validity; it must be used in a way that complies with legal constraints. The technology can support this, but ultimately a broader legal superstructure is needed, in the form of contracts and policies that are tailored to each specific use case.

LIGHTest's approach to legal compliance and legal validity is therefore based on ensuring transparency to its users (i.e. those that publish trust schemes, those that conduct trust translations or verify delegations, and those that make trust decisions on the basis of the policies), and providing a set of standardised legal tools to ensure that LIGHTest can indeed be deployed in specific use cases with appropriate consideration for their individual specificities.

4.2 What can LIGHTest deliver from a legal perspective?

LIGHTest is first and foremost a pilot project, and therefore needs to work within the confines of existing law; it is not viable to assume that legislation would be changed in the course of LIGHTest to meet the objectives of the project. This observation is of course trivial, but has some repercussions for the piloting, notably in relation to eIDAS compliance.

As is explained in D5.2 in detail, part of the piloting of LIGHTest consists of integrating certain delegation information into the DNS, through a mechanism of references. This will be done from an infrastructural perspective via so-called Delegation Publishers and Delegation Providers. The Delegation Publisher operates an off the shelf DNS server with DNSSEC extensions turned on, with DNS records pointing to delegation information. This substantive delegation information is stored by the Delegation Provider in a standardised format. The Delegation Provider provides a signed list that proves the claim of a proxy to act on behalf of a mandator. The list can be used to publish different delegation types. In practical terms, the Delegation Provider can be thought of as a repository of delegations, and the Delegation Publisher as the discovery component.

Conceptually, D5.2 provided the following graphical overview, showing the logical place of delegation in the validation of a transaction through LIGHTest:

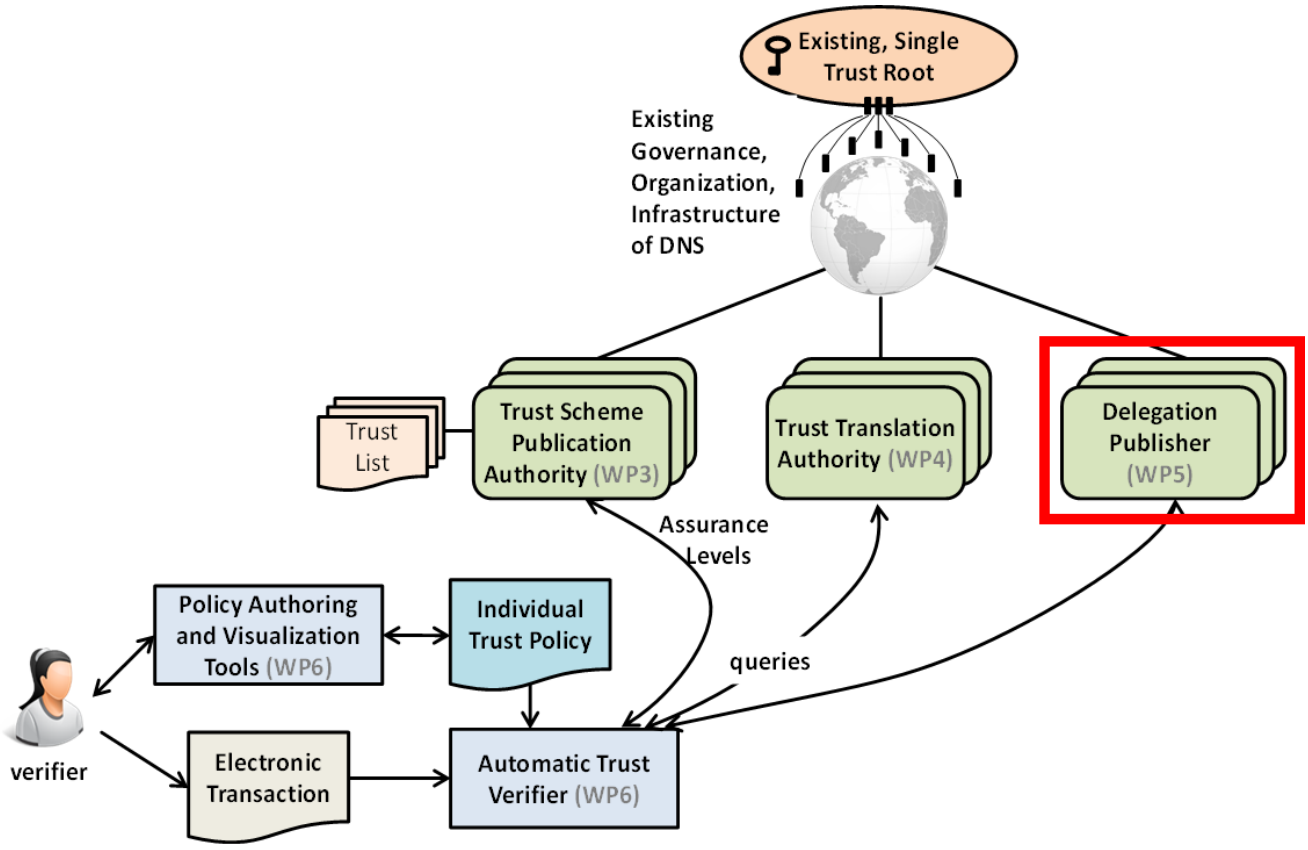

Figure 1: Delegation Publisher location in LIGHT^{est} - source: D5.2

Within LIGHTest, several types of delegations can be modelled. In each case, a person – a mandator – has given a certain authority to act on his/her behalf to another person, the proxy.

Conceptually, delegations can include person-to-person representations (mainly contractual delegations, i.e. one person granting someone the legal authority to represent them for certain aspects in certain contexts), company representations (discovering who can represent a legal entity), or even statutory mandates (granted by law, such as the power to represent one's children). In practice, LIGHTest has only piloted the former two (contractual mandates and company representations), excluding statutory representations.

Each of these types of delegations has specific legal challenges, including the identification of the parties, the definition of the delegation, the determination of the integrity and authenticity of the parties, its limitations in terms of scope and time, and its legal reliability (i.e. the extent to which a third party can reasonably depend upon it).

While some types of delegations have a clear legal background, this is not universally the case, and the legal framework is largely unharmonized at the EU level. By way of examples of this lack of harmonisation and the resulting legal challenges in relation to the two types of delegations within the scope of LIGHTest:

- Legal requirements for the creation of a contractual delegation can differ from country to county: in some cases signatures may be a constitutive requirement without which a mandate cannot exist, whereas in other cases informal mandates need not even be in writing. The question of whether a delegation requires only a signature from the mandator or also an explicit acceptance from the proxy is similarly dealt with differently from country to country. And for some types of contractual mandates, specific formalities such as notarisation or registration will be required.
- Similarly, the powers to represent a company will depend on the type of company, the type of representative, the transaction involved, and of course the country; neither the concepts nor the substantive rules are harmonised at the EU level. Furthermore, articles of association in a company can change the default rules enshrined into law (e.g. by requiring multiple signatures for transactions above a certain threshold).
- And of course, there is an overlap between both of the aforementioned categories: a company may give a contractual mandate to e.g. a third party to manage its taxes, payroll, social security requirements, asset management, etc; this is technically a contractual delegation falling within the first category described above, but its validity will be determined by company representation powers in the second category above.

Rules for transactions can be defined in a very ad-hoc and context specific manner, varying from country to country. A generic legal framework for the discovery and validation of delegations must therefore be created within LIGHTest that allows this variety to be captured, keeping into account that, in the absence of international legal harmonisation on this point, legislation will remain different from use case to use case and from country to country, and that LIGHTest as such therefore won't be able to affect the legal validity of a delegation itself, since this is determined by binding law. Instead, it must be capable of providing sufficient assurances that delegations which are discoverable, and which can be validated via LIGHTest comply with the needs of a relying party's use case.

The result is that delegation models applied by LIGHTest can be used in practice in a legally reliable manner, but only on a contractual basis. This deliverable describes how such a contractual framework can be established by a Delegation Publisher and a Delegation Provider, and what the challenges, opportunities and risks are. In the chapters below, we will examine:

- What the implications are of using the DNS to support the discovery of trust schemes and the making of trust decisions (Chapter 5). Specifically, this chapter will provide an analysis

of the governance assurances behind the DNS, in order to substantiate the appropriateness and robustness of this technology as a conveyor of trust information.

- What the legal tools are that LIGHTest uses to run its pilots (Chapter 6), and how these can be applied be interested users after the termination of the LIGHTest project by third parties for use cases that will not be piloted in LIGHTest itself, in any of the myriad of use cases that are listed in D2.3.

Collectively, this will demonstrate that LIGHTest can be relied upon from a legal perspective as well, and that LIGHTest as a technology can also be readily deployed in use cases where specific technological choices are not determined by law. In the longer term, it would also be possible for LIGHTest as a technology to become a common tool for mapping delegations in official databases, through changes in legislation that ensure that the information made accessible through LIGHTest is considered as authoritative.

5. Understanding the Domain Name System

5.1 Introduction to the genesis of the DNS

In its early days, Arpanet, the research network that would eventually evolve into today's Internet, was small enough that each node could maintain a database giving human-readable names to all the nodes it would need to communicate with. Over time, this database, a simple text file named HOSTS.TXT, became centrally maintained. Each node would retrieve updated versions as they became available. With the network growing quickly, however, the file became large, making updates expensive and slow. On the other hand, dealing with the constant flow of requests for new names and updates developed into an administrative nightmare.

As a response, Paul Mockapetris devised the Domain Name System, or DNS for short. Its initial specification was published via the Internet Engineering Task Force as a pair of documents, RFC 882 and RFC 883, in November 1983. In general terms, the system provides a network service that eliminates the need for an exhaustive central registry, thereby also eliminating the related administrative issues. Instead, the system mirrors the distributed nature of the Internet as a network of interconnected networks. It allows each participating network to set up, configure, and operate their own name resolution service and provides means for discovering and query these independent services. (Introduction cited from D2.7 DNSSEC Expertise and Building Blocks).

