D6.8

Cross-Border Legal Compliance and Validity of Trust Policy and Trust Decisions (2)

Document Identification	
Date	30.08.2019
Status	Final
Version	1.1

Related WP	WP 6	**Related Deliverable(s)**	D2.9, D2.10, D2.3, D6.8
Lead Authors	Hans Graux (TIL), Edwin Jacobs (TIL)	**Dissemination Level**	PU
Lead Participants	TIL, OIX, ATOS	**Contributors**	TIL
Reviewers	TUBITAK, NLNET		

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 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 policies can take many forms and cover many topics, and one of the challenges of LIGHTest is to find a way to ensure that they are created, applied and enforced to specific transaction types in a manner which is legally compliant and legally binding. While some trust policies have a clear legal background (e.g. the legal framework governing trust services in the EU is created by the eIDAS Regulation), trust policies in LIGHTest have a potentially much broader scope, and can cover a complex web of stakeholders (contractual signatories, policy makers, trust service providers, supervisory organisations, etc.). There is no guarantee that a specific legislation will apply to these stakeholders.

The objective of this deliverable is to provide an overview of how LIGHTest addresses the legal challenges in relation to trust policies and trust decisions, and which outputs have been created through various deliverables, including in relation to publication, translation and delegation. More explicitly, this deliverable explains how, based on the characteristics of LIGHTest as a project (Chapter 4), the DNS (Chapter 5) and the legal tools at our disposal in the context of LIGHTest (Chapter 6), we have created a legal solution framework that allows users of the LIGHTest technology to provide acceptable legal certainty in the trust policies which are processed through LIGHTest technology and in the trust decisions that users make on the basis of this trust information (Chapter 7). Furthermore, as a way of supporting sustainability, we provide a proposal of how LIGHTest infrastructure could be embedded in future legislation, using the eIDAS Regulation as an example.

This deliverable 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. 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.

It should be noted that this deliverable does not focus on the identification of legal, ethical and societal requirements in LIGHTest in general (which are identified in D2.10), nor does it contain model contractual terms for each of the core functions of LIGHTest (which can be found in the aforementioned deliverables D3.7 (for publication), D4.7 (for translation) and D5.7 (for delegation). Instead, it explains the interrelation between these topics and illustrates how LIGHTest has been piloted, and how it can be deployed in future scenarios, including after the project's termination.

2. Document Information

2.1 Contributors

Name	Partner
Hans Graux	TIL
Edwin Jacobs	TIL
Burçin Bozkurt Günay	TUBITAK
Martin Hoffmann	NLNET

2.2 History

Version	Date	Author	Changes
1.0	26.07.2019	TIL	Final draft
1.1	26.08.2019	TIL	Updates following internal review

3. Table of Contents

3.1 Table of Figures

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.

[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

- 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 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.

This also implies that LIGHTest cannot ensure that trust decisions made using LIGHTest technology are automatically legally valid without any further customisation, configuration, or tailoring to the challenges of each use case, in the same way that a word processor also cannot ensure that a contract written through the software is legally valid. 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, including in relation to eIDAS compliance.

As is explained in D2.10 in detail, part of the piloting of LIGHTest consists of integrating certain eIDAS trust policy information into the DNS. More explicitly, Article 22.1 of the eIDAS Regulation requires Member States to publish trusted lists containing at least the qualified trust service providers which are supervised in that Member State. The Regulation and its implementing decisions require that these trusted lists of Article 22.1 must be published using a technical specification that has been standardised and harmonised, namely the European technical specification (ETSI TS 119 612), which must mandatorily be used under an implementing decision of the eIDAS Regulation[2].

This implies that the reimplementation within LIGHTest of these trusted lists via the DNS constitutes a small but not insignificant variation on the requirements of the eIDAS Regulation: the authoritative lists are published by the supervisory bodies at the URLs identified by them, whereas LIGHTest aims to make them discoverable via specific pointers within the DNS. This is in itself not a big change: the URLs at which the supervisory bodies publish their schemes are publicly known, and there is no constraint with the law on how these URLs should be approached. Discovering trust schemes via a LIGHTest DNS tool is not contrary to the eIDAS Regulation: the aforementioned article 22 of the Regulation requires that each Member State establishes, maintains and publishes trusted lists in a secured manner in a form suitable for

[2] Specifically, Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) 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

automated processing. Furthermore, it requires the European Commission to make this information available to the public, through a secure channel, in electronically signed or sealed form suitable for automated processing. Both of these provisions could be satisfied through the use of LIGHTest technology; this simply constitutes a small variation of how the authoritative trust lists are discovered.

