D2.9

Social Impact Report

Document Identification	
Date	31.08.2017
Status	Final
Version	1.1

Related WP	WP2	**Related Deliverable(s)**	D2.3, D2.10-11
Lead Authors	Hans Graux	**Dissemination Level**	PU
Lead Participants	TIL	**Contributors**	USTUTT
Reviewers	FHG, EEMA		

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

This deliverable D2.9 – Social Impact Report was produced as a part of Task 2.7: Legal, Ethical and Societal Requirements and Constraints. Within the LIGHTest project, this task is intended to identify and address the ethical and societal implications of LIGHTest. Legal and ethical requirements are assessed elsewhere, notably in D2.10 - Legal, Ethical and Societal Requirements and Constraints. This deliverable focuses on the potential societal implications of LIGHTest, describing and assessing briefly how LIGHTest can impact society positively or negatively.

As this deliverable will explore, LIGHTest is predicated on the concept of supporting trust management (including discovery of trust information, trust translation and trust validation) as a way of supporting trust decision making, using the global DNS infrastructure as a communications tools for trust information. The improvements that LIGHTest brings can affect any application area in which trust decisions must be made, ranging from basic questions ('does this person work for this company?') to more complex issues ('does this electronic order form respect my requirements in relation to electronic signatures and identity of the customer?') or even highly nuanced policy issues ('is this diploma issued by that university on a different continent equivalent to a diploma from my own country?').

In all of these cases, LIGHTest can be used to discover trust information ('what are the rules for a specific context?'), to determine whether a specific transaction satisfies the requirements of a scheme ('is my transaction compliant with the rules of this scheme?'), or to translate the requirements of one scheme into those of another scheme ('since my transaction satisfies the rules of this known scheme, does it also satisfy the requirements of this different but similar scheme?').

The most direct intended societal impact of LIGHTest is to improve security in electronic transactions. Specifically, LIGHTest can be used to facilitate the retrieval of authoritative information in relation to electronic identification, electronic signatures, time stamps and other trust services, which are regulated under EU law. These trust services are the foundation upon which many trust decisions are made every day. The security benefits that LIGHTest can create for society as a whole (including citizens, businesses and public administration) are the most direct social impact.

Beyond this application area however, LIGHTest can generically be used to facilitate the discovery and use of trust information across a virtually unlimited range of contexts. It does so using an open technology, building on a global and interoperable standard (the DNS) that is transparent to any aspiring users, and allows it to be tailored to its context. In this way, LIGHTest thus supports transparency, accountability, economic growth and security in the information society.

2. Document Information

2.1 Contributors

Name	Partner
Hans Graux	TIL
Rachelle Sellung	USTUTT

2.2 History

Version	Date	Author	Changes
0.1	13.06.2017	TIL	Initial outline
0.2	06.07.2017	TIL	First content of sections 4 and 5
1.0	09.08.2017	TIL and USTUTT	Finalisation
1.1	31.08.2014	TIL	Quality review updates - typos

3. Table of Contents

3.1 Table of Figures

N.A.

3.2 Table of Tables

N.A.

4. Introduction

This deliverable D2.9 – Social Impact Report was produced as a part of Task 2.7: Legal, Ethical and Societal Requirements and Constraints. Within the LIGHTest project, this task is intended to identify and address the ethical and societal implications of LIGHTest. Legal and ethical requirements are assessed elsewhere, notably in D2.10 - Legal, Ethical and Societal Requirements and Constraints. This deliverable focuses on the potential societal implications of LIGHTest, describing and assessing briefly how LIGHTest can impact society positively or negatively.

Generally, LIGHTest is predicated on the concept of supporting trust management (including discovery of trust information, trust translation and trust validation) in a multitude of contexts using the global DNS infrastructure. The general ambition of LIGHTest therefore is to facilitate and streamline trust management, which is the foundation of security. Every security critical system, application, or process is ultimately based on trust: decisions to grant or deny access to certain information, systems or processes are based on an assessment of whether available information is sufficiently trustworthy to permit the desired activity. These types of decisions are made every day in virtually every transaction we are involved in: a concierge decides whether to trust your identity in order to allow you into a building, a bank decides whether to trust your credentials in order to permit a payment, and business partners in a meeting decide whether you are indeed an authorised representative of your organisation.

