D10.9

Standardization Report Year 2

Document Identification	
Date	01.08.2018
Status	Final
Version	Version 1.0

Related WP		**Related Deliverable(s)**	
Lead Authors	F.-M. Kamm	**Dissemination Level**	PU
Lead Participants	G+D	**Contributors**	Atos, NLnetLabs, OIX, FhG, TUG
Reviewers	EEMA, Correos		

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 focus of task 10.5 is to evaluate and contribute to international standardization activities and thus to align the project with global developments. This works bi-directionally, as partners of LIGHTest are also members of various standardization groups and bodies and industry alliances. Therefore, results from these groups can be fed into the LIGHTest project to allow for quick adjustments of the LIGHTest concept, if needed. In addition, innovative results from LIGHTest can be contributed to the standardization groups to maximise the impact of the project.

This deliverable summarizes the main activities of the most important standardization groups and industry alliances in which LIGHTest partners are actively involved. It also highlights the impact that group activities could have on the project.

As standardization activities are typically long-term activities with moderate progress within a reporting period, this deliverable is designed as continuously updated report, concentrating on the main activities and results within a certain reporting period.

For improved readability, chapters 4-6 are structured by standardization bodies or industry alliances and – if applicable – by subgroups.

2. Document Information

2.1 Contributors

Name	Partner
Frank-Michael Kamm, Jan Eichholz, Ulrich Stutenbäumer, Werner Neß,	G+D
Sue Dawes, Michelle Parkes	OIX
Martin Hoffmann	NLnetLabs
Sebastian Kurowski	FhG
Peter Lipp	TUG
Javier Cordero Presa	Atos

2.2 History

Version	Date	Author	Changes
0.1	23.07.2018	F.-M. Kamm	Initial version
0.2	23.07.18	Michelle Parkes	OIX part added
0.3	23.07.18	Martin Hoffmann	NLnetLabs part added
0.4	23.07.2018	Peter Lipp	TUG part added
0.5	23.07.2018	F.-M. Kamm	G+D part added
0.6	23.07.2018	J.C. Presa	Atos
0.9	24.07.2018	F.-M. Kamm	First complete version
0.95	24.07.2018	F.-M. Kamm	Integrated 1st reviewer comments
1.0	01.08.2018	F.-M. Kamm	Integrated 2nd reviewer comments

3. Table of Contents

4. ISO/IEC JTC1

4.1 SC 17 WG 4

4.1.1 Scope of the working group

In the last year the official scope and title of JTC1/SC17/WG4 has been discussed and was adopted by JTC1 SC17. The title was changed from "Cards and Personal Identification" into "Cards and Security Devices for Personal Identification". The scope now deals not only with identification documents and cards (ICC), but also with security devices and tokens.

Examples reflecting the new scope are standards like "ICC-managed devices" or "Privacy-enhancing protocols and services". The main topic of this scope change is to include more and more "personal identification with mobile devices" in the work of SC17 WG4.

4.1.2 Main achievements in year 2

Based on a study period in 2017 for Mobile ID Management with G+D's role as a rapporteur the final report leads to New Work Item Proposal (NWIP) for a standardisation project. The ballot of the proposal was successful and with new inputs and contributions a first working draft is in preparation. The new standard will have the ISO-number and name: "ISO/IEC 23220: Building blocks for identity management on mobile devices".

SC17 established in the meantime a new Chairman Advisory Group Sub Group reflecting the new topic of "Virtual ID". Within the group there is consent that the ID Management activities should cover also topics for virtual IDs. Therefore many members of WG4 joined and support the CAG sub group. First Webex conferences took place.

4.1.3 Impact on LIGHTest

The activities of SC 17 WG4 are focused on standardized mechanisms to manage identities on different mobile devices. The definitions are intended to be used also in other areas, e.g. authentication, verification and identification of legal entities. Therefore, the activities of this working group are strongly related to one of the major use cases of the LIGHTest infrastructure, i.e. the mobile ID application (WP 7). In this use case, derived identity credentials are generated and stored on mobile devices for further usage. The new standardisation project that has been started on ID management on mobile devices is an excellent fit for LIGHTest related topics as well as for feedback into LIGHTest on latest standardisation trends. With G+D as an active partner in this group a strong link to the LIGHTest project is given.