5.2 Conceptual framework

The DNS is more or less the Internet equivalent of a phone book. The DNS maintains a directory of all domain names and translates these into IP addresses, and/or provides other information related to the domain names.

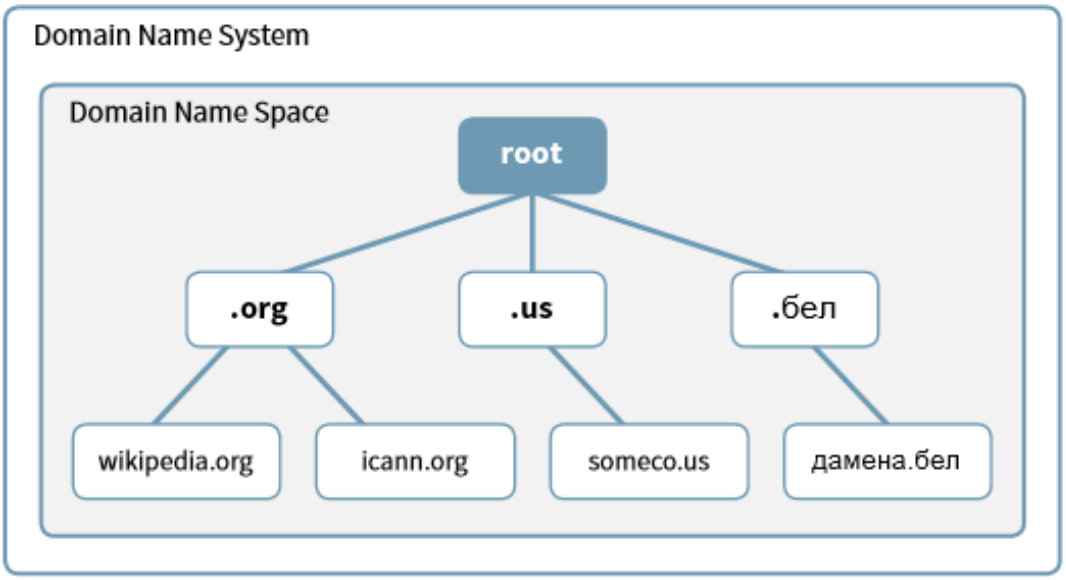

Figure 2: Domain Name System – Source: https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf

Information relating to all top-level domains is housed at a central registry coordinated by ICANN. Host companies and ISPs interact with this central registry to get updated DNS information in a cached model: the central registry can point them to a relevant DNS server for any given top-level domain, which in turn will be able to provide IP addresses of subdomains.

As an example of the usage of the DNS, when an individual types in a website address, his or her ISP will query the name servers, starting from the hard coded root servers (shown in blue in Figure 2) if the information is not locally cached by the ISP, to find out which name servers are associated to that domain name. One of those name servers is then contacted and will return the IP address for that domain name. The individual's computer can now connect to the computer that will serve up the requested website's homepage[2].

To examine this process in slightly greater detail: when an Internet user types a web address into a browser (or otherwise uses the DNS, e.g. for sending e-mails), the browser sends a query over the Internet to the DNS to find the website. The first server the query interacts with is the 'recursive

[2] For a more detailed overview, see https://whois.icann.org/en/dns-and-whois-how-it-works

resolver', which can be operated by the user's ISP or by a third-party provider. The 'recursive resolver' knows which other DNS servers it needs to ask to answer the original domain query.

The first DNS server the 'recursive resolver' talks to is a root server. The root servers run globally and each one knows DNS information about Top Level domains such as .com. The 'recursive resolver' asks a root server for DNS information about .com. There are 12 sets of root servers in more than 300 locations around the world. DNS ensures that any query will be sent to a server that isn't too far away from the user, in order to minimize response times.

Each Top Level Domain (TLD) DNS name server stores the address information for second level domains (e.g. parkesmarketing.com) within the top level. When a query hits the TLD server, the TLD server answers with the IP address of the domain's name server.

The 'recursive resolver' sends the query to the domain's name server. This DNS server knows the IP address for the full domain and that answer is returned to the 'recursive resolver'.

The 'recursive resolver' tells the browser which IP address should be targeted for a given website, and the browser can send a request to the relevant IP address to retrieve the website's content.

5.2.1. Root Name Servers

For the DNS to work, servers are required that respond to the queries that initiate the transaction between domain names and the values associated with those names. The servers are called Root Servers and form an important part of the DNS. They are located all over the world and are operated by 12 different organizations.

5.2.2. Trust Anchors

To prove that a DNS answer is correct, the DNS Security Extensions (or DNSSEC) provide a method to digitally sign DNS data. The keys necessary for verifying signatures are stored in the DNS itself. As a starting point for verification, at least one of these keys, called a trust anchor, needs to have been obtained from other means, such as the operating system or another trusted source. These starting points are called trust anchors, and are obtained from the operating system or another trusted source.

A significantly detailed document, the DNSSEC Practice Statement for the Root Zone Key Singing Key (KSK) Operator[3], outlines the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution Services that include at least the issuing, managing, changing and distributing DNS keys.

5.3 Relevant governance bodies of the DNS

5.3.1. Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN "oversees the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another".[4] The objective is universal resolvability, meaning that an Internet user obtains the same predictable results wherever he or she is located in the world.

Main role of ICANN

- ICANN coordinates unique IP addresses globally so we can have one global Internet. It coordinates the role of the Internet's naming system and has a role in the expansion and evolution of the Internet.
- One of ICANN's roles is to draw up contracts with domain name registries and runs an accreditation system for these registrars. These contracts provide a consistent and stable environment for the domain name system, and ensure that a common legal underpinning of the DNS is available and applied consistently.
- ICANN also helps coordinate how IP addresses are supplied to avoid repetition or clashes. ICANN is the central repository for IP addresses and these ranges are then supplied to regional registries who then distribute them to network providers.
- ICANN assists in the maintenance of the root servers that act as a main index to the Internet's address books. Root servers ensure the smooth functioning of the Internet and ICANN makes sure the system stays up to date.

[3] See https://www.iana.org/dnssec/icann-dps.txt
[4] See https://www.icann.org/resources/pages/what-2012-02-25-en

ICANN decision making

Suggested changes to existing network protocols can be raised by one of ICANN's supporting organisations and are followed by a report by an advisory committee. A report is then put out for public review. The ICANN board is provided with a report with discussions and recommendations. Either the changes are approved or rejected, with explanation given as to what needs to be resolved before approval.

5.3.2. IANA (Internet Assigned Numbers Authority)

The IANA is a department of ICANN which is responsible for three core tasks[5]:

1. Protocol assignments: in co-ordination with the IETF (Internet Engineering Task Force), protocol assignments are managed by maintaining the codes and numbers used in Internet protocols.
2. Internet Number Resources: this includes global co-ordination of IP (Internet Protocol) addresses and allocating ASNs (autonomous system numbers) to Internet registries, regionally.
3. Root Zone Management: top-level domain assignment to the operators for domains such as .uk and .com are key management activities as well as maintaining administrative and technical details. Authoritative records of all top-level domains are contained in the root zone.

ICANN provides forums and other development processes to develop the consensus-based policies that define how the IANA functions are performed, that organisations representing the global Internet community use. At the time of writing, the United States Department of Commerce's National Telecommunication and Information Administration (NTIA) plays a key role as a steward of ICANN's performance of the IANA functions. Other organisations representing the global Internet community also have stakeholder responsibilities, often defined via written agreements with ICANN.

[5] Full details about what ICANN does and doesn't do in its performance of the IANA functions are clearly defined in this document: https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf

ICANN controls the root zone through the IANA. The IANA function operates and maintains the root zone and the .int and .arpa domains.

The root is the upper-most part of the DNS hierarchy. IANA evaluate requests to change operators of country code domains as well as day-to-day maintenance of the details of the existing operators.

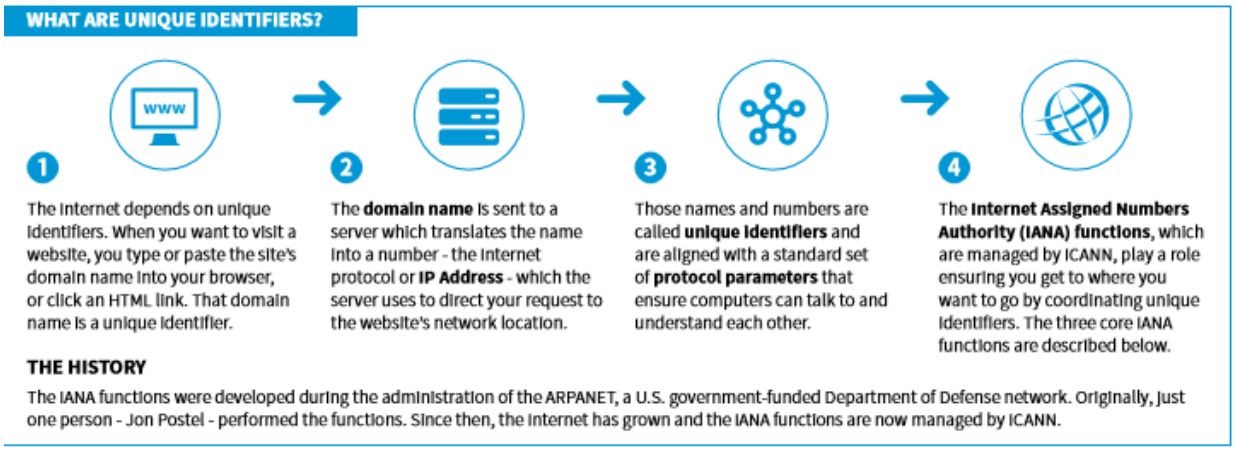

Figure 3: Understanding unique identifiers[6]

Multiple bodies within the ICANN policy development framework provide input into the policies used to manage the root of the DNS. For TLDs, the ccNSO (Country Code Names Supporting Organisation) and GNSO (Generic Names Supporting Organization) provide global-level policy recommendations to be applied to the management of ccTLDs and gTLDs in the root, respectively. These policies are created using open policy development processes.