From that perspective, trust is the foundation on top of which every system or process in the information society is built. If an illegitimate or hostile party manages to gain trust, it can compromise any system. Technology provides part of the solution, but not all of it: systems that feature near-absolute and cryptographically sound security can still be compromised if a skilled attacker obtains access to the relevant credentials or manages to circumvent them. By impersonating legitimate players or components, an attacker can gain access, manipulate data, or trigger illegitimate actions. Any security-critical system, application, or process is therefore only as secure as the trust management that builds its foundation and that permits presented information to be validated and assessed.

LIGHTest aims to provide a solid and secure foundation for supporting trust management and trust decisions. It renders trust management not only easier for verifiers, but also more secure, through the use of an open and transparent system for the discovery, translation and validation of trust information. In this way, it significantly reduces the attack surface of all systems that use LIGHTest for their trust management needs. This reduces opportunities for fraud, and thus also the cost of combating fraud, bringing social benefits not only to potential victims, but also to society, which would otherwise bear most of the costs of enforcement.

As will be explained in the sections below, LIGHTest can bring security benefits to a wide range of applications, systems and processes. Due to its open approach to discovering, translating and validating existing or new applications and systems, and due to its potential applicability even to complex electronic transactions, LIGHTest brings the benefits of a more solid trust management foundation to a wide range of application areas and stakeholders. This makes society more secure, and creates new opportunities for innovation and international – even global - cooperation.

Due to its almost universal applicability, LIGHTest brings these benefits of an improved security foundation to every facet of society, including citizens, businesses, and public administration.

The increased security is relevant to a wide range of application areas including finance, health, commerce, manufacturing, and many more. It can help to protect sensitive data of all kinds, including innovations that strengthen the competitiveness of European enterprises and the protection of personal data. When used for the protection of critical infrastructures such as power plants, energy networks, financial or transportation systems, the increased security provided by LIGHTest can help to guarantee values on which our society relies.

However, LIGHTest does not revolve exclusively around security. It also provides a generic tool that allows any citizen, business or organisation to reference trustworthy information, and that allows third parties to make accurate decisions based on that information. LIGHTest thus supports transparency and accountability through an open and broadly accessible toolset. In this way, LIGHTest can create significant positive social impacts. The sections below will examine this potential in greater detail, and will also indicate how potential negative impacts can be avoided.

5. Direct security and trust impacts of LIGHTest

The social impact which was initially targeted by the LIGHTest proposal relates to the specific context of electronic identification and trust services. Within the EU, electronic identification and trust services are governed by the eIDAS Regulation, i.e. 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. As the name suggests, this Regulation creates a harmonised EU level legal framework in relation to:

- The cross-border recognition of specific means of **electronic identification**. Essentially, the eIDAS Regulation allows Member States to notify means of electronic identification (such as eID cards or mobile identification systems) which are used towards the public sector within their own borders, and, subject to certain legal requirements and procedures, thereafter requires other Member States to recognise these notified means within their own e-government applications as equivalent to their own national means of electronic identification.
- The legal value of certain well-defined **trust services,** specifically electronic signatures, electronic seals, time stamps, electronic registered delivery services, and website authentication. Contrary to the provisions on electronic identification (which are oriented towards the public sector), the provisions on trust services emphatically consider these as market services which can be provided and used in a purely public sector context.

Given the scoping of the eIDAS Regulation, it provides a clear legal underpinning for answering some of the most crucial trust management questions, including who a person is and who they represent (both covered under electronic identification), whether a communication comes from them and whether it has been changed (provided by electronic signatures and electronic seals), when a specific piece of information existed (time stamps), whether a website is controlled by the entity claiming control over it (website authentication), and whether a message was securely sent and received by specific identified entities (electronic registered delivery services).

The legal toolbox created by the eIDAS Regulation is thus already quite broad and very useful in practice to facilitate certain trust management questions. To make sure that the Regulation functions effectively and that these services can all be deployed in the market, the Regulation establishes a very clear legal framework for supervising the trustworthiness of these 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).