However, LIGHTest goes beyond this process, and not only attempts to discover national trust lists governed by the eIDAS Regulation through the DNS, but also trust policies that determine how the national trust lists are used. To give a practical use case that LIGHTest pilots: the CORREOS pilot can use electronic signatures and electronic registered mail services which are referenced through national trust lists. In this case, the trust policy must not only reference the relevant trust list – which will include the Spanish official trust list which can be consulted via https://webgate.ec.europa.eu/tl-browser/ - /tl/ES, although other trust lists can be arbitrarily added – but it must also reference additional rules applied by the service provider, e.g. detailing how customers are identified (both senders and recipients), and/or how the time of sending/receipt is established. These elements are use case specific, and cannot be found directly in EU level legislation.

Since LIGHTest is not a supervisory body, the pointers introduced by LIGHTest to trust lists are not legally authoritative. Similarly, translations which are implemented via LIGHTest do not have any automatic legal authority behind them: while LIGHTest could be used e.g. to indicate equivalence between European qualified electronic signatures and non-European electronic signatures, this would be merely the opinion of a Trust Translation List Provider that established the translation. Similarly, delegation information discovered via LIGHTest is not legally authoritative, and principally reflects the information available to a Delegation Authority. None of this information is necessarily legally recognised under EU law.

Note that this does not imply that referencing trusted lists or translations in DNS is somehow unlawful or forbidden, but only that the information that LIGHTest will make available via the DNS is not legally authoritative: the only official trusted lists and trust translations are those published by competent authorities, whereas the LIGHTest information can only be considered a pointer to this information.

The result is that the LIGHTest pilots related to eIDAS can operate in practice, but only on a contractual basis. Ultimately, LIGHTest technology could be used to reference official trusted lists in an authoritative manner as well, the only requirement being that the aforementioned legislation (i.e. the European Commission's implementing decision) should then reference the use of the DNS as piloted by LIGHTest as a requirement for publishing trusted lists. Assuming that the LIGHTest piloting is completed successfully, this would be a potential path to sustainability for LIGHTest within the eIDAS context.

Given that legislative changes cannot be delivered by or within LIGHTest, this deliverable explains which legal assurances can be provided and how this was done in LIGHTest in practice. 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 has used to run its pilots (Chapter 6), including in relation to publication, translation and delegation. These tools – notably a series of checklists and templates of terms and conditions – can of course also be used after the completion of LIGHTest (or in parallel to LIGHTest) by third parties for use cases that will not be piloted in LIGHTest itself, such as the trade association example mentioned above, or 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.

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.

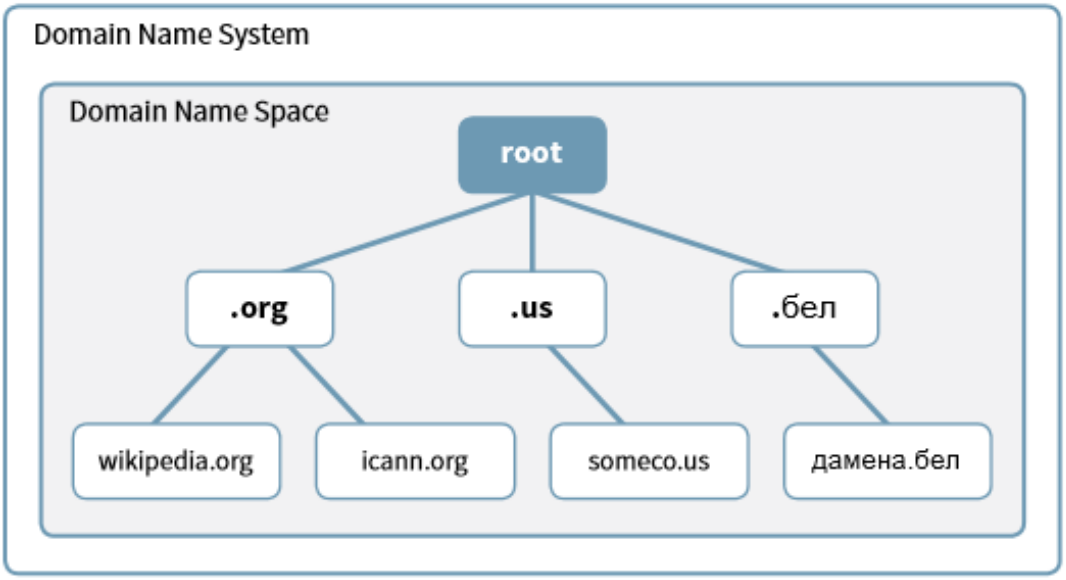

Figure 1: Domain Name System – Source: https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf

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 1) 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[3].