4.2 SC27 WG 4

4.2.1 Scope of the working group

The Scope statement of the ISO subcommittee (SC) 27, states that it focuses on the development of standards for the protection of information and ICT, including generic methods, techniques and guidelines to address both security and privacy aspects such as:

- Security requirements capture methodology
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components
- Security aspects of identity management, biometrics and privacy
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems
- Security evaluation criteria and methodology

As part of SC27, the scope statement of the WG 4 covers aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the lifecycle of such products and systems. The topics of WG 4 thus include:

- ICT security operations (for example readiness, continuity, incident and event management, investigation),
- Information lifecycle (for example creation, processing, storage, transmission and disposal),
- Organizational processes (for example design, acquisition, development and supply),
- Security aspects of Trusted services (for example in the provision, operation and management of these services),
- Cloud, internet and cyber security related technologies and architectures (for example network, virtualization, storage),

for digital environments, such as cloud computing, cyber, Internet, and organizations.

4.2.2 Main achievements in year 2

A 12 month Study Period on information security guidance for PKI Service Providers, that was initiated on October 27 on the 23rd ISO/IEC meeting was closed as per WG decision of the 24th meeting of ISO/IEC JTC 1/SC 27/WG 4. The study period was intended to determine the successor project of ISO/IEC TS 14516 “Guidelines for the use and management of electronic trust service providers“ as per WG decision of the 22nd ISO/IEC meeting. The Study Period

identified issues in terms of collisions between the terminologies of the previously cancelled ISO/IEC TS 14516 proposal and ETSI EN 319 411-1. A standardization project should therefore cover both terminologies. Additionally, the new standard should consider the provision of services by Certification Service Operators to one or more Certification Authority, and the optional provision of subsets of PKI services. It should be tailorable with respect to different security level requirements, use ISO/IEC 27009 to augment and extend ISO/IEC 27002, and should avoid overlapping with existing security controls in ISO/IEC 27002.

The discussion of the Study Period resulted in the recommendation to terminate the study period, and to concentrate the efforts on bringing ISO 21188 to a generic standard and to include the gaps that have been identified within the study period. ISO 21188:2006 “Public key infrastructure for financial services – Practices and policy framework“, which is covered by ISO/TC 68/SC 2 “Financial services, security“. The discussion concluded on the recommendation to contact TC 68 SC2 to participate in the SC27 meeting (and/or vice versa), and on the agreement that any generic PKI security standard has to be handled within SC 27.

A new study period was created to report on the collaboration with TC68 SC 2. The study period collaborated with TC 68 SC2 in order to find out how ISO 21188 could be used, potentially as base document for the SC27 standard. If the collaboration with TC68 SC2 does not yield a common proposal, a new work item proposal should be developed in SC27 to cover the gaps identified above. A request to transfer ISO 21188:2018 to SC27 WG4 has been declined by TC68 SC2. However, stronger collaboration will be sought on in the future, regarding PKI standards. Currently there are no further actions on a SC27 specific PKI standard.

A new study period has been initiated on the topic of IoT domotics. It is currently determining the reuse of existing standard, in order to ensure interoperability within the SC27 list of standards. The currently affected standards include ISO/IEC 30141, 27030, 27033, 27034, 27040, 24767-1, 24767-2, 14543, and 15045-3. LIGHTest could potentially impact this topic in the field of inter-device trust. However, the exact contribution will be clarified in light of the outcome of the study period, and the scope of the eventually created draft.

4.2.3 Impact on LIGHTest

The creation of a generic standard for the use and management of electronic trust service providers could impact the design and usefulness of the trust scheme publication authority TSPA (Workpackage 3), specifically the universal framework for the publication of trust schemes. Therefore, the further development regarding the development of a SC27 specific PKI standard will be closely monitored, in order to ensure alignment with the TSPA and vice versa. The same holds for any efforts in the field of IoT domotics.

5. ETSI

5.1 TC ESI

5.1.1 Scope of the working group

TC ESI is responsible for Electronic Signatures and Infrastructures standardization within ETSI. TC ESI is the lead body within ETSI in relation to Electronic Signatures and Infrastructures, including the preparation of reports and other necessary activities, by

1. Developing generic standards, guides and reports relating to electronic signatures and related trust infrastructures to protect electronic transactions and ensure trust and confidence with business partners,
2. Liaising with other ETSI bodies in relation to electronic signatures and related trust infrastructures,
3. Liaising with bodies external to ETSI in relation to electronic signatures and related trust infrastructures,
4. Establishing a continuing work plan in relation to electronic signatures and related trust infrastructures.