- The most trustworthy[1] 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.

The trust model of eIDAS is clear and complete. None the less, it has some shortcomings that LIGHTest can help to address. Firstly, as an EU level regulation, it doesn’t affect means of identification and trust services outside the European Union, limiting the geographic reach and impact. Secondly, it uses specific EU level tools to communicate the trust scheme information, namely the European Official Journal, and the trusted lists managed by Member State supervisory bodies. The latter are based on a European technical specification (namely ETSI TS 119 612), which must mandatorily be used under an implementing decision of the eIDAS Regulation[2].

As a result, the eIDAS Regulation cannot trivially be upscaled to have a more global scope, unless other countries can be convinced to use the same trust management model and technological choices.

To address this point, one of the earliest visions of LIGHTest was to re-implement the exact same trust model behind eIDAS using the DNS system instead. 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

[1] 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.

[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

would be 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 regions of the world could easily follow suit by making their own trust information (e.g. in relation to trusted identities in China, or trust services in the USA) discoverable via the DNS system, creating interoperability without having to adhere to a European ruleset or standard.

It should be noted that LIGHTest therefore doesn’t reject the trust model behind eIDAS or question its impact in practice. Rather, it aims to explore whether an alternative model for the discovery and validation of the trust management information behind eIDAS (like the notified means of identification and qualified trust service providers) could be used, in a way that strengthens internationalisation and harmonisation.

Furthermore, using DNS could also facilitate trust translation: where the eIDAS approach is perfectly suited for establishing equivalence between European means of identification and trust services, it is less capable of doing so for non-European ones where the same information is not available. The DNS could help to overcome that, by applying a homogeneous method of discovering comparable trust information on identification means and trust services. LIGHTest acknowledges that this step isn’t sufficient to solve the translation puzzle: the much harder step is defining precisely which non-European identities are equivalent to which European ones, and which non-European trust services satisfy the requirements of European qualified ones.

LIGHTest doesn’t solve this question, and doesn’t claim that trust translation somehow becomes trivial once trust information is discoverable through the DNS. The project does not assume that all information which can be discovered via the DNS will automatically be equally trustworthy. Rather, LIGHTest aims to show that the DNS is viable as a mechanism for discovering and validating trust information, and that it can also be used as a tool for translating trust.

In more pragmatic terms: if two partners (e.g. the EU and the USA) have decided that they wish to acknowledge the equivalence of certain electronic identities and/or trust services, they could use the tools that LIGHTest will provide to discover their trust scheme information, to validate it in individual transactions, and even to facilitate the translation of trust via the DNS based on their agreed equivalence rules. LIGHTest does not establish the equivalence or recognition as such; rather, it provides the toolset to find, validate and translate trust information in a homogeneous way, using a globally accepted standard.

This is the initial social impact claim of LIGHTest: it aims to foster interoperability and mutual recognition of trust services and electronic identification at the global level. Given the role of these services as critical enablers of security in any electronic transactions, the potential beneficial social impact of using the same global and trusted technology to solve this problem across the world is vast: trust services and electronic identities can be better leveraged while fully respecting national sovereignty on this point, international business transactions can be better secured as can e-government services and even citizen-to-citizen communications, innovation can be spurred and economic growth supported.

In contrast with these anticipated beneficial social impacts, negative impacts should be negligible. This is principally because LIGHTest does not aim to replace or erode existing trust schemes or government supervision models, which could certainly have a negative impact. To the contrary, LIGHTest provides a tool to better communicate, validate and use such schemes, using an established, secure and trusted technology, namely the DNS.

While LIGHTest does not exclude or solve flaws that could exist in schemes outside of LIGHTest – e.g. countries or organisations may discriminate against foreign trust services for irrational or political reasons – it does not exacerbate such problems either, or create new variations of these problems. In fact, LIGHTest could even become a driver to resolving these problems too, since the DNS system is highly transparent, and any unlawful discrimination thus becomes highly visible and explicit, making it easier to identify and discuss problems.

