D3.7

Cross-Border Legal Compliance and Validity of Trust Scheme Publication

Document Identification	
Date	31.08.2019
Status	Final
Version	1.1

Related WP	WP3	**Related Deliverable(s)**	D3.6, D2.9, D2.10, D6.7
Lead Authors	Hans Graux, Edwin Jacobs (TIL)	**Dissemination Level**	PU
Lead Participants	TIL	**Contributors**	OIX
Reviewers	UPRC, ATOS		

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 for making a decision on whether a transaction can be trusted or not.

Without focusing on the more complex cases of trust translation (examined in D4.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Translation (2)) and delegation (examined in D5.7 - Cross-Border Legal Compliance and Validity of Delegation (2)), decisions on whether to trust a transaction or not are taken by applying the rules of a trust scheme to a transaction. Trust schemes 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 schemes have a clear legal background (e.g. the legal framework governing trust services in the EU is created by the eIDAS Regulation[1]), trust schemes 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.

In the first version of this deliverable (D3.6 – Cross-Border Legal Compliance and Validity of Trust Scheme Publication (1)) which was produced in the first year of the project, we explored the legal challenges in relation to the publication and subsequent discovery of trust schemes 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 the trust schemes which are discovered via the DNS through the LIGHTest framework.

[1] 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

In the present deliverable, which is an updated version of D3.6, we provide the tools for establishing this legal solution, in the form of a standardised legal document that can be used in any situation where trust schemes are published and made available for discovery by 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 forms 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 deliverable 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.

2. Document Information

2.1 Contributors

Name	Partner
Hans Graux	TIL
Edwin Jacobs	TIL
Andriana Prentza, Jerry Dimitriou, Maria Siapera, Kostas Douloudis	UPRC
Javier Presa Cordero	ATOS

2.2 History

Version	Date	Author	Changes
1.0	26.07.2019	TIL	Draft for review
1.1	29.08.2019	TIL	Final updates after 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[2]. The trust policy is therefore simple and consists of the rules of the eIDAS Regulation which act as the trust scheme. The trust decision can therefore be correspondingly simple and will typically be 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 not. No notable margin of appreciation exists.

[2] 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 other 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, or a signed invoice – 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 and has passed a prior registration and identification process, 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 schemes 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 or tailoring to the challenges of each use case, in somewhat 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 by default; it must be set up and configured 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 deliverable 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[3].

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.

[3] 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

Discovering trust schemes via a LIGHTest DNS tool is not contrary to the eIDAS Regulation, and 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 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 the trust lists or to any other trust schemes are not authoritative. Note that this does not imply that referencing the published trusted lists 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 are those published by the Member States at the URLs identified by them, 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 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.

This deliverable describes how such a contractual framework can be established by a scheme publisher, 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 by interested users after the termination of the LIGHTest project 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 deliverable 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.

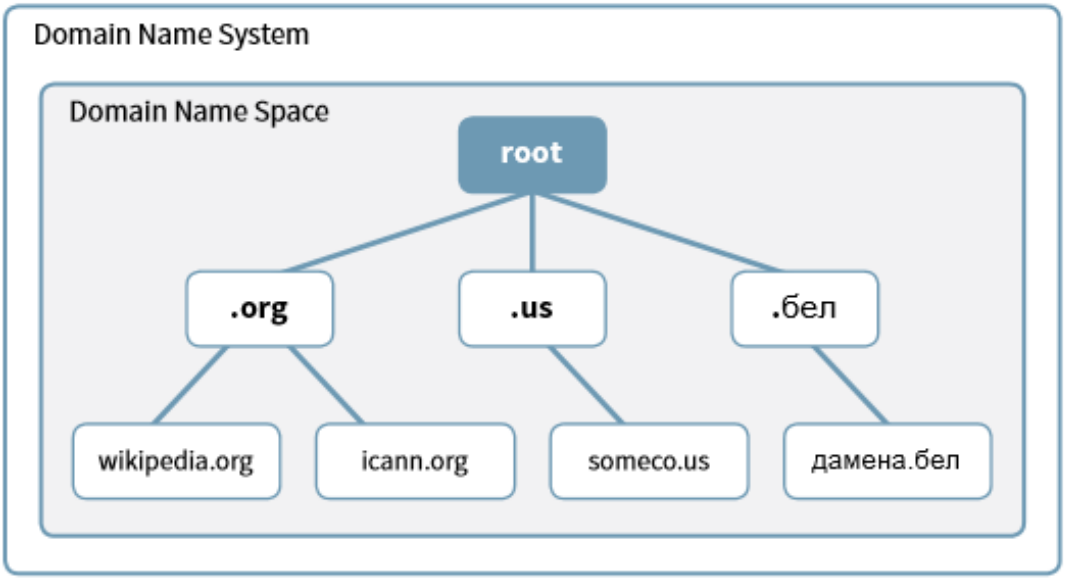

Figure 1: Domain Name System – Source: https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf

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[4].