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

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

over the Internet to the DNS to find the website. The first server the query interacts with is the 'recursive 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[4], 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".[5] 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.

[4] See https://www.iana.org/dnssec/icann-dps.txt
[5] 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[6]:

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.

[6] 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.

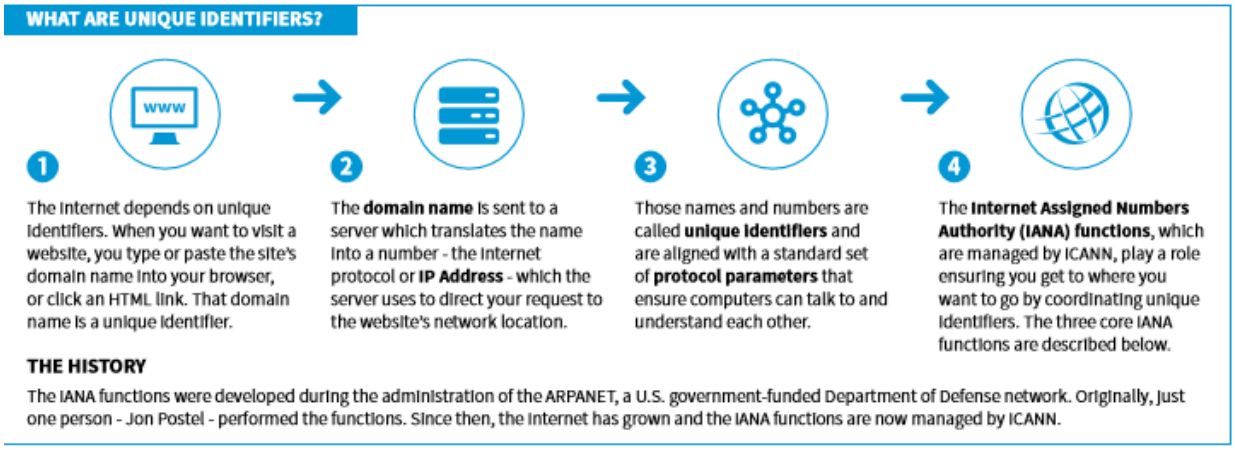

Figure 2: Understanding unique identifiers

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 and GNSO 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.

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

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)

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

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

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. 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

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[8]:

- 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:

[8] Source: https://tools.ietf.org/html/rfc5434

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 unauthorised 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 needs 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 explain how this has been done.

6. The legal toolbox of LIGHTest

6.1. Introduction

The sections above have explained the general difficulty of defining the exact legal requirements of each individual use case of the LIGHTest technology. LIGHTest has established a legal toolbox consisting of the instruments needed to deploy LIGHTest in any use case. As will be further explained in the section below, these consist of:

- A legal checklist (or more formally, 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 (including any specific applicable legislation). This will be further explained in section 6.2 below.
- Model terms and conditions that can be used as a template by aspiring LIGHTest users in order to set up the necessary contractual terms to allow the various LIGHTest functions and stakeholders to operate. This will be further explained in section 6.3 below.

It would not be possible to create one single checklist and one single template for terms and conditions that would cover all use cases. LIGHTest aims to support multiple functionalities, each of which has different stakeholders which are confronted with different legal challenges. At a minimum, the checklist and model terms must be tailored to these different functionalities. The graphical overview below summarizes these as follows:

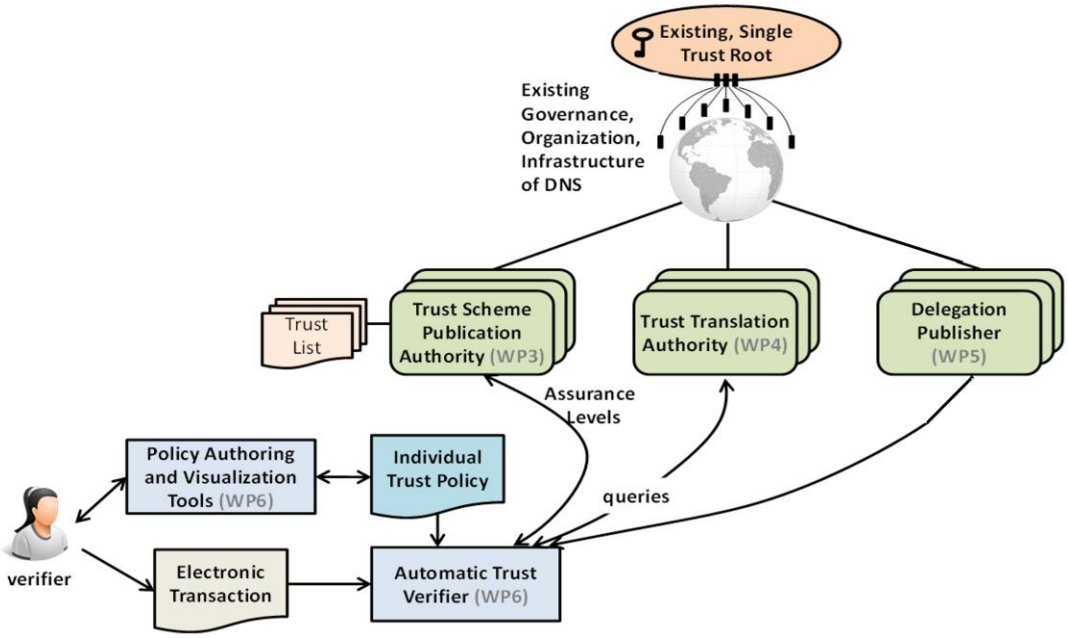

Figure 3: LIGHTest conceptual model (source: D3.1)

Three key functions are identified in this graphical overview, marked in light green boxes, with the following tasks (which may exist in combination in any given use case):

- A Trust Scheme **Publication** Authority makes trust schemes available, i.e. the rules stating whether, from its perspective and based on any laws that apply to the Authority, a specific class of transaction is trustworthy. It does not make decisions itself, but merely provides a set of rules that other parties may choose to rely on in its decision making.
- A Trust **Translation** Authority provides the translations of one specific known trust scheme (the Trusted Scheme) to at least one other (the Recognized Scheme), i.e. it allows relying parties to determine whether, based on the assessment of the Authority, the rules of a recognized scheme are equivalent to those of a known trusted scheme. It does not make decisions in relation to transactions itself, but provides a statement of equivalence between schemes.
- A **Delegation** Publisher provides references to delegation information (e.g. rights to represent a company or any individual for a specific purpose) which are stored by a Delegation Provider in a standardised format.

These three functionalities – publication, translation and delegation – differ sufficiently between each other to make it unviable in practice to define a single checklist for legal requirements and one single template for terms and conditions. For this reason, each function has been given a dedicated deliverable with separate checklists and separate model terms:

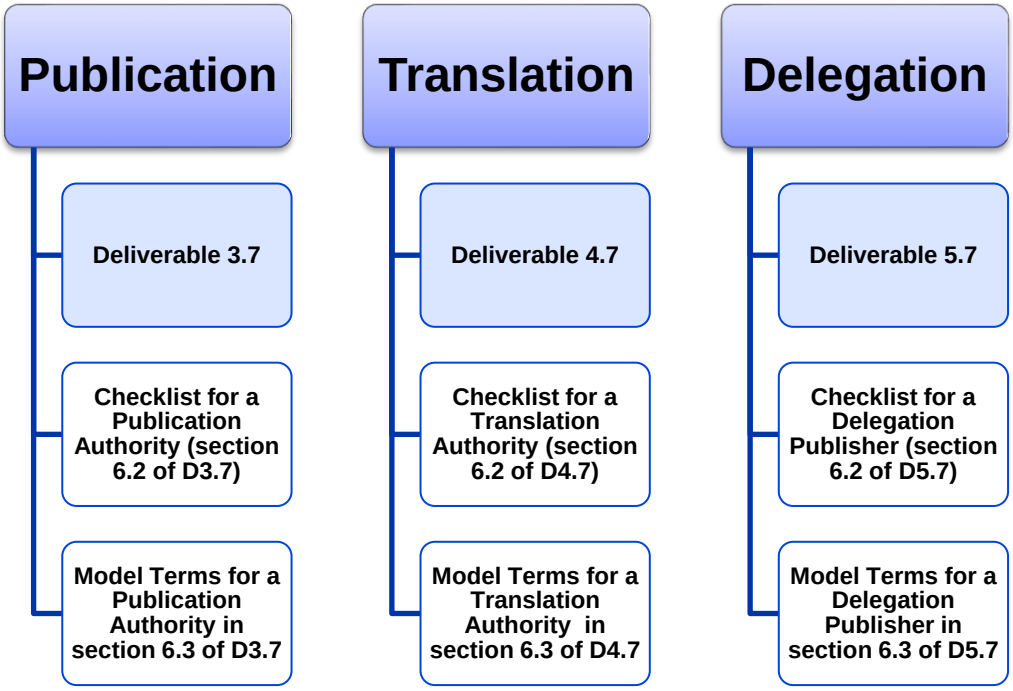

Figure 4: Structure of the legal tools

Collectively, these three deliverables allow any LIGHTest authority to identify their legal constraints and to draft up relevant contractual terms with relative ease.

6.2. Checklists – the need for case by case assessment

As was explained in D2.10, a key challenge for LIGHTest is that it is fundamentally a technology for the discovery, validation and translation of trust information. While the use cases that will be

piloted within LIGHTest are centred around the eIDAS context, there are many applications of the LIGHTest technology which do not involve trust services as defined within eIDAS.

Deliverable D2.3 - Requirements and Use Cases explored some of these in detail, but by way of a simple example: an European trade association could use LIGHTest to publish a list of its member companies and their categories of activities, thus allowing relying parties (consumers, companies and public authorities alike) to find and validate this information easily. In an international context, an international trade association could even use LIGHTest to link to European, American and Chinese trade associations, who in turn use LIGHTest to publish their members. In this way, LIGHTest is used for publication and validation of trust information by the regional trade association (who identify their respective trusted members), and for trust translation by the international trade association (who identifies the trusted regional trade associations). In these cases, neither data protection law nor eIDAS is relevant.

Since the number of application areas is practically unlimited – LIGHTest can be used whenever trusted information must be discovered, validated or translated – it is also not possible to abstractly list out all possible legal requirements. Therefore, it is also not possible to draft up a single contract or a single declaration that would be suitable for all LIGHTest use cases.

None the less, 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:

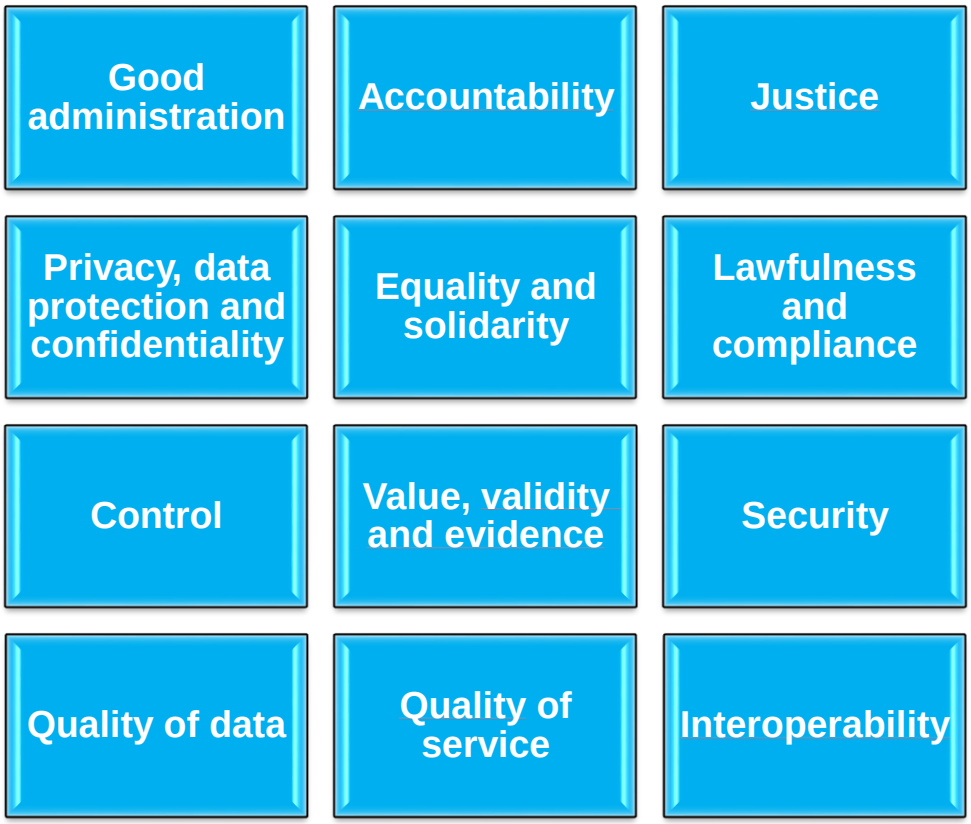

Figure 5: Canvas of the assessment framework

On the basis of this canvas, the following principles were derived, as was explained in D2.10:

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**: • LIGHTest technology must be implemented in a way that ensures non-discrimination: trust information must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving party on the basis of the trust information.