TC ESI works, in collaboration will CEN TC 224, on the execution of EC Mandate M/460 to provide a rationalized framework for digital signatures standardization, which is closely related to implementing Regulation (EU) No 910/2014 (eIDAS).

Some of the relevant standards developed in ESI are:

- TR 119 400: Guidance on the use of standards for trust service providers supporting digital signatures and related services,
- EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation,
- EN 319 102-2: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Signature Validation Report,
- TS 119 441: Policy requirements for TSP providing signature validation services,
- TS 119 442: Protocol profiles for trust service providers providing AdES digital signature validation services.

5.1.2 Main achievements in year 2

Currently TC ESI works on signature validation protocols directed at signature validation services as well as a signature validation report format. Such implementations can benefit from results of LIGHTest, especially of WPs 3-6. However it is too early to introduce LIGHTest results into standardization.

5.1.3 Impact on LIGHTest

Several standards that have been or are developed within ESI are relevant for using LIGHTest mechanisms in trust decisions. LIGHTest needs to be aware of any requirements when using ESI as a base infrastructure in e.g. eIDAS conformant signature validation.

6. Alliances/Industry

6.1 FIDO Security WG

6.1.1 Scope of the working group

The Security Requirements Working Group defines the policy and process for security evaluations and certifications of FIDO implementations, taking into account the ongoing evolution of security requirements and threats. The purpose of these security requirements is to produce security certified FIDO implementations in a way that is meaningful to relying parties, users, and B2B consumers of FIDO implementations, including security metadata and security certificates. Members of the LIGHTest project take actively part in the WG sessions.

6.1.2 Main achievements in year 2

A subgroup of the FIDO Security Working group for the definition of L1.5 has been created. Goal of this group is to define an enhanced software security based authenticator type. It is under investigation, if the certification can be done with the CSPN scheme defined by the French ANSSI.

- Security Levels have been re-sorted: Level 3 is now Level 2+
- Level 4 is now Level 3
- Level 5 is now Level 3+

The CC Partner Program for L3 certifications is ready. The FIPS 140-2 partner program is progressing.

With this level definition, a FIDO authenticator product can prove its security and attack resistance level in comparison to other types of authenticators. As part of the attestation scheme, this information provides additional assurance for the relying party about the security level of the used authenticator.

6.1.3 Impact on LIGHTest

The FIDO protocol and the work of the FIDO alliance is of significant importance for the LIGHTest project since the concept of a mobile ID derivation scheme is based on this protocol (WP 7). In the overall context of LIGHTest and the quest to enable trust propagation from the primary ID level to the derived mobile ID, the FIDO security evaluation scheme is a fundamental backbone for determining the overall trust level of a derived ID. The different security levels represent different types of secure storage of ID credentials and a different attack resistance. As a consequence, the FIDO security level will have a direct impact on the Level of Assurance of the derived ID. Therefore, it is essential for LIGHTest to follow the activities of the security

working group and to verify the compatibility of the security levels with the LoA and trust propagation scheme within LIGHTest.

6.1 JHAS

6.1.1 Scope of working group

JHAS is the Joint Interpretation Library (JIL) Hardware related Attacks Subgroup. The Joint Interpretation Library (JIL) is a European working group for questions regarding the application of the Common Criteria with participation from UK, France, Spain, the Netherlands and Germany. JHAS is a sub-group of this working group but originated from the Eurosmart working group ISCI-WG 2.

The scope of this group is the discussion and evaluation of attacks on smart cards or other form factors and related products, the maintenance of a countermeasure list and the document Attack Methods for Smartcards and Similar Devices (only available to CBs, ITSEFs and manufacturers active in JHAS) and the public document Application of Attack Potential to Smartcards (http://www.commoncriteriaportal.org/files/supdocs/CCDB-2013-05-002.pdf).