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

[4] 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[5], 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".[6] 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 the 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.

[5] See https://www.iana.org/dnssec/icann-dps.txt
[6] 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. The changes are either 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[7]:

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.

[7] 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 evaluates requests to change operators of country code domains as well as day-to-day maintenance of the details of the existing operators.

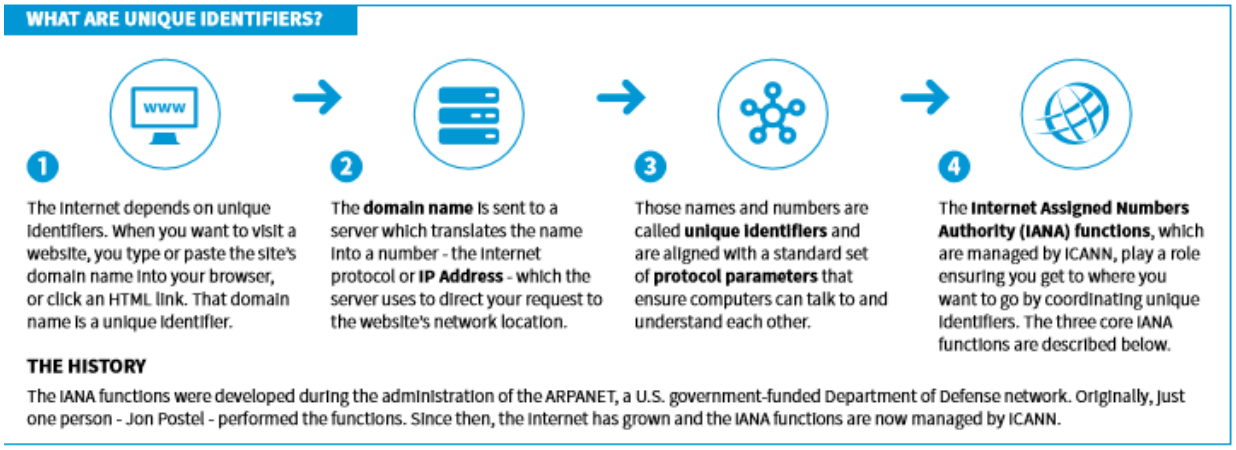

Figure 2: Understanding unique identifiers

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 policies 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."*[8] 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 groups and

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

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[9]:

- 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:

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

1. A 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 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. In order to help address this problem, deliverable 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 trust scheme publication:

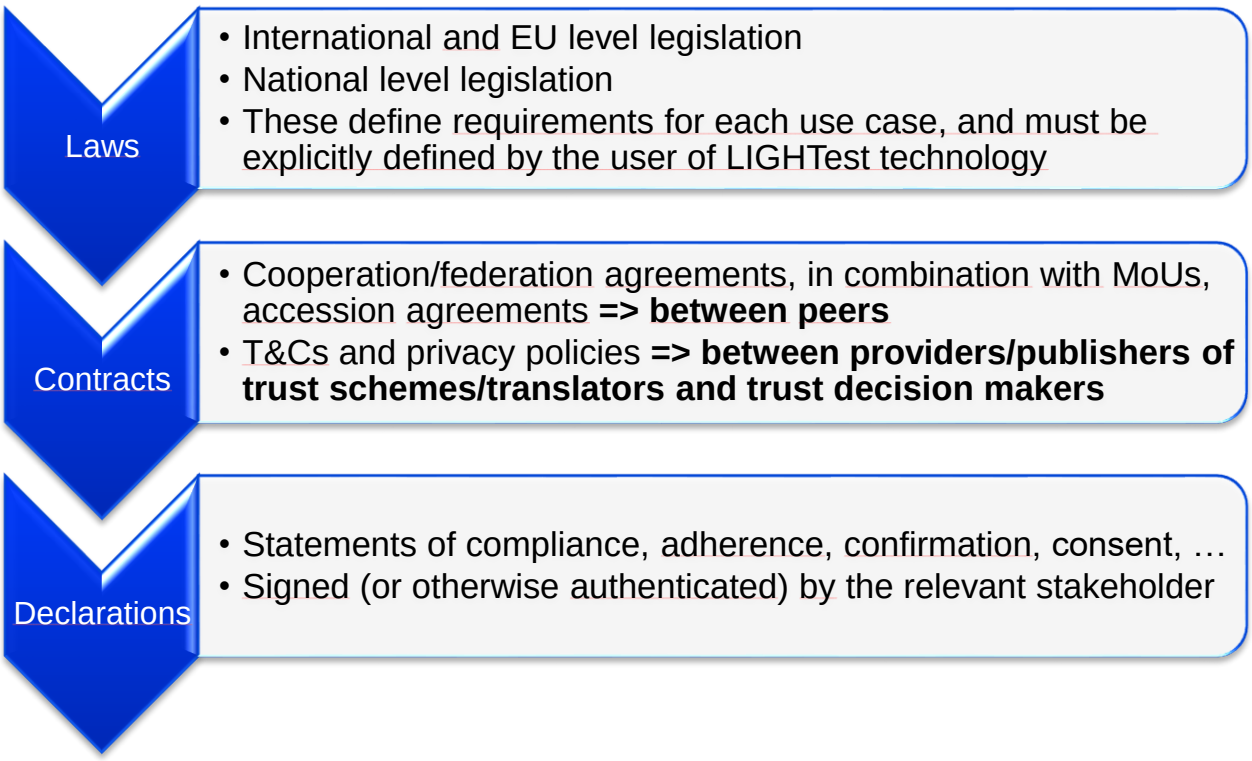

Figure 3: Logical model of the LIGHTest legal toolbox

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 – are considered static and immutable, in the sense that LIGHTest has no reliable way to change them in the course of the project.

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 deliverable 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 referencing authority.

For the avoidance of doubt, it is repeated that this deliverable *only* examines the legal challenges in relation to the publication of trust schemes. Other legal challenges in relation to decision making, delegation and trust translation are addressed in deliverables D5.7, D6.8 and D4.7, respectively; and ethical issues (including data protection compliance) are examined in D2.11. Furthermore, trust schemes must of course be drafted and published before they can be referenced; this is dealt with in deliverable D6.5 - Open Source Tool for Visualization and Editing of Trust Policies. The present deliverable assumes that a trust policy has been created that captures the concerns and priorities of the publishing entity, which can thereafter be applied by any relying party as a part of a trust policy to an electronic transaction, resulting in a trust decision.

Section 5 explained how the DNS operates as a system of open standards, which in effect allows the operator of any domain to create subdomains and pointers within that domain to information of any given nature. By way of a practical example, a company that controls the domain

companyname.eu can create subdomains such as activities.companyname.eu, or personnel.companyname.eu. These subdomains can contain a regular website, or they may point to structured resources. The model behind LIGHTest is that a subdomain such as scheme.companyname.eu could be used to point to a specific trust scheme which is owned, controlled, endorsed or simply used by the controller of companyname.eu.

The use cases that will be piloted within LIGHTest are centred around the eIDAS context, and the use of LIGHTest to discover trust scheme information is therefore conceptually relatively straightforward. As was explained in D2.10 (Legal and ethical requirements), the eIDAS Regulation establishes a clear trust management framework in relation to trust services. Specifically:

- Means of electronic identification, once they are notified by a Member State, undergo a peer review process by other Member States which takes one year, culminating in the publication of the means of electronic identification in the Official Journal (Article 9 of the eIDAS Regulation).
- The most trustworthy[10] trust service providers (referred to as qualified trust service providers in the Regulation) are required to undergo biannual external audits, the result of which must be presented to supervisory authorities which are designated in each Member State. Provided that the audit results are accepted, the providers are thereafter listed in a so-called trusted list, published by the supervisory authority in a standardised EU level format (Article 22).

Electronic identification and trust services under the eIDAS Regulation thus have a relatively clear trust management model behind them: a third party can rely on notified identities and qualified trust services because their assurances are legally defined, independently audited, and the outcomes are made public via the Official Journal (for identities) and national trust lists (for trust services). The published trust information is therefore available to support trust decisions.