Generally, within the initial focus area of LIGHTest – electronic identification and trust services as security enablers – the social impacts of LIGHTest are highly positive, with no clear negative risks.

6. Technological neutrality and openness – implications and potential impacts

In the preceding section, we explained the potential social impacts of LIGHTest from the principal perspective of the eIDAS Regulation (electronic identification and trust services), and the related security benefits for electronic transactions. This was the main initial focus of the LIGHTest project. However, the scope of application and the resulting social impacts of the LIGHTest technologies are significantly broader.

LIGHTest inherently provides technological neutrality, transparency, and overall flexibility. It is a technology which builds on the openly available DNS specifications, for which the source code needed to provide the LIGHTest functionalities will also be made openly available to interested parties, along with the relevant information for embedding LIGHTest into any pre-existing software or service.

The result is that the LIGHTest infrastructure can be applied to a broad array of different use cases, which significantly broadens its potential social impact. This section first dives more deeply into the LIGHTest infrastructure's strength of being a neutral technology and how it could be applied to a multitude of use cases beyond the eIDAS context that will be piloted in the project's duration. Secondly, this section focuses on the transparency and openness of the technology and how it could be used. Third, it goes over the flexibility of the LIGHTest infrastructure and its potential global impact. Lastly, the potential drawbacks of the LIGHTest infrastructure and technology will be touched on, to correctly recognise any weaknesses that should be tended to.

6.1 Neutrality of LIGHTest

The LIGHTest infrastructure is a neutral technology, in the sense that it is application agnostic: while it will be piloted for the eIDAS use cases during the project duration, the technology as such can serve as a standardized tool to support various types of digital transactions. The starting point is that trust information must be made discoverable via the DNS (for which LIGHTest will provide the tools), and that this trust information is thereafter used for validating transactions, translating trust schemes, or delegation of powers. LIGHTest infrastructure is a tool that can provide a standardized manner to support trust decisions in relation to any of these three basic functions (validation, translation, and delegation).

For the first function, verification, this is done by the LIGHTest component 'Trust Publication Authority', which basically lets the two parties on each end of the digital transaction to communicate or verify trust information (such as a trust policy or a trust scheme). In the eIDAS context (described in section 5 above), this would for instance relate to the verification whether the electronic signature on any given electronic document was created using the services of a European qualified trust service provider. The transaction in this case is the validation of the signature; the trust scheme is the supervision model of the eIDAS Regulation; and the role of eIDAS is to discover via the DNS whether the trust service provider is indeed supervised under the trust scheme.

But the neutrality of LIGHTest allows it to be used in very different contexts. For instance, if an American would like to study at a German University for a Master programme, it is necessary for them to verify that they have a Bachelor’s degree from a University that permits enrolment in the Master Program. To perform this process currently, it is necessary to get multiple notarizations to prove the authenticity and adequacy of the American Bachelor’s degree for enrolment in the German University’s Master programme. This process could be simplified by using the LIGHTest Infrastructure. LIGHTest can support this process: the German University would verify firstly that the student has a degree from an accredited American University, for instance by using the DNS records from the U.S. Department of Education to determine that the diploma and Bachelor’s programme are real and trustworthy (the discovery and validation functions of LIGHTest). This would automate the process that would typically take days or weeks to achieve.

Next, the German University could use LIGHTest to access the translation policies from e.g. the Germany Ministry of Education, to assess whether an equivalence has been established between the University’s Bachelor degree requirement, and the American Bachelor degree (the translation function of LIGHTest). If so, it can accept and enrol the student automatically, without notarisation processes or case-by-case assessments. If not, the assessments will still need to be done, and the outcome (either positive or negative) could be integrated into the translation policy so that re-assessment will not be necessary in the future. This second function is performed by the LIGHTest component ‘Trust Translation Authority’, which allows for the capability to determine equivalence between two trust schemes, and thus allows relying parties to determine whether a certificate or digital document that meets the requirements of one scheme also meets the requirements of the other.