	• LIGHTest technology must be implemented in a way that ensures transparency: the trust information to be transferred, its origins and meaning must be clearly known to the recipients. • LIGHTest technology must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving party to make any decisions on the basis of the information received, it must at least be able to semantically interpret the information.
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**: • LIGHTest technology must be implemented in a way that ensures that all participants are aware of their obligations and responsibilities, and notably what assurances are provided behind the communicated trust information. • The persons relying on LIGHTest technology must have the right to restitution of any damages caused by noncompliance with these obligations insofar as this is possible under applicable law and the contractual terms of the entity using LIGHTest.
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**: • LIGHTest technology must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of trust information exchanged via LIGHTest. • LIGHTest technology must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on LIGHTest as recipients or as relying parties on trust information communicated via LIGHTest.
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**: • LIGHTest technology should be implemented in a way that

	avoids the publication of personal data via the DNS, as explained in Chapter 3 of this report.
	• Any personal data processing in relation to the use of LIGHTest technology may only occur in accordance with applicable data protection law, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:
	  ○ lawfulness, fairness and transparency;
	  ○ purpose limitation;
	  ○ data minimisation;
	  ○ accuracy;
	  ○ storage limitation;
	  ○ integrity and confidentiality;
	  ○ accountability.
	• The requirements of Chapter 3 must at all times be adhered to.

Equality and solidarity	**Description**: LIGHTest technology must be implemented in a way that protects the persons concerned against discrimination. **Requirements**: • LIGHTest technology must be implemented in a way that ensures non-discrimination: trust information must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving entity on the basis of the trust information. • LIGHTest technology must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as any other persons benefiting from LIGHTest technology.
Lawfulness and compliance	**Description**: LIGHTest technology must be implemented in a way that ensures that trust information is only published, validated and interpreted in accordance with any specific legislation or other legal requirements that may apply to that trust information. **Requirements**: • Trust information may only be published, validated and interpreted through LIGHTest technology if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied, including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security, assurances or exclusions of liability, data or service quality

	arrangements, etc. The necessary contractual terms have to be implemented to ensure that these requirements are adhered to.
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**: • Appropriate audit and logging measures must be implemented to ensure that any use of trust information which is made available via LIGHTest can be verified by competent authorities 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**: • There must be an agreement between service providers and relying parties on the legal value and validity of the trust information, including specifically whether it can be considered authoritative (as is e.g. the case for trust list information in relation to qualified trust service providers), 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**: • Users of LIGHTest technology must follow LIGHTest's security measures and protect their infrastructure through appropriate technical and organisational measures to ensure a level of security appropriate to the risk. • Incident response measures must be implemented to ensure that the exchange of compromised trust information through LIGHTest is avoided, and can be notified to recipients if an incident should occur.
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**: • A legal framework must exist that clarifies the obligations of the participants in the use case in relation to the quality of the trust information, 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 entity at the source of the trust information 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 exchange of trust information. **Requirements**: • A legal framework must exist that clarifies 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). • An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary.
Interoperability	**Description**: LIGHTest technology must be implemented in a way that ensures semantic and technical interoperability of the trust information exchanged via LIGHTest. **Requirements**: • Appropriate agreements must be in place with respect to the technical and semantic characteristics of the trust information, taking into account linguistic challenges and diversity of legal systems. Trust information should not be exchanged using LIGHTest if interoperability is not ensured.

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. This also reduces the usefulness in practice of this checklist. For that reason, a more specific version of this check list

has been created in each of the three aforementioned deliverables, focusing the principles more narrowly on only those questions that are particularly relevant for entities that publish, translate, or reference delegations using LIGHTest technologies. In practical terms, these check lists 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.