[10] More accurately, this obligation is incumbent only on so-called qualified trust service providers, which must satisfy harmonised requirements in the Regulation. Nonqualified trust service providers can in principle offer equal or ever higher quality services, but as they are not necessarily assessed by a third party on this point and as they are not *ex ante* supervised by national supervisory bodies either, it is up to customers to verify on a case by case basis whether they consider a nonqualified trust service provider to be suitable for their purposes. It is not obligatory for a trust service provider to become qualified; this is a market decision that the trust service provider can make, by considering whether the cost and effort of being qualified (notably the expenses of the recurring audits) are offset by the market opportunities of being qualified.

Implementing this model in LIGHTest was relatively straightforward: each Member State already publishes its eIDAS trust list online, on the website of its supervisory authority, in a harmonised format. By way of example, the Belgian national list is referenced as being located at https://tsl.belgium.be/tsl-be.xml; similar lists exist for each Member State[11]. Thus, LIGHTest use cases could simply create a pointer in trust policies to the relevant scheme at tsl.belgium.be (and similarly at e.g. tsl.austria.at, tsl.germany.de, tsl.gov.uk, and so forth). In this context, the trust model remains intact: electronic identities would still be notified and assessed as eIDAS requires, and qualified trust services would still be audited and supervised by national supervisory bodies. But rather than publishing the outcome only in the strictly European Official Journal and trust lists, the outcome is then referenced directly via a trust scheme which is discoverable via the DNS as well. This would still allow third parties to access and validate the information, since only the medium of discovery of the trust information changes. More importantly, other trust lists in other areas of the world (including outside the EU) can easily be integrated in a trust scheme simply by adding a new pointer to the relevant trust list (e.g. in relation to trusted identities in China, or trust services in the USA – one might easily imagine tsl.china.cn or tsl.usa.gov), thus facilitating interoperability without having to adhere to a European ruleset or standard.

Beyond 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: a European trade association could use LIGHTest to publish a list of its member companies and their categories of activities (e.g. at members.associationname.eu) 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 (network.associationname.org), 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). Or as a more basic example, ceo.companyname.eu could directly link to identifying information for a specific company; this type of use case is examined in greater detail in D5.7 - Cross-Border Legal Compliance and Validity of Delegation (2).

This short overview serves to permit a few key observations to be made with respect to the legal compliance and validity of the publication of trust schemes. Firstly, the number of application areas

[11] The European overview linking to all national lists is published at https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xm

is practically unlimited: LIGHTest can be used whenever trusted information must be discovered by a relying party. Given this openness, it is also not possible to abstractly list out all possible legal requirements, which might vary from case to case. Continuing the examples above:

- In the eIDAS cases where information from the official eIDAS trust lists is made discoverable via the DNS, there is an absolute need for the DNS pointers to be authoritative and accurate. The information that the pointers link to must consist exclusively of the official eIDAS trust lists, with perfect integrity. There is no margin for error, or at least none more than for the currently existing trust lists;
- In the trade association example, legal requirements might be noticeably lighter. The information is not regulated as such, and the trade association itself can define its own responsibilities and liabilities. It may decide to make the scheme available on an 'as-is' basis, without any binding assurances of accuracy, and without liabilities behind it. This may be perfectly appropriate for some cases.
- In the company representation example, the information may not have any legal value, since the identification of managers is regulated by company law and managed via business registers. Unless legislation on this point is changed, the use of subdomains such as ceo.companyname.eu can be practically useful, but has no legal value, other than being a claim made by the controller of the companyname.eu domain.

As a second important consideration, it should be noted that the use of the DNS to make such information discoverable infers no inherent legal validity and provides no assurances of compliance. For this reason, LIGHTest provides tools that allow a user to identify their legal requirements (section 6.2 below) and to translate these into a usable contract towards relying parties (section 6.3 below).

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, deliverable 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 deliverable D2.10:

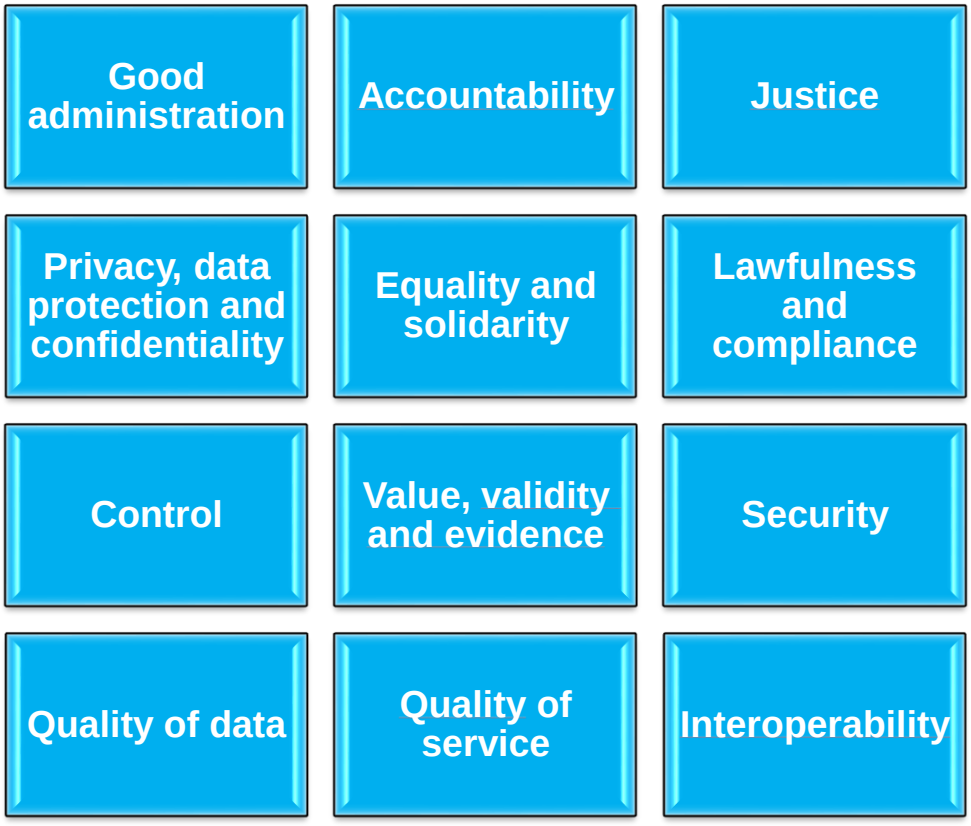

Figure 4: Canvas of the assessment framework

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 trust scheme publication, 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 publish trust schemes 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 trust scheme itself, which may not contain unlawful discriminatory provisions. • Transparency must be ensured; this also implies that the terms must be written in a manner which is comprehensible to the intended audience. These may be administrations, businesses or citizens, with or without prior knowledge of the context.
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 publishing entity in relation to the trust scheme. • This also includes any right to restitution of any damages caused by errors in the trust scheme.
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, trust schemes should not contain any personal data as defined under EU law. This rule should only be broken after a data protection impact assessment is conducted; this issue is further explored in T2.7 – D3.
Equality and solidarity	**Description**: LIGHTest technology must be implemented in a way that protects the persons concerned against discrimination. **Requirements**: • Trust information must be transferred on a neutral basis, without prejudicing any decisions that would be made by the relying party on

	the basis of the trust information. The contractual terms should make it clear that they address only publication, not the subsequent decisions made by the relying part. • 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 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**: • 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 trust scheme must be explicitly described in the contractual terms, 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**: • 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 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**: • 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 trust scheme 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 trust scheme publications 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

The need for contracts in LIGHTest stems mainly from the requirement to provide clear legal rules between the owners and publishers of trust policies, trust schemes and trust translations on the one hand; and towards trust decision makers on the other hand.

This specific deliverable is centred around the publication of trust information, and notably of trust schemes. The section above has already shown that the principal requirement is that relying parties – those that wish to discover and use the trust scheme – must know precisely what its legal value is, and whether it satisfies their legal requirements. Conceptually, this can be done through terms and conditions applied by the publisher of the trust scheme. This allows the publisher to tailor the legal assurances to its possibilities, means, and needs of its constituency. As noted above, in many cases a 'best efforts' commitment might be sufficient, whereas in other cases a binding commitment may be required on e.g. the quality of the information, its availability, compliance with data protection law or other laws (such as the eIDAS Regulation), approval of specific legal authorities or supervisors, and so forth.

Conceptually, it is worth underlining that the model contractual terms provided hereunder are intended to be used by the trust scheme publisher, i.e. the entity (usually a company or organization) that wishes to allow relying third parties to use the trust scheme. The trust scheme publisher is not necessarily the entity that actually created the trust scheme. It is perfectly possible that the trust scheme was established by a third party, and that the trust scheme publisher simply chooses to rely upon it in unmodified form. By way of example: a trust scheme may be used by a company to describe under which conditions invoices will be considered trustworthy, and therefore when they will be paid. It is possible that the company drafted and published its own policy. It is however equally possible that a third party – e.g. a vendor of automatic invoice processing software – to predefine a policy that the company simply relies upon without modifications, since the standard trust scheme is adequate for its purposes.