Advice on the technical management and configuration of the root is provided by a variety of different communities, including the ICANN Root Server System Advisory Committee (RSSAC) and the ICANN Security and Stability Advisory Committee (SSAC).

ICANN's other two Advisory Committees (the At-Large Advisory Committee and the Governmental Advisory Committee) consider and provide advice to the ICANN Board on policy matters. Open consultation is also used to engage industry experts and operators in activities such as developing the parameters by which Domain Name System Security Extensions (DNSSEC) were implemented in the root.

[6] Source: http://www.corporateassistance.asia/the-iana-functions-explained-new-icann-infographic/

5.3.3. Regional Internet Registries (RIRs)

There are five different global RIRs which are not-for-profit, membership based organisations that operate in different regions. Each RIR will distribute the Internet number resources allocated to network operators across its region. The allocation and assignment polices are defined by its own regional community. Each RIR community is open to all and anyone can take part in the policy development process.

- African Network Information Centre (AFRINIC) - Africa
- American Registry for Internet Numbers (ARIN) – US, Canada, some Caribbean and Antarctica
- Asia-Pacific Network Information Centre (APNC) – Asia, Australia, New Zealand
- Latin America and Caribbean Network Information Centre (LACNIC) – Latin America parts of Caribbean
- Reseaux IP Europeens Network Coordination Centre (RIPE NCC) – Europe, Russia, Middle East, Central Asia

As required under ICANN rules, *"an identical version of a global policy proposal must have consensus from all five of the RIR communities before it can be recommended for ratification, and then implemented by ICANN."*[7] Thus, some form of global governance is present behind the DNS.

5.3.4. Number Resource Organisation (NRO)

The Number Resource Organisation (NRO) unites all the RIRs in order to undertake joint activities such as technical projects and policy co-ordination.

The main aims are:

1. Protect the unallocated IP number resource pool
2. Promote and protect the bottom-up policy development process of the internet
3. Act as a focal point for Internet community input into the RIR system

5.3.5. Internet Engineering Task Force (IETF)

[7] See https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf

The IETF holds the technical stewardship of all technical standards of the Internet, of which DNS is only one. The IETF can be described as an international open community of network designers, operators, vendors and researchers. Technical work is carried out through working groups and the IETF holds meetings three times a year across global locations. There are also informal discussion groups, which are called BoFs (Birds of a Feather).

All working groups are arranged into areas and managed by Area Directors (ADs). These ADs are members of the Internet Engineering Steering Group. General consensus is used for decision making and mailing lists are used to hold discussions.

Request for Comments (RFC)

A Request for Comments (RFC) is a formal document that could be informational or intended to become Internet standards. Once the final version of the RFC becomes the standard, no further comments or changes are permitted. Future RFCs can supersede others.

There are three sub-series for IETF RFCs:

1. BCP – Best Current Practice
2. FYI – For your Information
3. STD – Standard – highest level of IEFT standards track

Birds of a Feather (BoF)

BoFs are an informal discussion group which is arranged in an ad hoc manner. They are initial meetings of members who may be interested in a particular issue. BoFs are held during the three yearly conferences and allow interested parties to carry out discussions without any pre-planned agenda.

Goals according to the IETF website

- There is a problem that needs solving and the IETF is the right group to attempt solving it
- There is a critical mass of participants willing to work on the problem
- The scope of the problem is well defined and understood, people generally understand what the working group will work on and what the deliverables will be
- There is agreement that the specific deliverables are the right set
- It's believed that the working group has a reasonable probability of having success

Recommended steps for a BoF:

1. Small group gets together privately to discuss possible problem statement and identifies work to be done

a. Does the work already fall within the scope of an existing working group?
b. What work groups are most closely related?
c. Consult with working groups to see if there is interest and whether the work is in scope
d. Consult with area specific mailing list about possible interest
e. Produce internet drafts describing the problem – drafts related to understanding the problem space are more valuable than drafts proposing specific solutions

2. Approach an Area Director to informally float the BoF and get feedback
3. Create a public mailing list and post a call for participation
4. Have substantive mailing list discussion – needs to be broader community interest
5. Submit a formal request to a have a BoF
6. Before the IETF meeting, areas of agreement and disagreement should be identified as lack of consensus is a main reason for not forming a working group
7. Before BoF produce a proposed charter and ask mailing list "should a working group with the following charter be formed"
8. Decide what questions will be asked during the BoF – ask mailing list for input

5.3.6. Domain Name System Security Extensions (DNSSEC)

As one of the major outputs of the IETF, a set of specifications has been defined for ensuring authenticity and data integrity to the DNS which is called the DNSSEC. The DNSSEC allows software to validate that DNS data has not undergone any modifications during its Internet transit. This is undertaken by incorporating public key cryptography into the DNS hierarchy, which forms a chain of trust that originates at the root zone.

Over the years a number of vulnerabilities in the DNS have been discovered that threatened the reliability and trustworthiness of the system. The DNSSEC is able to address these vulnerabilities by adding data origin authentication, data integrity verification and authenticated denial of existence capabilities to the DNS (i.e. validating that a certain domain name does not exist). With DNSSEC, the DNS protocol is less susceptible to attacks such as DNS spoofing attacks.

The IANA has developed a DNSSEC Practice Statement for the Root Zone KSK Operator and this covers practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. The policies and procedures cover areas such:

- Operational requirements: such as how to remove DNS resource records
- Operational controls: such as off-site backup
- Procedural controls: the trusted roles, and identification and authentication for each role

- Personnel controls: background check requirements, sanctions for unauthorized actions
- Technical security controls: such as private key protection and computer security controls

5.4 General conclusion in relation to the DNS

As this overview above has shown, the governance of the DNS has grown over the past decades into a model that is well-managed and fit for purpose. Integrating inputs and perspectives from a very broad range of stakeholders, the technical, substantive and procedurals assurance behind the DNS have matured significantly and, inter alia through DNSSEC, ensure that information in the DNS cannot trivially be modified by unauthorized parties. As summed up in the DNS Policy, Procedures and Guides, the DNS has clear governance assurances and requirements behind it.

However, the purposes for which the DNS was built and is currently being used do not match perfectly with the goals and requirements of the LIGHTest project. Specifically, LIGHTest aims to use the DNS to support the discovery of trust schemes in order to support trust decisions, trust translations and delegation. While this appears technically possible (the execution of LIGHTest will confirm or disconfirm this perspective), it is also clear that the DNS is not designed to convey such information. Information in the DNS can be depended upon to be sufficiently accurate insofar as it extends to the operation of the Internet, by linking domains to IP addresses. The DNS however offers no built-in assurances of the correctness of any other information that might be discovered via domain name servers, including the references to trust schemes for which LIGHTest aims to use it.

In the simplest terms: while the DNS is suitable to protect the integrity and availability of information in the DNS, it offers no legal guarantees on the authenticity, accuracy, or completeness of that information. These are all prerequisites for the successful use of LIGHTest as a technology, since relying parties need to be able to take trust decisions on the basis of trust information that they discover via DNS.

Therefore, LIGHTest will need to deploy a range of legal tools that can complement the governance assurances that are built into the DNS, thus filling the legal gaps. In Chapter 6 below, we will explain how this will be done.

6. The legal toolbox of LIGHTest

6.1. Introduction

The sections above have explained the difficulty of defining the exact legal requirements of each individual use case of the LIGHTest technology, including in the context of delegations, where there is a large variety in not only use cases and in the nature of the delegations themselves (contractual mandates, company representations, and statutory mandates), but also in applicable laws and legal constraints, which are unfortunately not harmonized either within the EU or at the international level. In order to help address this problem, D2.10 defined a legal assessment framework that allows any LIGHTest use case to be tested from a legal perspective, in order to identify specific legal requirements of that use case.

The objective of this deliverable is however not just to identify legal challenges, but also to find a way to resolve them. To do so, a legal toolbox is provided, containing the legal measures which are available within the context of the LIGHTest project.

Broadly, the following logical model can be proposed for the identification and resolution of legal issues, including in relation to delegations:

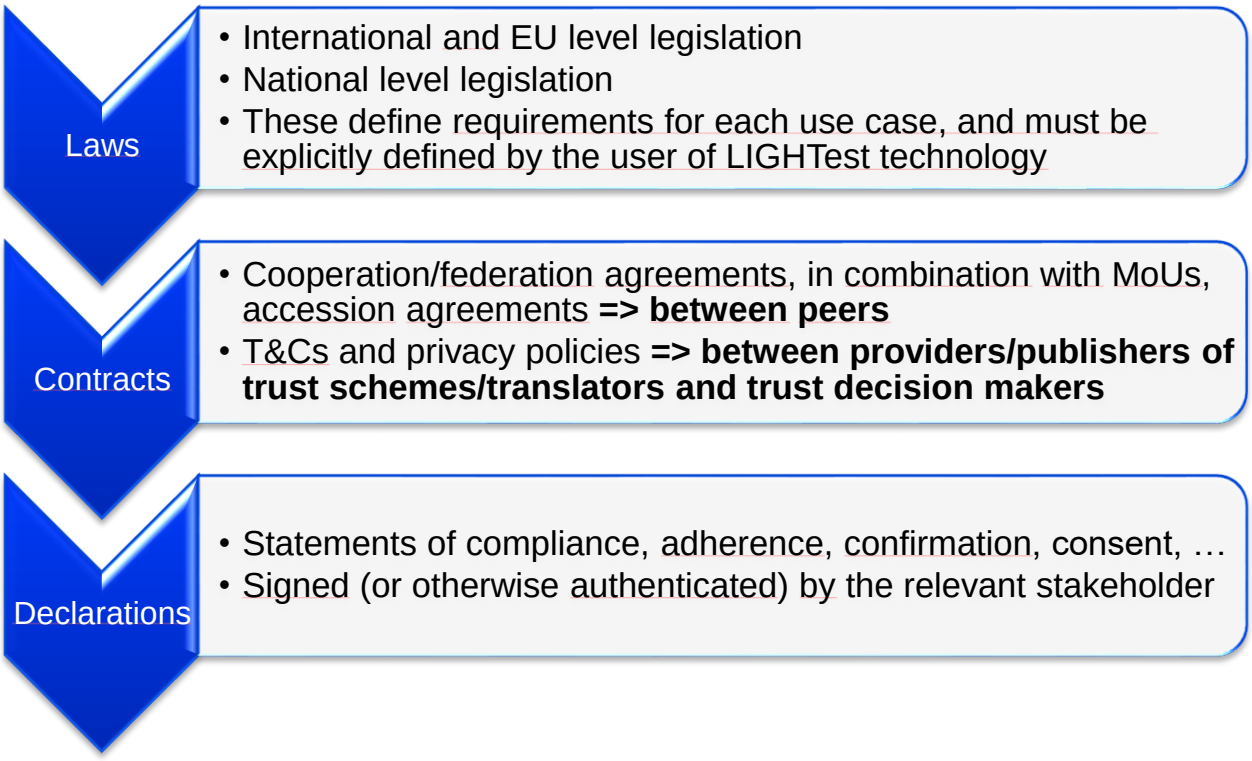

Figure 4: Logical model of the LIGHTest legal toolbox

In this figure, the first item ('Laws') refers to the legal context in which a LIGHTest use case operate, and which – for the purposes of the LIGHTest project – is considered static and immutable, in the sense that LIGHTest has no reliable way to change them in the course of the project. This includes laws dictating the legal authority of a mandate (e.g. granting an official legal status to company mandates in business registers) or the manner in which a mandate can be created (e.g. whether signatures are needed, or whether the mandate needs to be explicitly accepted by the proxy).

Within the LIGHTest pilots, the laws that were used to define the legal assessment framework (notably the EU Charter of Fundamental Rights, the now deprecated Data Protection Directive (DPD) and the current General Data Protection Regulation (GDPR), the eIDAS Regulation, and e-Commerce Directive) are a part of this context, as explained in D2.10. However, other use cases might need to take additional laws into account, e.g. in relation to public procurement, data location, information security, general commercial or civil law, and so forth.

As a result, in order to be able to use LIGHTest technology from a legal perspective as well, two steps need to be taken:

- Identification and assessment of applicable laws in order to identify relevant legal requirements and constraints – as noted above, these are use case specific, so that it would not be viable to abstractly list these in a way that would be accurate in all situations. None the less, a specific tool is provided in section 6.2 below to help third parties to conduct this assessment.
- Drafting relevant terms and conditions for the publication and referencing of a trust scheme, in order to determine precisely which guarantees and assurances are provided by a Delegation Publisher and a Delegation Provider.

LIGHTest uses the DNS for a number of functions, including the discovery and validation of delegations. Once delegation information has been made discoverable using LIGHTest, it can thereafter be applied by any relying party as a part of a trust policy to an electronic transaction, resulting in a trust decision. In more practical terms: a relying party who wants to determine whether a person is indeed the holder of a delegation that it claims to have, may use LIGHTest for that aspect of a trust decision. This deliverable D5.6 examines the legal challenges in relation to delegations which are discoverable via the DNS using LIGHTest.

For the avoidance of doubt, it is repeated that this deliverable *only* examines the legal challenges in relation to delegations. Other legal challenges in relation to decision making, trust translation and trust scheme publication are addressed in D3.7, D4.7 and D6.8 respectively; and ethical issues (including data protection compliance) are examined in T2.7-D3. Furthermore, trust schemes – including any delegations - must of course be drafted and made available by a Delegation Provider before they can be referenced by a Delegation Publisher; this is dealt with in D5.5 - T5.4: Open Source Client Library and Server Tools for Delegation.

The concepts and architectural approach to delegations in LIGHTest have been described in D5.2 - Conceptual Framework for Delegations. Briefly summarised, delegations are implemented in LIGHTest in the form of electronic mandates, i.e. credentials which are issued by a Delegation Provider, asserting that a person acting as a representative – a so called proxy - is empowered to act on behalf of a third party – the mandator - in electronic transactions, which are bound and limited to a certain scope.

Mandate chaining is also conceptually possible: a so-called intermediary can act as an interface between a mandator and a proxy; by way of example: the manager of a company is the proxy of that company, and may empower an employee to manage e.g. HR matters. In that case, the company remains the mandator, the manager becomes an intermediary, and the employee the proxy. All of these parties – the mandator, intermediary and proxy – can be both natural persons

and legal entities such as companies, although in most transactions the ultimate proxy will need to be a natural person, since companies can only act through a human representative.

The electronic mandates are stored by a Delegation Provider, and can be discovered through a Delegation Publisher, which operates a DNS server that can point to one or more Providers. If a person or company chooses to publish delegations itself, then that person or company in practice will act also as its own Delegation publisher (since they need to run a DNS server to point at delegations) and as its own Delegation Provider (since they need to store the delegation somewhere). This is not expected to become a common scenario and will not be piloted in LIGHTest, but conceptually it is possible and can be supported by the LIGHTest technology.

The content of a mandate has been defined in D5.2, and is split into two groups. As stated in D5.2, the first group of fields are mandatory as they must exist in every delegation; without them no delegation is possible. Mandatory fields are there to define the rough boundaries of a delegation and provide information about the Mandator. The content of a Mandate can be comprised of the following fields:

1. Identity information of the Representative, Mandator and Intermediary, together with their level of assurance
2. Date of Issuance
3. Validity time
4. Domain Specific (Scope of the empowerment), which defines the boundaries of how and where the mandate can be used, and is dependent on the business domain of the electronic transaction
5. General Restrictions regarding the usage of the mandate, such as disallowing further sub-delegations
6. Mandate enrolment Level of Assurance, which depends on the mandate issuing process of the Mandate Authoritative Source, the LoA of the eID, etc.
7. Secure Container showing that the content of this mandate has been issued by a Mandate Authoritative Source, for example, the mandate is signed by the Authoritative Source.

The second group of a delegation is domain specific. Just the mandatory information does not limit the proxy at all, except for the time in which the proxy is allowed to act on behalf of the Mandator. Domain specific information is required to limit the power of the Proxy. In practical terms, it can consist of descriptions such as:

- The proxy is allowed to represent the mandator towards entity X
- The proxy is allowed to represent the mandator for business process Y
- The proxy is allowed to represent the mandator for any amounts up to Z EUR

- Etc.

Domain specific information heavily depends on the area where LIGHTest is used and a taxonomy of powers is required in order to provide the domain specific information.

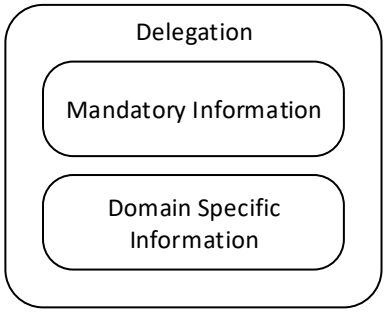

Figure 5: Schematic representation of the data saved in a delegation – Source: D5.2 - Conceptual Framework for Delegations

Based on the conceptual overview above, several clear legal challenges are present. These can be briefly summarised as follows:

Integrity and authenticity of the delegations: any relying party will need to be able to determine whether the delegation's integrity and authenticity is ensured. Integrity refers to the fact that the delegation is presented to the third party without changes or modifications, i.e. that the information contained in the delegation has not been corrupted in any form. Authenticity implies that the participants in the delegation – at a minimum the proxy and the mandator – are identified precisely and that the delegations can be determined to originate from them. Obviously, the issues of integrity and authenticity are closely linked to the topics of **electronic identification, electronic signatures and electronic seals,** as regulated via the eIDAS Regulation. The use of identities, signatures and seals that comply with the eIDAS Regulation in the creation, discovery and validation of delegations would be beneficial to facilitate the finding of integrity and authenticity.

Scoping the substance of the delegations: as already noted above, it can be highly challenging to standardise domain specific information in relation to mandates. While free text can in principle be used, this will typically make it impossible to automate delegation validation in any substantive manner, and undercut the value of LIGHTest. While standardisation of domain specific information is not a legal problem as such, from a legal perspective the main concern is that any standardised rendering of domain specific information must accurately describe the mandate in a way that is clear to the proxy, the mandator, and to third parties. This standardisation work can however build

on the high-level ontology of likely and common mandates which was developed in the STORK 2.0 Large Scale Pilot, covering both the scenarios of representation of legal entities and use cases in which one natural person would be authorized to represent another person. Within STORK 2.0, the following ontology was agreed[8]:

- ***General powers**:*
  - ***Description:** all powers that a natural person has in relation to itself, or all powers of representation in relation to an identified legal entity in all routine matters (including in commercial, human resource, general services, financial, representation and health powers), general corresponding to the authorities of a CEO or the powers of procuration (prokura) in countries that recognize this concept.*
  - ***Examples**: powers to sell products and services, etc.; hire, fire, establish wages and work conditions, etc.; rent buildings, contract various services, constitute companies and other legal entities, including all operations necessary to such creation, appoint representatives of the represented person, within the limits and powers granted by the charter, file for bankruptcy, go into receivership, initiate a winding up, request court protection from creditors, or any other acts that may intentionally terminate the entity or limit or suspend its ability to meet its obligations, etc.*

- ***Commercial powers***
  - ***Description:** all powers to represent oneself or an identified legal entity in common commercial matters.*
  - ***Examples**: powers to sell products and services; sign and present invoices and require its payment; participate to public and private procurement tenders (including the power to sign and submit offers within the limits set by the charter and the law; make all financial and operational transactions necessary to participate to tenders; including providing any necessary financial assurances or warranties; etc.).*