6.3. Creating contractual frameworks for trust policies and trust decisions

In line with the general approach outlined above, a series of template Terms and Conditions have been created for a Publication Authority in section 6.3 of D3.7, for a Translation Authority in section 6.3 of D4.7, and for a Delegation Publisher in section 6.3 of D5.7. While the details differ slightly, globally these templates follow a common structure that can be summarised as follows:

- **Preamble – Nature and goals of the Terms**: this section explains what the referenced scheme is intended to do, where it can be found, and who provides and maintains it.
- **Description of the Scheme:** this section explains what information can be obtained via the scheme.
- **Availability and permissible use of the Scheme:** this section explains who may rely upon the scheme, how it may be used, and also which uses are explicitly forbidden.
- **Changes in the Scheme and in these Terms:** this section explains any evolutions in the scheme or in the Terms, including how they are communicated and when changes enter into force. It also indicates whether and how the Authority or Publisher has the right to terminate the scheme.
- **Guarantees, warranties and liabilities in relation to the Scheme:** this section explains which responsibilities the Authority or Publisher undertakes and what assurances it provides (including in terms of availability, quality of the information and its legal value), and inversely which responsibilities and risks remain fully with the relying party.
- **Costs, fees and charges in relation to the Scheme** explains whether there are any costs related to the use of the Scheme, and if so, which.
- **Intellectual property rights to the Scheme** indicates whether any intellectual property rights are claimed by the Authority or Publisher, and which licence rights are granted to the relying party.
- **Data protection and privacy** governs whether any personal data is involved in the scheme, and if so, ensures that usage complies with the requirements of the GDPR.

- **Other terms** cover generic provisions that can be found in any contract, e.g. in relation to applicable law and dispute resolution.

This structure is applied consistently in all three sets of model terms, although of course details vary substantially. The topic of data protection and privacy is, by way of example, crucially important for delegation information, given that the processing of personal data is almost inevitable when the information describes the rights of one person to represent another. As a result, for Delegation Publishers this section is significantly larger and more complex than for Publication Authorities and Translation Authorities, neither of whom would process significant amounts of personal data as a general rule.

In all use cases, the texts should be reviewed by any aspiring user to assess their suitability for a specific context – including any issues identified through the check lists - and some tailoring is inevitable. To assist in that process, the template terms contain comment boxes indicating where customisation is particularly essential.

Fundamentally, the legal value of LIGHTest in relation to trust policies and the value of trust decisions taken on the basis of them is determined by the terms and conditions under which trust policies are made discoverable in LIGHTest. The resulting assurances can range from none at all ('information is 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 policy is guaranteed to be complete, correct, available at all times, authentic, and we warrant that it is suitable to support decisions taken on the basis of it'), with many possible nuances in between.

It should be noted that, as with any trust policy, the terms and conditions principally serve to make it clear for any relying party to what extent they can base their own trust decisions on the policy. The objective of LIGHTest after all is not to move all responsibility and liability to the entity making its trust policy available.

However, this does not imply that a decision maker (who may be an average consumer) is merely pointed by LIGHTest in the direction of a series of policies and is forced to make his or her own decisions. In most cases, software or automated services should be available that discover the policies and can support the decision-making process, even assuming the risks and responsibilities of the decision maker to some extent. This is the principal way in which LIGHTest can make it easier to find trust policies and to make justified trust decisions, which is one of the main drivers behind LIGHTest.

6.4. Looking towards the future: integrating LIGHTest into new legislation

Throughout the LIGHTest project, care has been taken to ensure that LIGHTest technology has been applied in accordance with applicable laws, both at the national and EU level, and that terms and conditions have been aligned with such laws. As already explained above, in the LIGHTest pilot areas, compliance with the European eIDAS Regulation – and to a lesser extent with national laws in relation to trust services and electronic communication – was the primary requirement.

In practice, this was less burdensome than might have been thought. The national trust lists under the eIDAS Regulation, which are the main trust schemes used in LIGHTest pilot areas, are well regulated and publicly available at URLs which are actively disseminated and promoted[9]. Establishing a DNS server with records that point to relevant trusted lists is relatively trivial, once the LIGHTest infrastructure had been designed and implemented. While these records themselves have no specific legal authority behind them, the trust lists themselves do, under Article 22 of the eIDAS Regulation which stipulates as follows:

Article 22 - Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. ***Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing****.*

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and ***details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto****.*

[9] See https://webgate.ec.europa.eu/tl-browser/#/

*4. The **Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing**.*

In other words, no part of the eIDAS Regulation precludes the use of the DNS (as LIGHTest does) to discover trust lists, since they are secured, signed through the DNS Security Extensions (or DNSSEC) – which legally qualify as a seal under EU law – and manifestly suitable for automated processing, since this is the heart of LIGHTest. The fact that the DNSSEC seal is not created by a national supervisory authority – as is the case for current trusted lists – is not legally problematic under the eIDAS Regulation, since this is not a legal prerequisite.