6.1.2 Main achievements in year 2

The active participation in all JHAS meetings and the discussion of new addressed attack paths and their CC ratings with relevant G+D experts was the main G+D contribution to the JHAS work in the last year. Additionally the recent JHAS initiative for improving the CC process was monitored and actively supported by G+D. Discussion about unrealistic attacks took place in a one day Workshop which was organized by G+D. Representatives from scheme, labs and vendors discussed very open and fruitful several discussed attacks with have resulted in unrealistic or unfair rating in the past and about 5 specific proposals regarding the interpretation of existing JHAS rating rules.

G+D is active member in different JHAS subgroups as:

- Cheating Vendors: output is a public document that discusses the options for customers to improve their assurance in certified products.
- System on Chip (SoC): output is guidance for the Certification of a Secure Sub-System within a SoC.
- Open Samples: output is an update of the relevant chapters in the document *Attack Methods for Smartcards and Similar Devices* that uses open samples (with known secrets/keys or deactivated counter measures) for different attack scenarios.
- Unrealistic attacks: planned output is the alignment and update of ranking rules in the JHAS document *Attack Methods for Smartcards and Similar Devices* to enable a CC evaluation laboratory to better focus on realistic attacks.

6.1.3 Impact on LIGHTest

Similar to the FIDO security working group, the JHAS activities are strongly related to the security level of storage environments for mobile ID credentials. They will therefore have a direct impact on the overall LoA and the trust propagation within the LIGHTest mobile ID use case. JHAS is focused mainly on hardware-based storage environments as they are used in smart cards. However, in more and more mobile device platforms similar environments are used as embedded chips and therefore play a major role especially for the high-end part of the LoA levels.

6.2 GSMA Mobile Connect

6.2.1 Scope of the working group

GSMA's Mobile Connect API is based on the same standards and attributes as defined by the OpenID Connect specification. OpenID Connect was adopted by the GSMA as the base protocol and framework for Mobile Connect, because of its openness and robustness.

The global infrastructure for electronic transactions is increasingly optimised for mobile devices. Most of the electronic transactions envisioned in the LIGHTest project rely on the strong mobile identity interoperability in use cases such as identification, authentication and signing of transaction data. In particular the work in WP7 "Derivation of Mobile ID's", that investigates, defines and develops an infrastructure for trust propagation of derived mobile IDs and for handling trust information on the device side, will be impacted by ongoing standards, development, and the relationship the LIGHTest project has with the GSMA and others.

On behalf of LIGHTest, the Open Identity Exchange is engaging in an ongoing informal liaison relationship focused on LIGHTest's ID Derivation work whose relationship will play a key role in the global adoption and interoperability of the LIGHTest effort. This informal liaison allows an agile engagement without the cost and complications of IPR and other business obligations.

6.2.2 Main achievements in year 2

During Year 2 we have connected more closely with GSMA via their involvement with the Mobile Operator Discovery Registration & Authentication (MODRNA) working group of OpenID Foundation (see section 6.4 for more information on engagement with OpenID and the MODRNA working group).

6.2.3 Impact on LIGHTest

The landscape of electronic transactions is dominated by mobile devices. Most of the electronic transactions in the context of the LIGHTest project are related to electronic identities and electronic signatures. In particular the work in WP7 will be impacted by the relationship the LIGHTest project has with the GSMA.

The GSMA is one of the four international bodies that it is proposed that we co-ordinate with for the ID Derivation work in particular, whose relationship will play a key role in the global adoption and interoperability of the LIGHTest effort.

The Open Identity Exchange (OIX) is engaging in an ongoing informal liaison relationship focused on LIGHTest's ID Derivation work whose relationship will play a key role in the global adoption and interoperability of the LIGHTest effort. This liaison allows for an agile engagement without the cost and complications of IPR and other business obligations.

6.3 Cloud Signature Consortium

6.3.1 Scope of the working group

The Cloud Signature Consortium started a group of industry and academic organizations committed to build a new standard for cloud-based digital signatures that will support web and mobile applications and comply with the most demanding electronic signature regulations in the world.

The goal is to provide a common technical specification that will make solutions interoperable and suitable for uniform adoption in the global market. This effort was inspired by the need to meet the highest level requirements of the European Union's Regulation on Identification and Trust Services (eIDAS), but its impact is expected to be global as demand for highly secure digital solutions continues to rise.

The Cloud Signature Consortium aims to make it simple for EU businesses and governments to successfully comply with this new regulation. The vision is to create a single digital market, across Europe and the globe.