This example illustrates the potential utility of LIGHTest in resolving even very complex trust decision problems. Since the viability of LIGHTest will be tested in this project, such highly complex use cases are not piloted during the pilot itself, but conceptually the LIGHTest technology should be usable to address these situations. Of course, the limitations should also be recognised: the university example would require that competent ministries of education exist that publish accredited universities via the DNS, and furthermore that recognition (translation) policies are objectively and formally drafted in a way that allows them to be applied automatically. Neither of these conditions is presently satisfied. None the less, the example shows the potential of LIGHTest beyond the tightly defined identification and trust service context.

6.2 Transparency and openness of LIGHTest

Transparency and openness are central principles of LIGHTest, which is visible in many areas. Firstly, DNS is used as the technology for discovering trust information and trust schemes. By design, the DNS is transparent: its specifications are entirely open without restriction to any interested party, so that any party can verify how it operates and what assurances are behind it. The LIGHTest project builds on this by creating technological components that allows trust information and trust schemes to be discovered via the DNS, and to allow validation and translation. These components will be made available as open source software, documented by publicly accessible deliverables, allowing any interested third party to conduct the necessary verifications, and to implement or modify LIGHTest into its own services. Transparency and openness are thus built into LIGHTest.

There is however an even more compelling and socially more relevant argument for calling LIGHTest open and transparent. At its heart, LIGHTest aims to support automated trust decisions (through validation of transactions, delegations or trust translations). Presently, the rules behind these decisions are often opaque: rules are not comprehensively defined or publicly available, so that relying parties can be made subject to hidden discrimination or unfair treatment.

Continuing the academic example above: a student who wishes their degree to be recognised in a third country currently cannot know comprehensively which factors will be considered, or whether congruent or different decisions have been made in the past, and why. In more practical terms: a student from the University of Mississippi may see their diploma declined, while a student from Yale University may see theirs accepted, without knowing the reasons behind it. Students from the University of Shanghai may be accepted, and those from Mogadishu declined, without knowing the objective reason.

LIGHTest requires that trust policies and trust schemes (including translations) are formalised and made accessible in a way that allows third parties to use them automatically, thus eliminating the potential for arbitrary discrimination. There will be perfectly valid reasons for accepting some transactions and rejecting others, but LIGHTest requires them to be made explicit. This supports social transparency and openness, creates accountability, and supports a more equal and fair society. This is a major social impact of LIGHTest.

Finally, there is no barrier to entry to using LIGHTest (other than the need to be transparent and open). The technology and relevant know-how will be available freely, and can be downloaded, implemented and used by citizens, businesses and public administrations alike, including non-profits and SMEs. It is a significant equalising technology, and this too is a major contribution of LIGHTest.

6.3 LIGHTest as a global and flexible technology

A key objective of LIGHTest is to provide a global and flexible technology. This priority was in fact one of the major drivers behind LIGHTest from the onset: observing that the eIDAS Regulation provided a strong and credible trust model for electronic identification and trust services within the European Union, the goal was to find a way to extend this model both geographically (identities and trust services outside the EU) and contextually (other trust information than the trust schemes of the eIDAS Regulation).

For this reason, LIGHTest builds on the DNS, a global and trusted communications technology, which LIGHTest aims to reuse. No part of the LIGHTest technology is inherently limited to an EU context: the selected pilots use the eIDAS Regulation as a starting input, but as noted above, this is only one use case of many. LIGHTest as such can be used anywhere in the world to support trust management and trust decisions.

LIGHTest as a technology is flexible too, since it does not replace or write trust schemes, but rather creates a toolset that allows trust schemes to be managed and used homogeneously and efficiently in any type of use case. This cuts down on the need to reinvent the wheel on a case by case basis: LIGHTest can be used for any trust scheme and any trust decision, whether based on a legislative framework, contractual assurances or even individual preferences, even at a very small ad hoc scale. The sole requirement is that the user must be willing to formulate specific trust decision rules and to use these in practice (i.e. it must be willing to make consistent decisions).

The LIGHTest technology can also be integrated with existing products or services to further improve security, flexibility, and scalability. Indeed, some of the pilots of LIGHTest precisely aim to integrate LIGHTest technology into existing software that supports trusted communication, to show that LIGHTest can enhance the functionality of existing products, rather than requiring that they are tailor built from scratch with LIGHTest in mind.