However, any LIGHTest DNS Server pointing towards the existing national trust lists is by definition not authoritative. The lists that it would reference have a specific legal status, but the DNS pointers themselves and the related service would not. This is only logical, since conceptually anyone could set up such a DNS Server, and set up an attack whereby the DNS records point to fake or corrupted trust lists. The only authoritative listing of trusted lists is therefore the one that the Commission maintains under paragraph 4 quoted above, which refers to the authoritative national lists, and which must comply with the requirements of a specific Implementing Decision of the eIDAS Regulation[10].

This Implementing Decision contains several requirements which are not problematic. It requires trusted lists to follow the format of the technical specification ETSI TS 119 612, as stated in Article 1 and Annex I of the Implementing Decision. The technical specification is not a problem as such – a DNS record could simply reference a trust list formatted in accordance with this specification.

The Implementing Decision also requires that the national trust lists are signed or sealed by a Member State, and that the European trust list is signed by the European Commission. Neither of these requirements poses a problem for LIGHTest: while DNSSEC signatures would be applied to the records, this part of the process is not covered by the Implementing Act. Only the trust lists themselves must be signed or sealed by the Commission or by the Member States, and this could still be done: DNSSEC signed pointers would reference the trust lists which are

[10] Specifically, Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) 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

signed or sealed by the Commission or by the Member States, in perfect compliance with the eIDAS Regulation and the Implementing Act.

However, there is one legal barrier that would stop Member States and the European Commission from being able to migrate to LIGHTest technology in the current state of play: the Implementing Act notes that:

*(3) Pursuant to Article 22(4) of Regulation (EU) No 910/2014, the Commission shall make available to the public, through a secure channel **to an authenticated web server**, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed form suitable for automated processing.*

*(4) The Commission may make available to the public, through a secure channel **to an authenticated web server**, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed human readable form.*

The Commission and Member States therefore would not have the possibility to use LIGHTest technology to reference the trust lists as the Implementing Act requires, since the Act requires authenticated *web* servers, not *DNS* servers. While this doesn't forbid the Commission or Member States from also running DNS servers with appropriate pointers to the applicable trust lists, these would not be authoritative; only the authenticated web servers would be considered legally official.

A simple and very minor fix would be to suppress the reference to *web* servers in these provisions, i.e. to amend the Implementing Act to simply read:

*(3) Pursuant to Article 22(4) of Regulation (EU) No 910/2014, the Commission shall make available to the public, through a secure channel **to an authenticated server**, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed form suitable for automated processing.*

*(4) The Commission may make available to the public, through a secure channel **to an authenticated server**, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed human readable form.*

This would allow the Commission and Member States to rely on DNS servers or web servers as desired, thus creating a choice between the LIGHTest technology and the current approach. Alternatively, the text could refer to authenticated *DNS* servers only, but this would again remove all flexibility, which is not generally desirable from a policy perspective.

While this is only one example of how LIGHTest could be embedded in or at least tolerated by legislation, other examples might be given. Beyond the eIDAS Regulation, a notable use case at the EU level would be the Business Registers Interconnection System (BRIS), which – as the name suggests – ensures that national business registers with company information can communicate and that search queries involving standardised information can be dealt with by each of them. The System is based on the BRIS Directive 2017/1132/EU establishing the general principles of the system, and on Regulation (EU) 2015/884 setting out technical specifications and procedures. Here too, the Commission could essential use LIGHTest as a technology for referencing business registers that satisfy the trust scheme created under the Directive (as a Publication Authority in the sense of LIGHTest), and the business registers individually referencing delegations to represent companies (as Delegation Publishers in the sense of LIGHTest).

The principal requirement to do so would not necessarily be that a DNS based referencing system would be incorporated as a requirement in legislation, but rather that the legislation would remain perfectly neutral on this point, so that the trust validation model established by LIGHTest could be used as well. In this way, LIGHTest could potentially become a staple technology for validating trust and supporting justifiable trust decisions, without necessary limiting future innovations. That approach could represent a useful policy step forwards for the European Union.

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

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

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.