- ***Human Resources powers***
  - ***Description:** all powers to represent oneself or an identified legal entity in common HR matters, including employment, contracting independent workers, and fulfilling any fiscal/social security/administrative obligations linked hereto.*
  - ***Examples**: powers to hire and fire employees; establish wages and work conditions; agree to collective labour agreements; initiate and decide disciplinary measures; organise and/or contract training; pay salaries; submit notifications to competent authorities in relation to all of the above, etc.*

- ***General services powers***

[8] Source: STORK 2.0 D3.6 Consolidated Legal Entities Report; see https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=75:d36-consolidated-legal-entities-report&Itemid=175

- ***Description:*** *all powers to represent oneself or an identified legal entity in common service contracts provided by third parties.*
- ***Examples****: powers to rent, buy, or sell movables or immovables (including buildings, vehicles, etc., but excluding financial assets); contract cleaning services; contract communications and ICT services and products; contract power supply; (buy or rent heating and air conditioning devices; etc.)*

- ***Financial powers***
  - ***Description:*** *all powers to represent oneself or an identified legal entity in interactions with financial services providers or insurance companies, including notably arranging payments and opening accounts.*
  - ***Examples****: powers to settle invoices, pay salaries, expenses; pay service and product suppliers; open, close and manage bank accounts; transfer money from/between accounts; contract credits; manage the financial assets of the represented person; enter into lease, factoring and credit agreements to finance the represented person; buy, alienate or mortgage shares owned by the represented person within the limits set by the charter and by the law; pay all debts of the represented person; acquire, sell, transfer, modify, exchange, alienate, rent and rent out the represented person's financial assets, including stocks and bonds and all other financial values; etc.).*

- ***Public interest representation powers***
  - ***Description:*** *all powers to represent oneself or an identified legal entity in interactions with governmental bodies or entities providing services of public interest.*
  - ***Examples****: powers to represent the represented person at governmental bodies like tax agencies, social security, town hall, courts of justice; organise and manage the representation of the legal entity in all civil, criminal and administrative court proceedings, including starting a proceedings in court on behalf of the legal entity against any third party, organise and manage the representation of the legal entity before public notaries or other public officers, agree to a binding settlement in relation to a dispute prior to initiating any court proceedings, start an arbitration or mediation proceedings, sign all official notifications received by the legal person in relation to on-going disputes, etc.*

- ***Health powers***
  - ***Description:*** *all powers to represent oneself or an identified natural person in interactions with health care professionals.*
  - ***Examples****: powers to consult person's medical file, to seek second opinions, to decide on the treatment to give the patient or to cease/change treatments, etc.*

As STORK 2.0 acknowledged, this ontology is high-level, and consists of archetypes. It was not intended to provide a comprehensive solution that would offer complete certainty in all solutions; rather, it was created to offer a workable model that would permit the implementation of pilots and that would offer sufficient security and trustworthiness in practice. The ontology is also

expandable, and could be further refined to add nuances. In this way, a basic building block was provided that could solve a practical challenge with adequate – but not perfect – legal certainty.

Compliance and legal recognition: even if the integrity and authenticity of a delegation is ensured and the substance has been clearly defined, relying parties will generally want assurances that the delegation was created and is managed in accordance with applicable laws. One might for example. imagine for certain delegations that they must be created in writing, even in hand written form, possibly with notarisations or mandatory registrations. In such cases, being able to find delegation information through LIGHTest does not guarantee that the delegation was created and still exists in accordance with applicable laws. This problem is exacerbated by the fact that, even at the EU level, laws in relation to contractual delegations and company representation (as the main delegation types targeted by LIGHTest) are largely unharmonized: there is no conclusive list of legal requirements for delegations. Given that LIGHTest aims to be used at the global level, and not purely for EU based use cases, the complexity of ensuring compliance with applicable laws is clear.

Trustworthiness (including delegation duration and quality): finally, in practical terms, the source of mandate information within LIGHTest is the Delegation Provider that stores the delegation information. This implies that relying parties must be able to trust in the fact that the information provided by the Delegation Provider is accurate, up to date, and complete. If the Delegation Provider does not provide assurances on this point, a third party can have no justifiable trust in the legal dependability of the delegations.

The analysis above both illustrates the main legal compliance problem of LIGHTest – the fact that legal requirements of delegations are unharmonized and not subject to standardisation – and the possible solution – namely the fact that relying parties must ultimately rely on the Delegation Provider as the source of trust. In any circumstance, a relying party can be guaranteed when using LIGHTest that the delegation information originates from a known and identifiable Delegation Provider.

The relying party will not necessarily be able to identify what the legal framework in relation to a specific delegation was (especially for delegations which are subject to foreign law), but it will be able to find the Delegation Provider that originated the delegations. This implies that, if the Delegation Provider is required to publish the assurances that it provides in relation to the delegations that it makes available via LIGHTest, relying parties have a viable avenue for making trust decisions.

This approach is capable of addressing the challenges identified above:

- **Integrity and authenticity can be provided by the fact that the Delegation Provider electronically signs the delegations** that it makes available to third parties (or more accurately from a legal perspective: it electronically seals the information, since signing implies human intervention). This provides integrity (in the sense that relying parties can determine that the information was not corrupted after the signing by the Delegation Provider) and authenticity (in the sense that relying parties can determine that the delegation information originated from the Delegation Provider). Thus, the link between the delegation and the Delegation Provider is clear. There is clear potential added value for the Delegation Provider to use qualified electronic seals as defined under eIDAS compliance to seal the assertions, and even qualified timestamps to assert timing of the mandate (starting time and current validity). However, this won't be mandatory within LIGHTest, since that would cut off some use cases where eIDAS compliance isn't strictly necessary, and would also make LIGHTest fully EU-specific, since the concepts of qualified seals and qualified timestamps are unique to the EU.
- **The scope of delegations can be standardised and defined precisely by each Delegation Provider.** This is a viable approach, since it is likely that any Delegation Provider will deal with only a relatively narrowly defined context of delegations. E.g. a business register identifies the managers (under whatever name) of its companies, a tax administration might register the accountants who are allowed to represent specific clients, etc. The scoping in each context can be standardised and defined on a case by case basis, in a way that is logically understandable, consistent and reasonably complete for the Delegation Providers and the third parties that it wishes to assist.
- **The compliance and legal recognition burden can be more easily shouldered by the Delegation Provider,** since it will know the complexities of its delegations and the applicable rules. The Delegation Provider will need to determine itself whether the delegations that it makes available are legally valid, and communicate its assurances on this point to relying parties. This does not imply that a Delegation Provider *must* assume full responsibility and liability for legal compliance of its delegation information; to the contrary, it can also explicitly disclaim responsibilities on this point. By way of example, a Delegation Provider might simply indicate that information is only provided on an 'as-is' basis without any assurances of compliance or any liability. More realistically, the Delegation Provider may also just limit its responsibilities by stating e.g. that it can only assert that the delegations were compliant with its own national laws at the time of their registration. The main objective is to provide sufficiently clear and comprehensive information that permits relying parties to make trust decisions on the basis of the delegation information.
- **Finally, the trustworthiness of the delegations can be addressed in the same way: the Delegation Provider can and must communicate to third parties which assurances (if any) it provides in relation to the delegation information that it makes available.**

This approach is pragmatic, and essentially has one key legal characteristic: **the information that the Delegation Provider offers (the electronic mandate) should not be considered as the delegation as such, but rather as an electronic assertion from the Delegation Provider that a delegation exists that meets the description of the electronic assertion**. To clarify the difference: it is possible that e.g. a contractual delegation requires the signatures of both the mandator and the proxy. Using the mechanism described above, a relying party however would not receive an electronic delegation containing the signature of the mandator and proxy. It would instead receive an electronic assertion, sealed by the Delegation Provider, confirming the existence of a contractual delegation and the key terms (the parties, date of creation, scoping, duration, etc; as described above).

The strength of this approach is that it can be applied in any use case, for any delegation in a global context, which is a key objective of LIGHTest. The weaknesses are twofold: firstly, it is only usable in cases where an assertion (rather than the original delegation) is acceptable for the relying party. If a relying party must receive the original delegation for whatever reason rather than an assertion from a Delegation Provider, the LIGHTest approach will not necessarily be sufficient. Secondly, it relies on the establishment of trust between the relying party and the Delegation Provider. At a minimum, this implies that the Delegation Provider publishes the terms and conditions under which it makes the delegations available. This issue will be examined in the following section.