This too is an expected social impact of LIGHTest: it allows existing applications and services to grow to a global scale, thus boosting economic growth, interoperability and security.

6.4 Potential negative impacts and how to mitigate them

Inherently, LIGHTest is an agnostic technology that has no obvious negative social impacts. This is not to say that negative impacts cannot possible occur, but rather that these negative impacts would be the result of a misapplication of LIGHTest or incorrect expectations. Specifically, three categories of potential negative social impacts have been identified:

- Firstly, the **risk of misuse of the DNS**. LIGHTest depends on trust information or trust policies to be discoverable via the DNS. This implies that users of LIGHTest must create pointers in the DNS to specific trust policies, trust schemes or trust information. This creates the risk that users see the DNS as a tool for making any information discoverable; this is indeed already possible (already prior to LIGHTest), but would be a mistake. The DNS should be used to make information discoverable that should be publicly available. More specifically, private or confidential information should not be disclosed via the DNS. This is also why LIGHTest has specific legal and ethical requirements not to make personal data discoverable via the DNS.
- Secondly, the **misunderstanding of the reliability of trust information.** LIGHTest will use the DNS to retrieve trust information, such as trust policies or trust schemes. This does not imply that this trust information is inherently reliable or a good basis for decision making. More generally, LIGHTest does not take the position that any information findable via the DNS is correct, accurate, complete, trustworthy, or fit for purpose. As explained in D2.10 - Legal, Ethical and Societal Requirements and Constraints, the legal value and validity of information which is discovered via the DNS does not come from the DNS itself; it must come from elsewhere. In LIGHTest, this issue is resolved by creating an appropriate contractual framework around the pilots; if successful, the legal value could also originate from legislation (i.e. laws might specifically refer to the use of LIGHTest technology for the publication and discovery of authoritative information). LIGHTest as such does not create legal value from scratch; it is merely a toolset.
- Thirdly, the **assumption that LIGHTest inherently ensures fair trust decisions.** As explained above, the value from LIGHTest comes from the fact that it provides a technology for the discovery, validation and translation of trust information and for making trust decisions. LIGHTest however does not ensure that these trust decisions are reasonable or fair. By way of example: a company's policy in relation to receiving orders from customers might simply be that it refuses any business from a given country, or it may only accept electronic signatures from its own region. As a more extreme example: an organisation may only recognise men as valid representatives of a company, systematically refusing to communicate with women. LIGHTest would not filter out unfair, imbalanced or blatantly illegal trust policies; it would only make them explicit and visible. LIGHTest thus presents a step forward compared to the status quo – in the sense that it becomes harder to hide unlawful policies – but it is not a panacea that ensures universal lawfulness and unfairness.

It should be stressed that these potential negatives are not inherently related to LIGHTest; rather, they relate to potential misuses or misunderstandings of LIGHTest, against which LIGHTest explicitly counsels.

7. Conclusions

As the overview above has shown, the potential beneficial social impact of LIGHTest is vast. The most direct intended impact of LIGHTest is to improve security in electronic transactions. Specifically, LIGHTest can be used to facilitate the retrieval of authoritative information in relation to electronic identification, electronic signatures, time stamps and other trust services, which are regulated under EU law. These trust services are the foundation upon which many trust decisions are made every day. The security benefits that LIGHTest can create for societye (including citizens, businesses and public administration) are the most direct social impact.

Beyond this application area however, LIGHTest can generically be used to facilitate the discovery and use of trust information across a virtually unlimited range of contexts. It does so using a neutral and open and technology, building on a global and interoperable standard (the DNS) that is transparent to any aspiring users, and allows it to be tailored to its context. In this way, LIGHTest thus supports transparency, accountability, economic growth and security in the information society.

8. 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 15 May 2017

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 15 May 2017

See notably WP136, Opinion 4/2007 on the concept of personal data, adopted on 20th June 2007; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf; last visited on 15/05/2017

9. 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 people’s 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), IBM Danmark (DK) and Globalsign (FI). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.