The Cloud Signature Consortium has changed its legal status to an established non-profit association pursuant to Belgian Law located at De Meeûssquare 37, 4th floor, 1000 Brussels.

6.3.2 Main achievements in year 2

The consortium has published a draft for a signature creation API, based on web-services and JSON, which provides a standard interface allowing applications to access remote signature creation services, and is actively working on implementing these specifications. Work on signature validation service specification have been put on hold but will be worked on during the upcoming period.

6.3.3 Impact on LIGHTest

Since one of the use cases of LIGHTest is electronic signatures, this group has a high relevance for the project. Signature validation services will be able to use LIGHTest results for their implementations. Consortium meetings can be used to educate consortium members about LIGHTest.

6.4 OpenID Connect

6.4.1 Scope of the working group

The scope of the working group this first year was to begin the process of approach to the OpenID Foundation, the OpenID Board and the relevant OpenID working groups in order to inform and align with one of the important international standards bodies that LIGHTest wishes to collaborate with.

The OpenID standard provides a framework for communication between the OpenID acceptor (the 'relying party') and the identity provider. The OpenID 'Attribute Exchange extension' to the standard facilitates the transfer of user attributes, such as name and gender from the OpenID identity provider to the relying party. The current version is OpenID Connect 1.0.

A standard is only as good as its adoption and as of March 2016 significant adoption has occurred, with over 1 billion OpenID enabled accounts on the Internet, involving organisations such as AOL, Flickr, France Telecom, Google, Amazon.com, Microsoft, Wordpress, IBM, PayPal and many others. Many of the larger organisations require users to provide authentication in the form of an existing email account or mobile phone number in order to sign up for an account, which then can be used as an OpenID identity.

Relevant OpenID Working Groups:

The MODRNA (Mobile Operator Discovery, Registration & autheNticAtion) working group is developing a profile of OpenID Connect tailored to the specific needs of mobile networks and devices, intended for use by mobile network operators (MNOs) providing identity services to Relying Parties and extensions to OpenID Connect that are needed in the context of GSMA's Mobile Connect initiative. These include transaction authorisation, account migration and server-initiated authentication.

The International Government Assurance Profile (iGov) working group is developing a security and privacy profile of the OpenID Connect allowing users to authenticate and share consented attribute information with public sector services across the world. This profile, once completed will allow standardised integration with public sector relying parties in multiple jurisdictions.

The Chairman of Open Identity Exchange is the Executive Director of the OpenID Foundation and is leading the global collaboration for LIGHTest with this standards body. The Open Identity

Exchange is engaging in an ongoing informal liaison relationship focused on LIGHTest's ID Derivation work whose relationship will play a key role in the global adoption and interoperability of the LIGHTest effort. This informal liaison allows an agile engagement without the cost and complications of IPR and other business obligations.

6.4.2 Main achievements in year 2

The consortium partner, Open Identity Exchange has continued to provide updates to OpenID Foundation Board meetings.

Recently at the Identiverse conference in Boston, OpenID Foundation agreed with the Open Banking Implementation Entity to integrate its standards development and certification efforts into the OpenID Foundation's effort. This offers LIGHTest an excellent opportunity to utilise OpenID Foundation's international outreach meet ups, workshops and conferences and become part of the agenda.

Two workshops have been planned in November 2018, one in Singapore and one in Sydney. Both workshops will feature LIGHTest along with Open Banking and will engage the OpenID Foundation community. A further workshop is planned in Europe in October with the same agenda. The intent is to update the community as a whole in at this appropriate time in the project. This outreach further afield, allows LIGHTest to be introduced into the Asia Pacific area, and also capitalise on the IETF meeting that will be taking place in Bangkok later in the year.

MODRNA

On an on-going basis, there will be regular calls set up with the MODRNA work group which will allow the long term aims of the LIGHTest project to be voiced and cover the current status of the standardisation work package and what needs to be achieved by the end of the project. LIGHTest will fit well into this working group due to the cross-operator and cross-country interoperability aspect of LIGHTest.

iGOV

Regular calls will be set up which will be similar to the above MODERNA working group, which will allow for engagement on the LIGHTest standardisation working package.

6.4.3 Impact on LIGHTest

An informal liaison with the OpenID Foundation can make significant contributions to the success of LIGHTest by coordinating with the development of the iGOV profile of OpenID Connect which will help map identity standards across the UK, US and Canadian governments.