6.2. Identifying legal constraints for a specific use case – the LIGHTest legal compliance assessment framework

Given the broad range of potential use cases, it is not possible to draft up a single contract or a single declaration that would be suitable to generically address the legal compliance and validity requirements of all LIGHTest use cases. Nonetheless, D2.10 defined a generic analytical framework that allows legal, ethical and societal challenges for LIGHTest use cases to be identified. The framework consisted of a statement of principles that can be used as assessment criteria to determine whether a LIGHTest use case is likely to encounter specific types of legal, ethical and societal challenges and what the resulting requirements might be. The following visual canvas containing the principles of the assessment framework was provided and commented in D2.10:

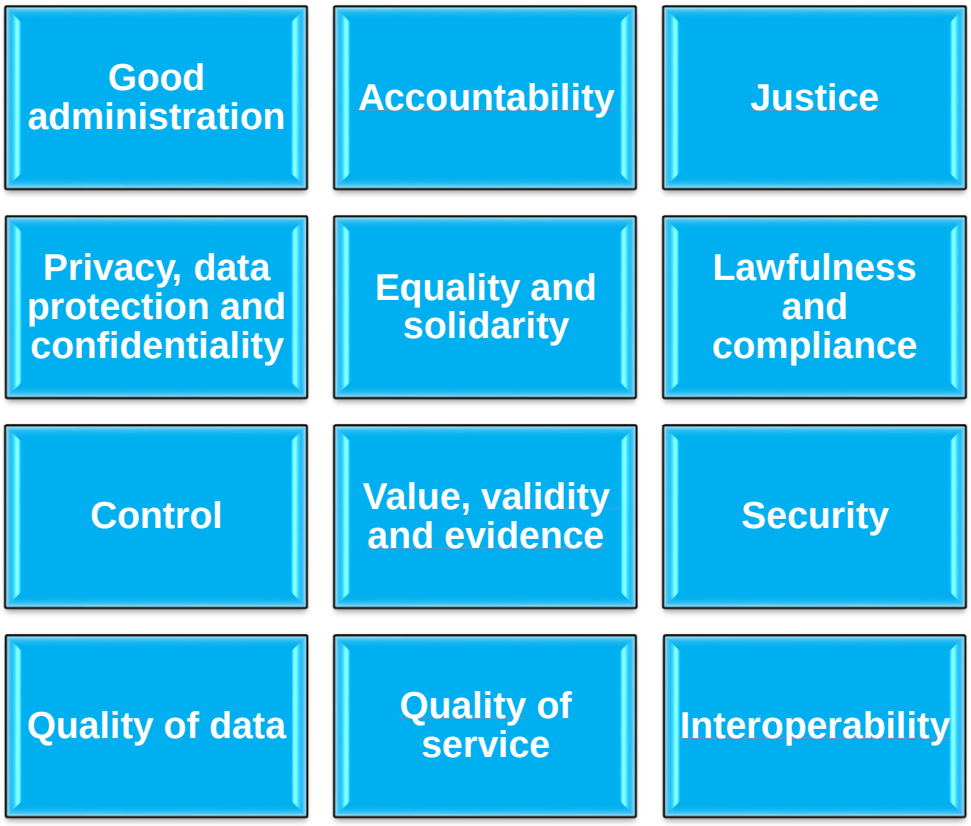

Figure 6: Canvas of the assessment framework

These principles are relatively high level by necessity, given that they are designed to be applicable to any potential use case of the LIGHTest technology. However, specifically for the context of delegations, a more specific check list has been created, building on the generic principle list from D2.10, and focusing the principles more narrowly on only those questions that are particularly relevant for entities that map and provide delegation information using LIGHTest technologies. This check list is reprised below. In practical terms, this check list can be used to assess any given use case, in order to identify relevant legal challenges and issues which may need to be addressed by the standardised terms and conditions in section 6.3 below:

Principles	Description and resulting requirements

Good administration	**Description**: LIGHTest technology must be implemented in a way that ensures that transactions are handled impartially, fairly and within a reasonable time. **Requirements**: • The principle primarily affects the quality of service of the Delegation Provider: comparable requests must receive comparable responses to avoid discriminations, and the availability of the delegation data must be defined at an appropriate and acceptable level.
Accountability	**Description**: LIGHTest technology must be implemented in a way that ensures that responsibilities are clearly allocated between each participant in the exchange of trust information. **Requirements**: • On the basis of the contractual terms, relying parties must be able to determine what assurances are provided by the Delegation Provider in relation to the delegation information, and notably whether the information in relation to the delegations has any basis under law, or whether the information is merely a reflection of the Delegation Provider's own policies. • This also includes any right to restitution of any damages caused by errors in the delegation.
Justice	**Description**: LIGHTest technology must be implemented in a way that ensures the right to recourse for the persons relying on LIGHTest technology, and that contains appropriate enforcement mechanisms. **Requirements**: • On the basis of the contractual terms, relying parties must be able to determine applicable law and any dispute resolution mechanisms. • Appropriate identifying information and contact mechanisms must be provided to relying parties.
Privacy, data protection and confidentiality	**Description**: LIGHTest technology must be implemented in a way that safeguards the fundamental rights to privacy and data protection for natural persons, and respecting the legitimate interests of confidentiality and of professional and business secrecy. **Requirements**: • As a matter of principle, any trust information in LIGHTest infrastructure should not contain any personal data as defined under EU law. However, while the delegation information is stored by the Delegation Provider outside of the DNS (and therefore arguably outside of LIGHTest infrastructure), the Delegation Publisher must inherently provide pointers to personal data held by the Delegation Provider itself; therefore personal data will be processed. The contractual terms must ensure that such data will be processed by the Delegation Provider in accordance with the GDPR.
Equality and solidarity	**Description**: LIGHTest technology must be implemented in a way that protects the persons concerned against discrimination. **Requirements**: • Delegation information must be provided on a neutral basis, following the rules provided in the contractual terms, and without prejudicing any decisions that would be made by the relying party on the basis of

	the delegation information. The contractual terms should make it clear that they address only the delegation information, not the subsequent decisions made by the relying party. • Universal accessibility must be ensured, including to persons with disabilities. Accessible support and communication mechanisms must be provided.
Lawfulness and compliance	**Description**: LIGHTest technology must be implemented in a way that ensures that delegation information is only provided in accordance with any specific legislation or other legal requirements that may apply to the Delegation Provider. **Requirements**: • The contractual terms may be finalised only after identifying which legislation applies to the use case. This can be constrained to some extent by explicitly identifying applicable laws under which the trust scheme may be relied upon.
Control	**Description**: the implementation of LIGHTest technology must contain appropriate controls to ensure that the provided trust information is relevant and to allow incidents to be detected and addressed. **Requirements**: • Audit and logging measures must be referenced in the contractual terms, in case of disputes (including the identification of the sending and receiving parties, the time of the exchange, and the integrity/authenticity of the exchanged data itself).
Value, validity and evidence	**Description**: the legal value and validity of any trust information exchanged via LIGHTest must be clear to all participants in a transaction. **Requirements**: • The legal value and validity of the delegation information must be explicitly described in the contractual terms, including specifically whether it can be considered authoritative (as is e.g. the case for company representation data obtained directly from the business register, i.e. cases where the operator of the business register is the Delegation Provider), or whether it can otherwise be relied upon to be genuine or to be covered by any contractual assurances.
Security	**Description**: LIGHTest technology must be implemented in a way that protects the exchanged trust information against modification during transit, thereby ensuring its integrity and authenticity to the extent required by the use case. **Requirements**: • Contractual terms should reference the chosen technical and organisational measures and contain breach notification mechanisms to allow problems to be addressed.
Quality of data	**Description**: LIGHTest technology must be implemented in a way that provides a clear shared understanding between all participants in the use case on the quality of the trust information. **Requirements**: • The contractual terms should clearly state the obligations of the participants in the use case in relation to the quality of the delegations,

	including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • A feedback mechanism must be in place that allows the persons involved to contact the Delegation Provider to correct any inaccuracies.
Quality of service	**Description**: LIGHTest technology must be implemented in a way that provides a clear shared understanding between all participants in a use case on the quality of the services for the trust translation. **Requirements**: • The contractual terms should clearly state the obligations of the participants in the use case in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear).
Interoperability	**Description**: LIGHTest technology must be implemented in a way that ensures semantic and technical interoperability of the trust information exchanged via LIGHTest. **Requirements**: • The contractual terms should clearly state the requirement for the relying party to ensure that the delegation information is processed in accordance with LIGHTest's technical standards.

Table 1: Assessment framework – principles and requirements for trust scheme publication

In the section below, we will show how the requirements of the assessment framework in relation to delegations can be met through contractual terms. A general template structure is provided, along with summary guidance on options and choices to be made.

6.3. Contractual terms – model terms and conditions and implementation guidance

6.3.1. General approach

This deliverable is focused on delegation. The section above has already shown that the principal requirement is that relying parties – those that wish to rely on the delegations – must know precisely what its legal value is, and whether it satisfies their legal requirements.

Since LIGHTest is unable to change legislation, the emphasis within the LIGHTest project is on identifying contractual terms that clarify the legal value of delegations that can be discovered via LIGHTest, thereby also affecting the validity of the decisions made on the basis of them. As a result of this focus, the main need is defining terms and conditions that govern the responsibilities of Delegation Providers.

It should be emphasised also that the scope of LIGHTest is not to critically assess, improve, or otherwise modify delegations. From the perspective of LIGHTest, delegations exist as an external input: LIGHTest does not define what they should contain or create them, nor does it enhance, lower or otherwise affect their legal value, their strengths or weaknesses. LIGHTest is a tool for making delegations discoverable via the DNS and to make trust decisions on the basis of them. Therefore, the terms and conditions should not go into details on the procedures behind the creation of delegations – other than, if appropriate, any assurances that the delegations were established or are maintained in accordance with explicitly identified laws. The main concern is ensuring their availability, findability and usability.

In addition, LIGHTest also cannot control any uses made of discoverable delegations: while the legal terms and conditions may forbid specific uses (or more likely: limit any legal assurances to specific use cases), it is possible due to the open nature of the DNS that third parties choose to ignore such restrictions. Specifically, there is nothing in practice stopping third parties from accessing and using delegations which are made openly available. This cannot be controlled; however, Delegation Providers can control the legal risks for them by publishing their own terms, including responsibilities and liabilities that they accept or waive.

In other words, any Delegation Provider must declare via legal terms whether it ensures compliance of its delegations with existing laws (and if so, which ones), and which assurances it provides in relation to the delegations that it makes accessible. These can range from none at all ('the delegations are published as is, without any assurances of availability, reliability or accuracy, and should be relied upon on the user's own risk') to very stringent ('the referenced delegations are guaranteed to be authoritative: they are complete, correct, available at all times, authentic, and a reflection of applicable law'), with many possible nuances in between.

Hereunder, a set of model terms and conditions for Delegation Provider is included. As noted above, the text should always be reviewed to assess its suitability for a specific context, and some tailoring is necessary – indicated hereunder by the generic [*description*] tag indicating that unique content must be added. Where appropriate comment boxes in blue colouring have been added to

explain which of the principles in section 6.2 the terms relate to, or which choices the trust scheme publisher should make.