From the perspective of a relying party however, this distinction is not relevant: it merely wishes to know whether a specific trust scheme can be used, and which trust decision must thereafter be made. The origins of the trust scheme are not relevant.

It should furthermore be emphasised that the scope of LIGHTest is not to critically assess, improve or otherwise modify trust schemes. From the perspective of this deliverable, trust schemes 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 trust schemes discoverable via the DNS and to make trust decisions on the basis of them. Therefore, contractual terms should not relate to the contents of trust schemes. The trust schemes will be published by the users of LIGHTest, typically on a website, and are unaffected by LIGHTest. The project's concern is ensuring the availability, findability and usability of the policies.

In addition, LIGHTest also cannot control any uses made of the published trust schemes: 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 integrating pointers to published trust schemes on their own domains, in external documents or in PKI certificates. This cannot be controlled; however, publishers of trust schemes can control the legal risks for them by publishing their own terms.

Hereunder, a set of model terms and conditions for trust scheme publishers 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 trust scheme publication

Preamble – Nature and goals of these Terms

These terms and conditions (hereafter collectively referred to as the 'Terms') govern the use of the trust scheme relating to [*briefly describe the scope and goals of the trust scheme*] (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 Publisher 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 Publisher bears no responsibility or liability of any kind towards the User or towards any third party for such use.

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

Comment: the publisher 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 referenced by the Publisher in order to permit the User to [*describe why the Publisher makes the Scheme available to the User, i.e. what trust decisions it aims to enable*].

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 Publisher 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 Publisher'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 Publisher 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.

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, which can cause confusion in the market.

The Publisher 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 Publisher does however guarantee that the information included in the Scheme complies fully with article X of legislation Y, and the User may rely on such compliance 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 Publisher 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 Publisher has the right to temporarily or permanently terminate references to the Scheme, and to update, revise or delete the Scheme (or parts thereof). If this happens, the Publisher will endeavour – but is not legally required to do so – to provide you as the User with timely written notice in advance, for which the Publisher may rely exclusively on the website where the reference to the Scheme is made available. The notice will summarily describe such changes.

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 Publisher 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 in practice. Note that it is perfectly appropriate for some schemes to contain no binding assurances at all from the Publisher; in this case the paragraph above may simply state: "The Publisher has taken all commercially reasonable efforts and due care to ensure that the Scheme 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 Publisher, including with respect to fitness for any purpose. The Publisher cannot be held responsible or liable in any way and under any legal theory with respect to these Terms or the Scheme".

The Publisher 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 Publisher 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 Publisher 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 Publisher 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 Publisher'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.

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

The Publisher 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 Publisher, 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 Publisher 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.

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 Publisher.

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 Publisher 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 Publisher or by third parties with whom the Publisher 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 may incidentally and exceptionally result in the Publisher processing personal data in relation to you as the User, 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'). Insofar as this is the case, the Publisher as identified above shall act as a data controller as defined under the GDPR, and will only process your 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 publisher's legitimate interest in ensuring that the Scheme can operate in practice). Your personal data shall only be entrusted by the Publisher to service providers who support the Publisher in the execution of these Terms, who will be bound to the Publisher through contracts that comply with the requirements of the GDPR. No personal data of the User shall be sent by the Publisher to a third country or international organisation. The User's personal data shall be retained by the Publisher for a maximum duration of one year after the User's use of the Scheme via the Publisher's services. The User has the right to request from the Publisher access to and rectification or erasure of personal data or restriction of processing concerning the User, or to object to processing as well as the right to data portability. The User has 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: schemes generally shouldn't contain any personal data. However, accessing a Scheme via the Publisher may still incidentally result in the processing of personal data, namely the IP addresses and log data from the User who tries to obtain the Scheme via the Publisher. While this is a purely technical and routine form of data processing with minimal data protection risks, the GDPR may still 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 simply delete this information.

More sensitive data processing is likely to occur by the User itself, following its accessing the Scheme. This is however the sole responsibility of the User itself, as the last paragraph indicates; the Publisher bears no responsibility or liability on this point.

Other provisions

The Publisher 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 Publisher may not have any control over such websites and/or materials belonging to third parties, the User acknowledges and accepts that the Publisher 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 Publisher 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 its of such websites.

If the Publisher 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 Publisher 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 Publisher 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 10

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.