Just as lightest builds on the successful infrastructure of the DNS systems, it can also build of the most widely adopted identity verification standard, OpenID Connect standard for

authentication. These standards will be critical to the success of the LIGHTest pilots and to the adoption of LIGHTest protocols and open source tools.

6.5 IETF

6.5.1 Scope of the working group

The Internet Engineering Task Force is a standards organization tasked with developing and promoting the technical protocols and other standards governing the Internet. It is a volunteer organization open to participation by anyone without formal membership.

Work within the IETF is taken up by topical working groups which are chartered to develop or maintain one or more protocols or technical areas of the Internet.

For LIGHTest, the IETF is relevant as the standards organization responsible for Domain Name Systems (DNS). Any extensions to the DNS developed as part of LIGHTest should be standardized by the IETF.

6.5.2 Main achievements in year 2

Another informal gathering similar to the Bar BoF arranged in March was held by NLNET during the 100th IETF meeting in Singapore in November 2017. Attendance was somewhat limited with only four people present in the meeting. Because of this, NLNET engaged members of the IETF's DNS community in hallway discussions wherever possible. Both in the meeting and in the discussions, the revised architecture for the LIGHTest infrastructure was received favorably.

During year 2, the IETF's DNSOP working group was active in an effort to standardize the use of underscore labels in DNS names, a feature heavily relied on by LIGHTest. NLNET observed and engaged in this process since it is a foundation for the standardization work to come out of LIGHTest. Once it has concluded or advanced far enough to build upon, the LIGHTest DNS standardization work will be picked up in year 3.

6.5.3 Impact on LIGHTest

Standardization work with the IETF is important for wide acceptance and deployment of LIGHTest as the DNS will be integral part of the LIGHTest framework. In addition, the DNS community in the IETF can provide valuable feedback regarding the architecture of the infrastructure and its security and reliability considerations.

6.6 Universal Postal Union

6.6.1 Scope of working group

The identified standards related to the project topics (iD authentication, eSignature, eStamp,…) are:

- **S33 - Interoperability framework for postal public key infrastructures**: The objective of this standard is to create a common Postal Public Key Infrastructure (PKI) to provide global certification and security services aimed at globally binding the identity of individuals and organisations with their public key. The framework itself and its first four elements (PKI structure, cryptographic algorithms, data formats and data dissemination protocols) are included in the initial draft standard.

- **S39 - Trusted Time Stamp**: The standardisation of the trusted time stamp can be seen as the electronic replacement of the present postmark on regular mail. As such, the service requires electronic security features to reproduce some characteristics of the traditional postmark such as a time and date stamp given by a postal operator acting as a trusted third party in a communication. The service is a first example of a Global Postal Trust Service (GPTS) allowing Postal operators to bring e-mail up to the same level of acceptance that hard-copy mail currently enjoys. Via the trusted time stamp service, e-mail messages will be given, by the Postal operators acting as a trusted third party.

- **S52 - Functional specification for postal registered electronic mail**: This standard defines the functional specification of a secure electronic postal service, referred to as the postal registered electronic mail or PReM service. PReM provides a trusted and certified electronic mail exchange between mailer, designated operators and addressee/mailee. In addition, evidence of corresponding events and operations within the scope of PReM will be generated and archived for future attestation. This standard is not used too much, apart from some operators who have adopted it.

- **S64 (predecessor of PostID, and just approved S68) - Postal identity management**: Describes identity management elements and identifies common protocols used to exchange identity assertions and attributes for the purpose of enabling customer access to applications in the postal network. The identity elements are defined to ensure interoperability of credentials issued by postal operators or by others for use in the postal network. It defines the terms and functions of postal identity management processes and environment. It is intended to provide a basic understanding of identity management roles, technologies, activities and principles.

- **S68 - Postal identity management trust framework**
  This standard describes the processes in establishing and managing digital identity systems, and how those systems can interoperate through the federation and use of

digital credentials across domains and applications. It defines a basic trust framework as well as listing the supported protocols necessary for technological implementation

All Universal Postal Union (UPU) standards have an access/use costs associated for all external entities.

6.6.2 Main achievements in year 2

The consortium partner, Correos has continued to provide updates on the standards and the activities of the UPU that might be of interest on LIGHTest project, as Correos is an active member if the UPU. After some analysis between these standards and the integration of LIGHTest standards, the main focus is on internet domain DANE as it will be used during the pilot use cases development. Still some key benefits of these standards are being evaluating during the design of demonstrator use cases as part of the implementation phase of LIGHTest platform.