6.3.2. Sample terms and conditions for a Delegation Provider

Preamble – Nature and goals of these Terms

These terms and conditions (hereafter collectively referred to as the 'Terms') govern the use of the delegation information services relating to [*briefly describe the scope and goals of the delegations, including their origins, purpose and semantic contents used*] (hereafter referred to as the 'Scheme'). A copy of the Scheme is available at [*insert URL*].

The Scheme is available to and may be relied upon by any persons (including natural persons and legal entities) who have been invited in writing by the Provider to do so, and who have accepted these Terms (hereafter referred to as the 'User', or as 'you'). The User must read and accept these Terms before relying on the Scheme. The User can print or store a local PDF copy of the Terms on their own chosen information system.

Comment: it is worth defining precisely who may rely on the Scheme in a legally binding manner, and excluding any other persons from the scope of these Terms.
Local storage of the Terms is strongly recommended in order to comply with the legal requirement that terms and conditions must be available to the Users on a durable medium for consumer oriented online services.

By relying on the Scheme, the User confirms that he, she or it is bound by these Terms, as amended from time to time. The User confirms that he, she or it has received, read and understood these Terms and has accepted the content thereof without reservation. If the User has any reservations in relation to any part of these Terms, the User shall refrain from using the Scheme or from relying on it in any manner, and the User accepts that the Provider bears no responsibility or liability of any kind towards the User or towards any third party for such use.

The delegation information service is provided by [*identify the Delegation Provider by name, address, and any national business register number*], hereafter referred to as the 'Provider'. For any questions or concerns in relation to the Scheme or to these Terms, the Provider can be contacted at [*provide contact information, at a minimum an e-mail address*].

Comment: the Provider should be identified as required under the e-Commerce Directive, and contact information should be provided in accordance with the transparency principle.

Description of the Scheme

The Scheme is made available by the Provider in order to permit the User to [*describe why the Provider makes the Scheme available to the User, i.e. what delegations it aims to make available*].

The Scheme does not provide any payment services, nor does it constitute a trust service as defined in the eIDAS Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Comment: it can be useful to describe also what the Scheme is not intended to be (i.e. a trust service in the paragraph above), simply for the avoidance of doubt.

Availability and permissible use of the Scheme

The Scheme is available solely to persons who are legally adults under [*refer to applicable national law]* law, and who have legal capacity to sign contracts. Users who do not meet this requirement may not use the Scheme.

Furthermore, the Scheme is available solely to persons who have been invited by the Provider to rely on it, explicitly and in writing. Users who have not received such a written invitation may not use the Scheme.

Comment: this paragraph can be omitted if the Scheme is available to anyone. Inversely, it can also be tailored to the use case – e.g. the Scheme is available solely to persons who are members of the Provider's organisation, or who have a specific license to practice in a specific sector, or who comply with a specific law – this should always be tailored to the exact circumstance.

The Provider grants you as the User a temporary, non-exclusive individual and non-transferable right to use the Scheme. You are not entitled to pass it on in any manner whatsoever, commercialise it, or to claim any ownership or authorship in relation to it or any parts of it, including any specific information from any individual delegation.

Comment: this paragraph can be omitted if the Scheme is intended to be freely available to anyone. It is mainly useful to avoid 'forking', i.e. cases where (near-)duplicates of a scheme are copied under other names, or 'database scraping' where the delegation information is extracted comprehensively, one delegation at a time, which can cause confusion in the market.

The Provider does not in any way guarantee or undertake that the Scheme or particular facilities or parts thereof satisfy legal requirements which are incumbent upon you as the User.

Comment: it is generally useful to include a paragraph such as the one above to highlight that the Terms do not remove any legal responsibilities from the User, unless this was explicitly intended to be the case. Depending on the use case, it may be desirable to add exceptions – e.g. 'The Provider does however guarantee that the delegation information included in the Scheme corresponds fully and entirely to the information referenced in article X of legislation Y in relation to business registers in Country Z, and the User may rely on the accuracy of such data under these Terms'.

You as the User agree and affirm that you will only use the Scheme for the purposes that are allowed on the grounds of these Terms and the applicable legislation and regulations or generally accepted practice. The Provider may at any time issue instructions to the User regarding the use of the Scheme for operational, quality and security reasons. The User undertakes to follow these instructions.

You as the User agree that you will not use the Scheme for the following purposes:

a) to disseminate or promote in any other manner, documents that are illegal, intimidating, threatening, harmful, unlawful, defamatory, humiliating, insulting, violent, obscene or vulgar, or which constitutes a breach of the privacy of others, or that is hateful, racist or ethnically insulting or otherwise offensive;

b) to pretend to be a person or entity that you are not;

c) to set up activities constituting a breach of copyright or other intellectual property rights (including uploading documents which you are not entitled to upload);

d) to upload, post, sign e-mail, send, file or make available in any other manner materials containing viruses or other computer codes, files or programs that are designed to damage, hinder or restrict the normal operation of the Scheme (or a part thereof) or of other computer software;

e) to hinder or disrupt (including any unauthorised access to, unauthorised use or perusal of data or traffic) the Scheme, servers or networks linked to the Scheme, or policy, requirements or prescriptions of networks linked to the Scheme, or attempt to undertake any of these actions;

f) to plan or develop illegal activities;

g) to collect other Scheme users' personal information and file it with a view to using it in connection with one of the above-mentioned prohibited activities or in any other unlawful manner.

Comment: while this is very context specific, it is generally useful to include a paragraph excluding some manifestly unlawful use cases.

Changes in the Scheme and in these Terms

The Provider has the right to temporarily or permanently terminate references to the Scheme, and to update, revise or delete the Scheme (or parts thereof), including notably by adding new delegations, updating them as needed, or by removing older delegations, as deemed appropriate by the Provider. If this happens, the Provider is not required to provide you as the User with any notice.

Comment: in some cases a Scheme will need to remain available, or a guarantee of availability and/or prior notice may be needed. The model clause above is intended for situations where Schemes may be dynamically changed or removed.

Any use of or reliance on any part of the Scheme by the User is always subject to the version of the Terms which are current at the time of use or reliance by the User. The User is therefore advised to verify any changes to these Terms prior to using or relying on the Scheme in any way.

Comment: as Schemes and Terms can evolve over time, a revision clause such as the one above is strongly recommended.

Guarantees, warranties and liabilities in relation to the Scheme

The Provider warrants and represents that [*enumerate any guarantees as explicitly and unambiguously as possible*].

Comment: this paragraph is highly context dependent. Generally, it should include any guarantees which are necessary for a relying party to use the Scheme for reliance on the delegation information in practice. Note that it is perfectly appropriate for some schemes to contain no binding assurances at all from the Provider; in this case the paragraph above may simply state: "The Provider has taken all commercially reasonable efforts and due care to ensure that the Scheme and the delegation information included therein is suitable for the purposes of use as described in these Terms. However, the Scheme is made available on a best efforts basis only, purely for the User's convenience, and the Scheme is referenced without any assurances or guarantees whatsoever by the Provider, including with respect to fitness for any purpose. The Provider cannot be held responsible or liable in any way and under any legal theory with respect to these Terms or the Scheme".

Inversely, if the Provider does wish to guarantee the quality of the data – e.g. because its delegation information is authoritative and legally guaranteed to be accurate under national law, the paragraph above may simply state: "The Provider maintains the Scheme and the delegation information included therein in accordance with its obligations under article X of legislation Y in relation to business registers in Country Z. The Provider therefore warrants and represents that the User may rely on the accuracy of such data as provided by that law".

The Provider shall take all commercially reasonable efforts and take due care when providing and maintaining the Scheme on a continuous 24/7 basis. However, you as the User accept that you have no guarantee or expectation of permanent availability of the Scheme except as set out under these Terms, and you as the User shall not legally rely or depend on its continuous availability, notably when required to satisfy legally binding deadlines or retention obligations. The Scheme may be available more slowly, may not available or perform unpredictably from time to time due to various factors, including location, internet connection speed, technical reasons, scheduled or unscheduled maintenance or updates.

The Provider shall take all commercially reasonable efforts and take due care to ensure that the Scheme is available free of loss of data, corruption, attacks, viruses, interference, hacking or other security breaches.

The Provider is not responsible or liable for any damage due to the fact that you have not observed these Terms. This includes any damage of any nature whatsoever arising from the unlawful use of the Scheme, or from the User's failure to assess compliance with any legal obligations or requirements which are incumbent upon them.

Furthermore, the Provider is not liable for the consequences of any temporary unavailability, suspension, disruption or delay in all or certain functionalities of the Scheme pursuant to maintenance works, defects or force majeure or pursuant to any incident which is beyond the Provider's reasonable control; nor for any damage as a result of any difficulty or temporary impossibility to use the Scheme or to gain access to the content of the Scheme, or as a result of any telecommunications system error which has the consequence that the Scheme is unavailable. This also excludes any responsibility or liability for the consequences of any unavailability, suspension, disruption or delay relating to underlying sources of data provided by third parties which are used by the Scheme, including any delegation information provided or maintained by third parties.

The provisions of this Article do not curtail the Provider's liability for its own wilful error, gross negligence or fraud.

The Provider is not liable for any force majeure event, including but not limited to general disruptions in electric networks and energy services, telecommunications networks, internet services, third party service providers; natural disasters, general strikes, wars and terrorist attacks, or acts of God.

The liability of the Provider, irrespective under which legal doctrine and irrespective or the nature of the damage, is in any event confined to the repair of the proven, foreseeable, direct and personal damage that the User has suffered, excluding, yet not limited to, any indirect or consequential damage, including specifically any loss, corruption or removal of information or loss

of business, income, profit, or reputation. The sum and aggregate liability of the Provider under these Terms towards the user is at any rate capped at 2.500 EUR per event which caused harm to the User.