6.6.3 Impact on LIGHTest

Since these standards are related to trust services within the eIDAS context and relevant for LIGHTest demonstrator use cases, LIGHTest results (e.g. the improved use of DANE) could be re-used by the UPU in order to enhance the latest top-level domain up to date. In addition, the LIGHTest community would be expanded by actively contributing to these groups, supported by the Universal Postal Union. This is an excellent opportunity to leverage LIGHTest results for a broader user community.

6.7 .post

6.7.1 Scope of the working group

.post is the UPU's sponsored top-level domain for the postal sector supported by the Domain Name System Security Extensions (DNSSEC). The domain's technical infrastructure became a reality in 2012, and member countries and their designated operators can now register for their domains and explore the possibilities of .post.

Some posts have plans to use .post to stimulate cross-border e-commerce and hybrid mail, for example. The platform's goal is to interconnect current and future electronic postal services and make them interoperable in a secure and trusted environment. It will authenticate postal service providers and strengthen the postal brand globally.

.post intends to link the physical and digital worlds, creating a secure platform that enables postal e-services to be delivered to all citizens and businesses. Applications, such as identity management, e-shops, e-payments, e-forms, secure postal mailboxes, address management, hybrid mail and advertising mail, would have a home on this future platform.

More than 70 per cent of the world's posts say that electronic services are strategically important to their business, according to a UPU research. This finding provides impetus to the goal of developing the .post (dotpost) platform, and the 2012 Universal Postal Congress decided that work should continue in this regard.

In 2009, the Universal Postal Union became the first United Nations agency to be granted a sponsored top-level domain for the postal sector. There is a Correos member (Victor Martin) that is part of the Steering Committee for .post, allowing LIGHTest to have a direct channel of communication.

6.7.2 Main achievements in year 2

During this second year of the project, the main focus is to continue the analysis of the key benefits of this standard, identifying how .post could obtain benefits from the integration of the LIGHTest results and vice versa. As the design and implementation phase is in progress, this mutual collaboration is being evaluated.

6.7.3 Impact on LIGHTest

Being .post 100% secured by DNSSEC, and as the case of UPU, the target is to re-use any LIGHTest results by UPU in order to enhance the latest top-level domain up to date. In LIGHTest, certificates will appear in three different places:

- as part of an electronic transaction whose trustworthiness needs to be verified,
- as part of secure network communication,
- as part of signatures for trust-related information.

In each of these cases, the certificates are used for verifying data only and LIGHTest needs to provide a way to verify in turn whether the certificates are indeed authorized to be used for this data.

In principle, DANE provides a solution for exactly this problem using DNS. The Transport Layer Security Protocol (TLSA) mechanism has been designed specifically for the second appearance if TLS is used as the transport protocol for secure network communication. LIGHTest only needs to specify that such records must be present and all certificates must validate considering their content when using the secure communication channel.

For the first appearance as part of an electronic transaction, there is a specific mechanism yet. The record data of either TLSA or SMIME records can be used to deliver the information necessary for verification – as they are identical, either can be chosen purely on taste. If they are to be used, a domain name for where these records will be placed needs to be specified and standardized as part of the LIGHTest project. Similarly, information for verification of certificates

used with trust-related information can be stored in DANE resource records under a yet to be specified domain name.

7. Summary /Conclusions

As shown in the last chapters (4-6), the LIGHTest project has a broad reach into global standardization activities due to the active engagement of project partners. Important use cases, like mobile IDs and electronic signatures, are well covered by several groups. Thus, the LIGHTest project is aware of important ongoing standardization activities.

The second year has already seen some progress on intensifying the relations between LIGHTest and some relevant standardization groups. Further progress is to be expected in year 3 when the project results of LIGHTest will become even more concrete and tangible. The foundation of new standardization activities in “classical” ISO/IEC groups related to mobile IDs (like in SC17 WG4) is really fortunate for the LIGHTest activities and opens up new opportunities to align with standardization.

In addition, existing liaisons with important groups like the IETF have been developed further, thus providing the foundation for an even intensified exchange in year 3.

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 started on September 1st 2016 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.

The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.