Comment: liability provisions are highly context dependent. The paragraphs above contain relatively broad exclusions and limitations of liability, which are generally acceptable when schemes are made available free of charge. In commercial services, more business oriented liability arrangements – in line with commercial fees paid – may be justified. Similarly, broad exclusions of responsibility or liability may be infeasible when the Delegation Provider is a public authority providing the data under a specific legal mandate. In such cases, it may be more appropriate for the Terms to state that "The Provider maintains the Scheme and the delegation information included therein in accordance with its obligations under article X of legislation Y in relation to business registers in Country Z. The Provider therefore warrants and represents that the User may rely on the availability of the Scheme as provided by that law, and the Provider accepts its responsibilities and liabilities as defined by the laws of its state of establishment".

Costs, fees and charges in relation to the Scheme

The use of and reliance on the Scheme is free of costs, and no charges will apply other than any costs, fees or charges which are agreed separately between you as the User and the Provider.

The User must personally bear any additional costs related to the purchase, installation and operation of any devices and software used by the User in relation to the Scheme, and the costs that its network provider charges for access to the Internet.

Comment: as above, these model clauses assume a Scheme which is made available gratis. This may not be viable or appropriate under all use cases. Note however that the clause still considers it possible that separate fees may be warranted for related products or services (by way of example: license fees for software that the Provider makes available which use the Scheme).

Intellectual property rights to the Scheme

You as the User agree and accept that the Scheme and all components thereof, including yet not restricted to, graphic elements, user interface, scripts and software that are used to implement the Scheme, and any intellectual property rights vested therein, whether or not these are registered, and regardless of where in the world they exist are owned by the Provider or by third parties with whom the Provider has signed appropriate agreements, and that these Terms do not grant you any ownership or usage rights in relation to the Scheme except as specifically set out in these Terms. It is forbidden to duplicate any parts of the Scheme.

Comment: schemes are generally not creative works which are protected under copyrights or other intellectual property rights, and their general availability generally means that they also do not qualify as

a business secret. None the less, the paragraph above provides a baseline for avoiding unwanted re-use of the Scheme

Privacy and data protection

You as the User agree that use of and reliance on the Scheme results in the processing of personal data, as defined by the General Data Protection 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 or 'GDPR'), in relation to the persons identified in any individual delegation.

With respect to the operation and maintenance of the Scheme and in making delegation information available to you under these Terms, the Provider as identified above shall act as a data controller as defined under the GDPR, and will only process the personal data for the purposes of enabling your use of the Scheme as permitted under these Terms (based on the necessity of such processing for the performance of a contract to which the User is party), and to ensure the accurate and effective operation of the Scheme (based on the Provider's legitimate interest in ensuring that the Scheme can operate in practice).

The personal data shall only be entrusted by the Provider to service providers who support the Provider in the execution of these Terms, who will be bound to the Provider through contracts that comply with the requirements of the GDPR. No personal data shall be sent by the Provider to a third country or international organisation. The personal data shall be retained by the Provider for the period of time agreed with the relevant persons identified in the delegation information for each individual delegation, or for as long as required under applicable law in the Provider's country of establishment. Any person identified in a delegation has the right to request from the Provider access to and rectification or erasure of personal data or restriction of processing concerning the them, or to object to processing as well as the right to data portability, subject to the conditions stipulated within the GDPR. Such persons have the right to lodge a complaint with a supervisory authority.

Note that, if the User processes personal data as a part of its use of the Scheme, the User will likely fall under the scope of the GDPR as well, acting as an independent controller. The User is solely responsible for complying with applicable law.

Comment: providing delegation information or using the information will generally result in the processing of personal data, namely of the persons identified in the delegations (one of whom may be the User, although this is certainly not guaranteed. As a result, the GDPR may apply. The lengthy first paragraph

above is intended to include the minimal set of information required under the GDPR. While the modalities may be varied (e.g. different storage period), it is not recommended to delete this information. Note also that this paragraph should be reviewed and tailored to the exact situation. By way of example, the legal basis for processing will not be legitimate interest for a public authority, but rather the performance of a public task; this would need to be revised. Similarly, the right to deletion of data or the right to port data to a different provider will not apply when the Provider is a public authority with a legal mandate and obligation to maintain the data. If the Provider is a public authority in the EU, it is usually obliged to appoint a data protection officer, who should be consulted on the clause above, and who should conduct a data protection impact assessment prior to deploying LIGHTest technology. The latter point is commented in greater detail in T2.7-D3: Legal, Ethical and Societal Requirements and Constraints (2).

Further personal data processing is likely to occur by the User itself, following its accessing the Scheme and obtaining the requested delegation information. This is however the sole responsibility of the User itself, as the last paragraph indicates; the Provider bears no responsibility or liability on this point.

Other provisions

The Provider may adjust the technical specification or properties of the Scheme for the purposes of technical, operational, legal or economic needs. If such change substantially influences use of the Scheme, the User's sole remedy is to terminate use of the Scheme. The User must always ensure interoperability with the technical requirements of the Scheme, and the User is presumed to have accepted any changes and additions if they continue to use the Scheme.

If one or several provisions of these Terms were to be or become invalid or null and void, this shall not affect the validity of the other provisions. The invalid or null and void provision shall be replaced by a provision that approximates as much as possible the intention of the invalid or null and void provision.

Nothing in these Terms shall be interpreted as a transfer of any interest, title or licence to the User.

Certain content, components or facilities of the Scheme can contain materials originating from third parties and/or hyperlinks to other websites, resources or other content. In view of the fact that the Provider may not have any control over such websites and/or materials belonging to third parties, the User acknowledges and accepts that the Provider is not responsible for the availability of such websites or resources, does not confirm or guarantee the accuracy of such websites or resources and shall never be liable or responsible for any content, advertisements, products or materials on or available through such websites or resources. The Provider shall not in any manner whatsoever be responsible or liable for damage or supposed damage the User has suffered, either directly or indirectly, due to your use of such websites or resources.

If the Provider does not exercise or maintain a right to or provision of these Terms, this may not be interpreted as a declaration of a waiver of such right or provision or of any other rights or

provisions. The User agrees that, unless there is a provision to the contrary in these Terms, third parties cannot derive any rights from these Terms.

The User may not transfer to any third party his, her or its rights and obligations under these Terms. The Provider reserves the right to transfer any rights and obligations under these Terms to any third party.

These Terms, together with the documents to which they refer, constitute the full and complete binding contract between the User and the Provider with regard to the Scheme.

These Terms are governed by [*name a country*] law. Any dispute on the coming into effect, interpretation or execution of these Terms falls under the exclusive jurisdiction of the Courts in [*location*].

Terms and conditions v.[add version number] – Last updated on [add the date of the last edit]

Comment: given that terms and conditions often evolve over time, it is strongly recommended to add a version number and timestamp to facilitate discussions relating to the applicable terms at any given time. Older versions of the Terms should be archived.

7. References

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; last visited on 12 August 2019

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); see http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679; last visited on 12 August 2019

Regulation 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 (eIDAS Regulation); see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG; last visited on 12 August 2019

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC); see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765; last visited on 12 August 2019

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002; last visited on 12 August 2019

ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance; see http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138; last visited on 12 August 2019

FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors; see http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf; last visited on 12 August 2019

D2.1 - Inventories (1); see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D2.3 - Requirements and Use Cases; see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D2.9 - Social Impact Report; see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D2.10 - Legal, Ethical and Societal Requirements and Constraints (1); see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D4.1 - Conceptual Framework for Trust Scheme Translation (1); see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D4.6 - Cross-Border Legal Compliance and Validity of Trust Scheme Translation (1); see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D5.2 - Conceptual Framework for Delegations (2); see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

D6.7 - Cross-Border Legal Compliance and Validity of Trust Policy and Trust Decisions (1); see https://www.lightest-community.org/deliverables; last visited on 12 August 2019

8. Project Description

LIGHTest project to build a global trust infrastructure that enables electronic transactions in a wide variety of applications

An ever increasing number of transactions are conducted virtually over the Internet. How can you be sure that the person making the transaction is who they say they are? The EU-funded project LIGHTest addresses this issue by creating a global trust infrastructure. It will provide a solution that allows one to distinguish legitimate identities from frauds. This is key in being able to bring an efficiency of electronic transactions to a wide application field ranging from simple verification of electronic signatures, over eProcurement, eJustice, eHealth, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things.

Traditionally, we often knew our business partners personally, which meant that impersonation and fraud were uncommon. Whether regarding the single European market place or on a Global scale, there is an increasing amount of electronic transactions that are becoming a part of peoples everyday lives, where decisions on establishing who is on the other end of the transaction is important. Clearly, it is necessary to have assistance from authorities to certify trustworthy electronic identities. This has already been done. For example, the EC and Member States have legally binding electronic signatures. But how can we query such authorities in a secure manner? With the current lack of a worldwide standard for publishing and querying trust information, this would be a prohibitively complex leading to verifiers having to deal with a high number of formats and protocols.

The EU-funded LIGHTest project attempts to solve this problem by building a global trust infrastructure where arbitrary authorities can publish their trust information. Setting up a global infrastructure is an ambitious objective; however, given the already existing infrastructure, organization, governance and security standards of the Internet Domain Name System, it is with confidence that this is possible. The EC and Member States can use this to publish lists of qualified trust services, as business registrars and authorities can in health, law enforcement and justice. In the private sector, this can be used to establish trust in inter-banking, international trade, shipping, business reputation and credit rating. Companies, administrations, and citizens can then use LIGHTest open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHTest project starts on September 1st and has an estimated cost of almost 9 Million Euros. It is partially funded by the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321. The LIGHTest consortium consists of 14 partners from 9

European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHTest attempts to build up a global community based on international standards and open source software.

The partners are ATOS (ES), Time.lex (BE), Technische Universität Graz (AT),EEMA (BE), G+D (DE), Danmarks tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), Ubisecure (FI), and University of Piraeus Research Center - UPRC (GR). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.